

安裝指南
January 5, 2009

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 \(http://www.novell.com/info/exports/\)](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 \(http://www.novell.com/company/legal/patents/\)](http://www.novell.com/company/legal/patents/) 中所列之一或多項美國專利，以及在美國與其他國家 / 地區之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 \(http://www.novell.com/documentation\)](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 \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](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為其各別擁有廠商的財產。

目錄

關於本指南	7
1 ZENworks Endpoint Security Management 綜覽	9
1.1 系統需求	10
1.2 關於 ZENworks Endpoint Security Management 手冊	10
2 安裝 ZENworks Endpoint Security Management	13
2.1 安裝前的資訊	13
2.2 安裝套件	13
2.2.1 關於主安裝程式	13
2.3 安裝選項	13
2.4 安裝順序	14
2.5 安裝 ZENworks Endpoint Security Management 之前	14
3 執行單一伺服器安裝	17
3.1 安裝步驟	18
3.2 啓動服務	18
4 執行多重伺服器安裝	19
5 執行規則配送服務安裝	21
5.1 安裝步驟	22
5.1.1 典型安裝	23
5.1.2 自訂安裝	25
5.2 啓動服務	28
6 執行管理服務安裝	29
6.1 安裝步驟	30
6.1.1 典型安裝	31
6.1.2 自訂安裝	35
6.2 啓動服務	38
7 執行管理主控台安裝	39
7.1 安裝步驟	39
7.1.1 典型安裝	40
7.1.2 自訂安裝	40
7.2 啓動主控台	42
7.2.1 新增 eDirectory 服務	43
7.2.2 設定管理主控台的許可設定	45
7.2.3 發行規則	48
7.3 安裝 USB Reader	48

8	執行用戶端位置保證服務安裝	49
8.1	安裝步驟	50
8.2	CLAS 容錯移轉安裝	50
8.3	將公用金鑰傳送至管理服務	50
9	Endpoint Security Client 3.5 安裝	53
9.1	基本 Endpoint Security Client 3.5 安裝	53
9.2	MSI 安裝	54
9.2.1	指令行變數	57
9.2.2	與 MSI 套件一同配送規則	59
9.2.3	從 MSI 進行 Endpoint Security Client 3.5 的使用者安裝	59
9.3	執行 Endpoint Security Client 3.5	59
10	ZENworks Endpoint Security Client 4.0 安裝	61
10.1	基本 Endpoint Security Client 4.0 安裝	61
10.2	MSI 安裝	64
10.2.1	使用主安裝程式	64
10.2.2	使用 Setup.exe 檔案	64
10.2.3	完成安裝	65
10.2.4	指令行變數	66
10.2.5	與 MSI 套件一同配送規則	67
10.3	執行 Endpoint Security Client 4.0	67
10.4	Endpoint Security Client 4.0 中不支援的功能	67
11	ZENworks Endpoint Security Management 安裝	69
11.1	不受管理的 Endpoint Security Client 安裝	69
11.2	獨立管理主控台	69
11.3	配送不受管理的規則	70
A	文件更新	71
A.1	2009 年 1 月 5 日	71

關於本指南

本《Novell® ZENworks® Endpoint Security Management 安裝指南》提供 ZENworks Endpoint Security Management 元件的完整安裝指示，並協助管理員準備該元件並加以執行。

本指南中的資訊是以下列方式編排：

- ◆ 第 1 章 「ZENworks Endpoint Security Management 綜覽」 (第 9 頁)
- ◆ 第 2 章 「安裝 ZENworks Endpoint Security Management」 (第 13 頁)
- ◆ 第 3 章 「執行單一伺服器安裝」 (第 17 頁)
- ◆ 第 4 章 「執行多重伺服器安裝」 (第 19 頁)
- ◆ 第 5 章 「執行規則配送服務安裝」 (第 21 頁)
- ◆ 第 6 章 「執行管理服務安裝」 (第 29 頁)
- ◆ 第 7 章 「執行管理主控台安裝」 (第 39 頁)
- ◆ 第 8 章 「執行用戶端位置保證服務安裝」 (第 49 頁)
- ◆ 第 9 章 「Endpoint Security Client 3.5 安裝」 (第 53 頁)
- ◆ 第 10 章 「ZENworks Endpoint Security Client 4.0 安裝」 (第 61 頁)
- ◆ 第 11 章 「ZENworks Endpoint Security Management 安裝」 (第 69 頁)

使用對象

本指南是針對 ZENworks Endpoint Security Management 管理員所撰寫。

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 \(http://www.novell.com/documentation/feedback.html\)](http://www.novell.com/documentation/feedback.html)，寫下您的意見。

其他文件

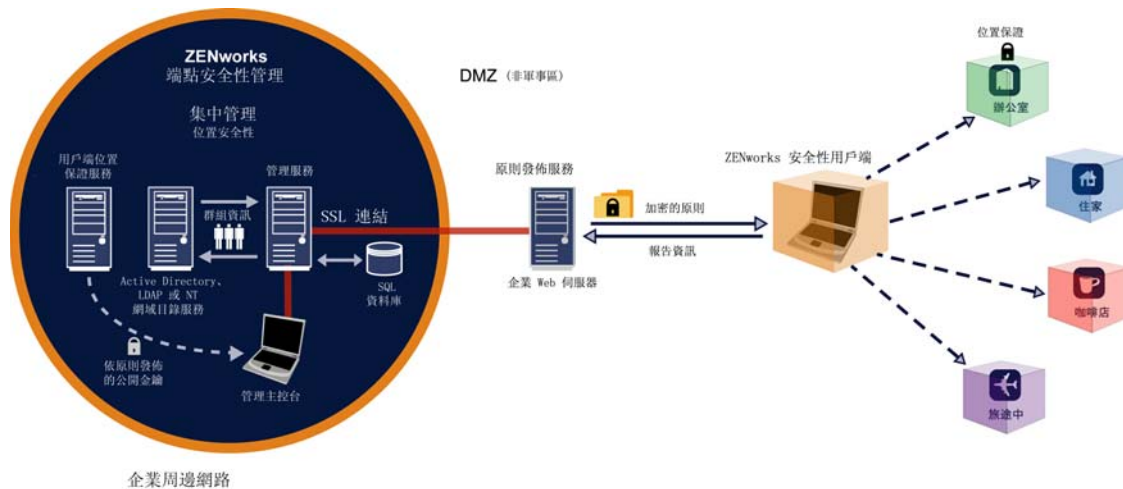
此外，您還可以透過 ZENworks Endpoint Security Management 的其他支援文件 (包括 PDF 與 HTML 格式)，來瞭解本產品並加以實作。如需更多文件，請參閱 [ZENworks Endpoint Security Management 3.5 文件網站 \(http://www.novell.com/documentation/zesm35\)](http://www.novell.com/documentation/zesm35)。

ZENworks Endpoint Security Management 綜覽

1

Novell® ZENworks® Endpoint Security Management 包括五個高階的功能元件：「規則配送服務」、「管理服務」、「管理主控台」、「用戶端位置保證服務」及 Endpoint Security Client。下圖會以結構方式顯示這些元件：

圖 1-1 ZENworks Endpoint Security Management 架構



Endpoint Security Client 負責在端點系統上強制執行配送的安全性規則。在所有的企業電腦上安裝 Endpoint Security Client 後，這些端點現在便可連接至公司周邊外部並依然保持其安全性，而周邊內部的端點則可在周邊防火牆內獲得額外的安全性檢查。

系統會個別安裝每個中央管理元件 (除了單一伺服器安裝以外)。如需詳細資料，請參閱 [第 3 章「執行單一伺服器安裝」\(第 17 頁\)](#)。

以下的元件會安裝在公司周邊內部的安全伺服器中：

- ◆ **規則配送服務**：負責將安全性規則配送給 Endpoint Security Client，並從 Endpoint Security Client 取回報告資料。「規則配送服務」可部署於 DMZ 中 (於企業防火牆外部)，以確保行動端點的規則會定期更新。
- ◆ **管理服務**：負責使用者規則指定和元件驗證，報告 ZENworks Endpoint Security Management 報告的資料取回、建立及散佈，以及安全性規則的建立和儲存。
- ◆ **管理主控台**：這是可見的使用者介面，可直接於代管「管理員服務」的伺服器上執行，或者在位於公司防火牆內部且連接至「管理服務」伺服器的工作站上執行。「管理主控台」可用於設定「管理服務」，以及建立和管理使用者與群組安全性規則。您可以使用管理主控台來建立、複製、編輯、散佈和刪除規則。
- ◆ **用戶端位置保證服務**：可提供密碼保證，以保證安裝 Endpoint Security Client 的設備確實位於定義的位置，如同其他現有網路環境參數所表示的。

1.1 系統需求

伺服器系統需求	端點 (用戶端) 系統需求
作業系統： Microsoft Windows Server 2000 SP4 Microsoft Windows 2000 Advanced Server SP4 Windows 2003 Server	作業系統： Windows XP SP1 Windows XP SP2 Windows 2000 SP4 Windows Vista SP1 (32 位元) Windows Server 2008 (32 位元)
處理器： 3.0 GHz Pentium 4 HT (或更高速度) 至少要有 756 MB RAM (建議使用 1 GB+)	處理器： 600MHz Pentium 3 (或更高速度) 至少要有 128 MB RAM (建議使用 256 MB 或以上)
磁碟空間： 500 MB：不含本機 Microsoft SQL 資料庫 5 GB：包含本機 MS SQL 資料庫 (建議使用 SCSI)	磁碟空間： 必要空間為 5 MB，建議要有額外的 5 MB，以用於報告資料
需要的軟體： 支援的 RDBMS (SQL Server Standard、SQL Server Enterprise、Microsoft SQL Server 2000 SP4、SQL 2005) Microsoft Internet Information Services (針對 SSL 進行設定) 支援的目錄服務 (eDirectory™ 或 Active Directory) .NET framework 3.5 (僅適用於伺服器與管理主控台)	需要的軟體： Windows 3.1 Installer 所有的 Windows 更新程式都必須是目前的版本
獨立管理主控台： 支援的 RDBMS (SQL Server Standard、SQL Server Enterprise、Microsoft SQL Server 2000 SP4、SQL 2005、SQL Express)	

「規則配送」、「管理」及「用戶端位置保證」服務需要啓用一個「本機」ASP.NET 2.0 帳戶。如果停用此帳戶，服務將不會正確運作。

1.2 關於 ZENworks Endpoint Security Management 手冊

ZENworks Endpoint Security Management 手冊可為本產品的使用者提供三個層級的指導。

- ◆ 《ESM 安裝指南》：本指南提供 ZENworks Endpoint Security Management 元件的完整安裝指示，並協助管理員準備以及執行這些元件。這是您現在閱讀的指南。

- ◆ 《ZENworks Endpoint Security Management 管理指南》：本指南的適用對象為需要管理服務、建立企業的安全性規則、產生和分析報告資料，以及為使用者提供疑難排解的ZENworks Endpoint Security Management 管理員。本手冊中提供完成這些任務的指示。
- ◆ 《ZENworks Endpoint Security Client 3.5 使用者指南》：本指南可指導使用者進行Endpoint Security Client 的操作。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。

安裝 ZENworks Endpoint Security Management

2

以下各節包含與安裝 Novell® ZENworks® Endpoint Security Management 有關的詳細資訊：

- 「安裝前的資訊」(第 13 頁)
- 「安裝套件」(第 13 頁)
- 「安裝選項」(第 13 頁)
- 「安裝順序」(第 14 頁)
- 「安裝 ZENworks Endpoint Security Management 之前」(第 14 頁)

2.1 安裝前的資訊

ZENworks Endpoint Security Management 安裝軟體的實體必須受到保護，以避免任何企圖竄改或未授權的使用。管理員也必須檢閱安裝前以及安裝指南以確保 ZENworks Endpoint Security Management 系統的運作不會中斷，或者因為硬體保護不足而受到損害。

安裝此軟體的管理員必須是伺服器 and 領域的主要管理員。若您使用企業 SSL 證書，則必須使用相同的使用者名稱來建立 SSL 根安全性證書。

2.2 安裝套件

若是從 DVD 進行安裝，則會啟動主安裝程式 (Master Installer)，它會利用簡易的安裝介面以引導 ZENworks Endpoint Security Management 管理員執行安裝程序。將安裝 DVD 載入每台機器以存取主安裝程式，並安裝需要的元件。

2.2.1 關於主安裝程式

在啟動時，主安裝程式將顯示兩種功能表選項：「產品」和「文件」。

「產品」連結將開啓安裝功能表。此畫面上的功能表項目將為每個元件啟動指定的安裝程式。對於 Endpoint Security Client 3.5 或 Endpoint Security Client 4.0，您可以使用額外選項，以「管理員模式」啟動安裝，這有助於 ZENworks Endpoint Security Management 管理員建立 MSI 套件，以方便配送 (請參閱第 9.2 章「MSI 安裝」(第 54 頁))。

如需關於 ZENworks Endpoint Security Management 元件的完整操作資訊，請參閱《ZENworks Endpoint Security Management 管理指南》，該指南可從「文件」連結獲得。

2.3 安裝選項

您可以使用「單一伺服器」或「多重伺服器」安裝模式來安裝 ZENworks Endpoint Security Management 後端元件。「單一伺服器」安裝適用於不需要進行定期規則更新的小型部署。「多重伺服器」安裝適用於需要進行定期規則更新的大型部署。請詢問 Novell 專業服務 (Novell Professional Services) 以判斷您適用哪一種安裝類型。

Endpoint Security Client 可在未連接「規則配送服務」的情況下運作 (如有需要)。您也可以基於評估目的，選擇性地安裝「獨立管理主控台」。您可以在 [第 11 章「ZENworks Endpoint Security Management 安裝」\(第 69 頁\)](#) 中找到「不受管理」操作模式的安裝敘述。

2.4 安裝順序

您必須按照以下順序安裝 ZENworks Endpoint Security Management：

1. 單一伺服器安裝或多重伺服器安裝
 - ◆ 規則配送服務
 - ◆ 管理服務
2. 管理主控台
3. 用戶端位置保證服務
4. Endpoint Security Client 3.5 或 Endpoint Security Client 4.0

2.5 安裝 ZENworks Endpoint Security Management 之前

在開始安裝之前，ZENworks Endpoint Security Management 管理員必須考慮一些問題：

使用者將如何接收 ZENworks Endpoint Security Management 安全性規則？

規則配送的選項圍繞在使用者是否可隨處接收規則更新 (即使在中央網路之外)，以及使用者是否僅能在安全網路內 (或透過 VPN 連接時) 接收更新。針對必須經常更新其 ZENworks Endpoint Security Management 安全性規則的組織，我們建議使用多重伺服器安裝，以將「規則配送服務」置於 DMZ 以外的 Web 伺服器上。

您適合哪一種伺服器部署？

如果您的組織僅擁有幾部伺服器，您可能只需要單一伺服器安裝。如果問題不在於伺服器的可用性，您可能需要考慮用戶端部署的大小，以及在防火牆之外操作的使用者數量。

您可使用哪一種 SQL 伺服器部署？

ZENworks Endpoint Security Management 會在安裝時建立三個 SQL 資料庫。如果您只進行小型部署，可以將單一 SQL 資料庫或伺服器端資料庫安裝在「規則配送」和「管理服務」的伺服器上。若要進行大型部署，必須使用個別的 SQL 資料庫伺服器從「規則配送」和「管理服務」接收資料。僅允許以下的 RDBMS 類型：

- ◆ SQL Server Standard
- ◆ SQL Server Enterprise
- ◆ Microsoft SQL Server 2000 SP4

如果是已命名的執行個體，則伺服器必須使用以下方式組態：

```
Provider=sqloledb
```

```
Data Source=ServerName\InstanceName (此定義類型對於 ZENworks Endpoint Security Management 的安裝來說是必要的)
```

Initial Catalog=DatabaseName

User Id=Username

Password=Password

將 SQL 設為「混合」模式。

安裝期間的使用者名稱和密碼不能是領域使用者；它必須是擁有 SysAdmin 權限的 SQL 使用者。

您要使用現有的證書來建立 SSL 通訊嗎？或使用 Novell 自我簽署證書？

針對災難復原和容錯移轉的設計，您必須使用企業 SSL 證書，或另外發行的「證書權限」(VeriSign、GeoTrust、Thawte 等) 進行 ZENworks Endpoint Security Management 的完整部署。當您使用自己的證書時，系統會將 Web 服務證書和根 CA 建立在指定為「規則配送服務」的機器上，然後將其配送至適當的機器。若要建立企業證書權限 (Enterprise Certificate Authority)，請參閱 Microsoft 網站中的按步驟指示，以安全地設定證書權限。

如需進行試用或小型部署 (少於 100 個使用者)，您可以使用 ZENworks Endpoint Security Management 自我簽署證書。執行典型安裝時，Novell SSL 證書將會安裝在伺服器上。

如何部署 Endpoint Security Client？

您可以將 Endpoint Security Client 軟體分別部署在每個端點上，或透過 MSI 推送 (Push) 進行部署。您可以在 [第 9.2 章「MSI 安裝」](#) ([第 54 頁](#)) 中找到與建立 MSI 套件有關的指示。

您的規則要以機器為基礎，還是要以使用者為基礎？

您可以將規則配送至單一機器中，每個登入該機器的使用者都會接收相同的規則，或者您也可以個別為使用者或群組設定規則。

每種安裝都會有數個先決條件。我們建議您在為任何元件執行安裝之前，都必須完成每個先決條件的檢查清單。請檢閱以下頁面中的清單：

- ◆ [第 3 章「執行單一伺服器安裝」](#) ([第 17 頁](#))
- ◆ [第 5 章「執行規則配送服務安裝」](#) ([第 21 頁](#))
- ◆ [第 6 章「執行管理服務安裝」](#) ([第 29 頁](#))
- ◆ [第 7 章「執行管理主控台安裝」](#) ([第 39 頁](#))
- ◆ [第 8 章「執行用戶端位置保證服務安裝」](#) ([第 49 頁](#))
- ◆ [第 9 章「Endpoint Security Client 3.5 安裝」](#) ([第 53 頁](#))

執行單一伺服器安裝

ZENworks® Endpoint Security Management 單一伺服器安裝 (Single Server Installation, SSI) 可允許「規則配送服務」和「管理服務」共存於相同的伺服器中，若未使用此安裝選項時則無法共存。基於安全性考量，伺服器必須部署在防火牆內，使用者必須位於公司架構內或透過 VPN 連接時才能接收規則更新。

基於安全性和功能性的原因，您無法將「單一伺服器安裝」部署在主要領域控制器 (PDC) 上。

附註：我們建議您在設定 (強化) SSI 伺服器時，停用所有的應用程式、服務、帳戶以及伺服器功能性所不需要的其他選項。執行此作業的步驟將視本機環境而定，因此無法預先說明。我們建議管理員參閱 [Microsoft Technet 安全性網頁 \(http://www.microsoft.com/technet/security/default.mspx\)](http://www.microsoft.com/technet/security/default.mspx) 中適合的區段。《ZENworks Endpoint Security Management 管理指南》還提供其他的存取控制建議。

若要保護僅存取受信任的機器，可將虛擬目錄和 IIS 設定為具有 ACL。請參考以下文章：

- ◆ [Granting and Denying Access to Computers \(授予和拒絕電腦存取 \) \(http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx\)](http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx)
- ◆ [Restrict Site Access by IP Address or Domain Name \(透過 IP 位址和領域名稱限制網站存取 \) \(http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066\)](http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)
- ◆ [IIS FAQ: 2000 IP address and domain name restrictions \(IIS FAQ：2000 個 IP 位址和領域名稱限制\) \(http://www.iisfaq.com/default.aspx?View=A136&P=109\)](http://www.iisfaq.com/default.aspx?View=A136&P=109)
- ◆ [Working With IIS Packet Filtering \(使用 IIS 封包篩選 \) \(http://www.15seconds.com/issue/011227.htm\)](http://www.15seconds.com/issue/011227.htm)

基於安全性考量，我們強烈建議您在任何的 IIS 安裝中移除以下預設資料夾：

- ◆ IISHelp
- ◆ IISAdmin
- ◆ Scripts
- ◆ Printers

我們也建議您使用 [microsoft.com \(http://www.microsoft.com/technet/security/tools/locktool.mspx\)](http://www.microsoft.com/technet/security/tools/locktool.mspx) 提供的 IIS Lockdown Tool 2.1。

2.1 版是由各大適用 IIS 相關 Microsoft 產品的範本所驅動。請選取最符合此伺服器角色的範本。如果您不確定，建議您使用動態 Web 伺服器範本。

在開始進行安裝「之前」，請確定已完成以下必要條件：

- 確認可存取已支援的目錄服務 (eDirectory™、Active Directory 或 NT Domains)。只有當「單一伺服器服務」安裝在 Microsoft Windows 2000 Advanced Server (SP4) 上時，才能支援 NT 領域。
- 如果您使用 eDirectory 服務進行部署，請確定 Novell Client™ 已安裝在伺服器上，並可正確驗證至 eDirectory。請建立不會變更的帳戶密碼，可以供「管理主控台」驗證時使用 (請參閱「[新增 eDirectory 服務](#)」(第 43 頁))。

- ❑ 對於 Endpoint Security Client 至「單一伺服器」的伺服器名稱解析，請驗證目標電腦（已安裝 Endpoint Security Client）可 Ping SSI 伺服器名稱。若不成功，則您必須在繼續進行安裝之前先將問題解決。（將 SSI 伺服器名稱變更為 FQDN/NETBIOS、將 AD 變更為使用 FQDN/NETBIOS、變更 DNS 組態、修改目標電腦上的本地主機檔案以包含正確的 MS 資訊等）。
- ❑ 啟用或安裝 Microsoft Internet Information Services (IIS)，並將其設定為接受保全插槽層 (SSL) 證書。

重要：請勿在「安全通訊」頁面選取「必須使用安全通道 (SSL)」核取方塊（在「Microsoft 電腦管理」公用程式中，展開「服務和應用程式」>展開「Internet Information Services (IIS) 管理員」>展開「網站」>以滑鼠右鍵按一下「預設的網站」>按一下「內容」>按一下「目錄安全設定」索引標籤>按一下「安全通訊」群組方塊中的「編輯」按鈕）。選取此選項會中斷 ZENworks Endpoint Security Management 伺服器與端點上之 ZENworks Endpoint Security 用戶端之間的通訊。

- ❑ 如果您使用自己的 SSL 證書，請確定已將 Web 服務證書和根 CA 載入機器，且在之前步驟中驗證的伺服器名稱（無論是 NETBIOS 或 FQDN）符合在 IIS 中設定之證書的「發給」值。
- ❑ 如果您使用自己的證書，或者已安裝 Novell 自我簽署證書，您也可以已在已安裝 Endpoint Security Client 的機器中嘗試使用以下 URL 來驗證 SSL：`https://SSI_SERVER_NAME/AuthenticationServer/UserService.aspx`（其中 SSI_SERVER_NAME 為伺服器名稱）。這將會傳回有效的資料 (html 頁面)，而不是證書警告。任何的證書警告都必須在安裝前解決，除非您選擇使用 Novell 自我簽署證書。
- ❑ 確定可存取支援的 RDBMS (Microsoft SQL Server 2000 SP4、SQL Server Standard、SQL Server Enterprise)。將資料庫設為「混合」模式。

3.1 安裝步驟

在主安裝程式功能表中選取「單一伺服器安裝」。此安裝會結合「規則配送服務」和「管理服務」的安裝。如需詳細資訊，請參閱第 5 章「執行規則配送服務安裝」（第 21 頁）與第 6 章「執行管理服務安裝」（第 29 頁）。

如其他服務之個別安裝一般，「典型」設定將安裝服務的預設值以及 Novell 自我簽署的 SSL 證書。「自訂安裝」允許管理員決定目錄路徑，並允許使用企業所有的憑證機構。

3.2 啟動服務

合併的「配送服務」及「管理服務」會在安裝後立即啟動，而不需將伺服器重新開機。您可以使用管理主控台內的「組態」功能來管理「配送」與「管理服務」。如需詳細資訊，請參閱《ZENworks Endpoint Security Management 管理指南》。

在完成安裝後，您也可以將「管理主控台」和「用戶端位置保證服務」安裝在此伺服器上。若要將管理主控台安裝在個別機器上，請將「ZENworks Endpoint Security Management 安裝程式檔案」資料夾複製到指定的管理主控台機器以完成安裝。

請繼續進行第 5 章「執行規則配送服務安裝」（第 21 頁）。

執行多重伺服器安裝

當您進行大型部署時，或者必須將「規則配送服務」置於公司防火牆之外，以確保周邊外的使用者能收到定期規則更新時，我們建議您進行「多重伺服器」安裝。多重伺服器安裝必須至少在兩個個別的伺服器上進行。如果您嘗試將個別的「規則配送服務」和「管理服務」安裝在相同的伺服器上，安裝將會失敗。如需詳細資訊，請參閱第 3 章「執行單一伺服器安裝」(第 17 頁)進行單一伺服器安裝。

在開始進行「多重伺服器」安裝時，必須將「規則配送服務」安裝在公司防火牆之外或之內的安全伺服器上。若需要更多的資訊，請參閱第 5 章「執行規則配送服務安裝」(第 21 頁)。

完成安裝「規則配送服務」後，請接著安裝「管理服務」。若需要更多的資訊，請參閱第 6 章「執行管理服務安裝」(第 29 頁)。

我們建議您也將「管理主控台」安裝在此伺服器上。如需詳細資訊，請參閱第 7 章「執行管理主控台安裝」(第 39 頁)。

請繼續進行第 5 章「執行規則配送服務安裝」(第 21 頁)。

執行規則配送服務安裝

您的使用者無論是在網路內，或者位於 DMZ 外部，都必須能夠連接代管「ZENworks® Endpoint Security Management 規則配送服務」的主機伺服器。在進行安裝前，請確定您已將必要的軟體安裝在伺服器中（請參閱「系統需求」（第 10 頁））。在選取伺服器之後，請注意伺服器名稱，包括 NETBIOS 和完整網域名稱 (Fully Qualified Domain Name, FQDN)。

基於安全性和功能性的原因，您無法將「規則配送服務」部署在主要領域控制器 (PDC) 上。

附註：我們建議您在設定 (強化) SSI 伺服器時，停用所有的應用程式、服務、帳戶以及伺服器功能性所不需要的其他選項。執行此作業的步驟將視本機環境而定，因此無法預先說明。我們建議管理員參閱 [Microsoft Technet 安全性網頁 \(http://www.microsoft.com/technet/security/default.mspx\)](http://www.microsoft.com/technet/security/default.mspx) 中適合的區段。《ZENworks Endpoint Security Management 管理指南》還提供其他的存取控制建議。

若要保護僅存取受信任的機器，可將虛擬目錄和 IIS 設定為具有 ACL。請參考以下文章：

- ◆ [Granting and Denying Access to Computers \(授予和拒絕電腦存取 \) \(http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx\)](http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx)
- ◆ [Restrict Site Access by IP Address or Domain Name \(透過 IP 位址和領域名稱限制網站存取 \) \(http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066\)](http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)
- ◆ [IIS FAQ: 2000 IP address and domain name restrictions \(IIS FAQ：2000 個 IP 位址和領域名稱限制\) \(http://www.iisfaq.com/default.aspx?View=A136&P=109\)](http://www.iisfaq.com/default.aspx?View=A136&P=109)
- ◆ [Working With IIS Packet Filtering \(使用 IIS 封包篩選 \) \(http://www.15seconds.com/issue/011227.htm\)](http://www.15seconds.com/issue/011227.htm)

基於安全性考量，我們強烈建議您在任何的 IIS 安裝中移除以下預設資料夾：

- ◆ IISHelp
- ◆ IISAdmin
- ◆ Scripts
- ◆ Printers

我們也建議您使用 [microsoft.com \(http://www.microsoft.com/technet/security/tools/locktool.mspx\)](http://www.microsoft.com/technet/security/tools/locktool.mspx) 提供的 IIS Lockdown Tool 2.1。

2.1 版是由各大適用 IIS 相關 Microsoft 產品的範本所驅動。請選取最符合此伺服器角色的範本。如果您不確定，建議您使用動態 Web 伺服器範本。

在開始進行安裝之前，請檢查以下必要條件：

- ❑ 確定「管理服務」(MS) 至「規則配送服務」(DS) 的伺服器名稱解析：確定驗證目標電腦 (已安裝 MS) 可 Ping DS 伺服器名稱 (若是在網路防火牆內部設定 DS 則為 NETBIOS，若在 DMZ 外部安裝則為 FQDN)。
- ❑ 若能成功，則這就是在安裝中要輸入的伺服器名稱。若不成功，則您必須在繼續進行安裝之前先將問題解決。

- ❑ 確定 Endpoint Security Client 至 DS 的伺服器名稱解析：驗證端點用戶端 (已安裝 Endpoint Security Client) 可 Ping 上述使用的相同 DS 伺服器名稱。若不成功，則您必須在繼續進行安裝之前先將問題解決。
- ❑ 啓用或安裝 Microsoft Internet Information Services (IIS)，確定您已啓用 ASP.NET，並將其設定為接受保全插槽層 (SSL) 證書。

重要：請勿在「安全通訊」頁面選取「必須使用安全通道 (SSL)」核取方塊 (在「Microsoft 電腦管理」公用程式中，展開「服務和應用程式」>展開「Internet Information Services (IIS) 管理員」>展開「網站」>以滑鼠右鍵按一下「預設的網站」>按一下「內容」>按一下「目錄安全設定」索引標籤>按一下「安全通訊」群組方塊中的「編輯」按鈕)。選取此選項會中斷 ZENworks Endpoint Security Management 伺服器與端點上之 ZENworks Endpoint Security 用戶端之間的通訊。

- ❑ 如果您使用自己的 SSL 證書，請確定您已將 Web 服務證書載入機器，且在之前步驟中驗證的伺服器名稱 (無論是 NETBIOS 或 FQDN) 符合在 IIS 中設定的證書 *Issued to* (簽發給) 值。
- ❑ 如果您使用自己的 SSL 證書，請驗證從 MS 伺服器至 DS 伺服器的 SSL：開啓「管理服務」上的 Web 瀏覽器，並輸入以下 URL：https://DSNAME (其中 DSNAME 為 DS 的伺服器名稱)。這將會傳回有效的資料 (可能是 Page under Construction (網頁正在建立中))，而不是證書警告。任何的證書警告都必須在安裝前解決，除非您選擇使用 Novell 自我簽署證書。
- ❑ 請確認可存取受支援的 RDBMS (Microsoft SQL Server 4 SP2005、SQL Server Standard、SQL Server Enterprise、SQL Server 2005)。將資料庫設為「混合」模式。此資料庫可由「管理服務」伺服器，或者是經由企業防火牆保全之共享伺服器所代管。

5.1 安裝步驟

按一下「安裝介面」功能表中的「規則配送服務安裝」。「規則配送服務」的安裝就會開始。

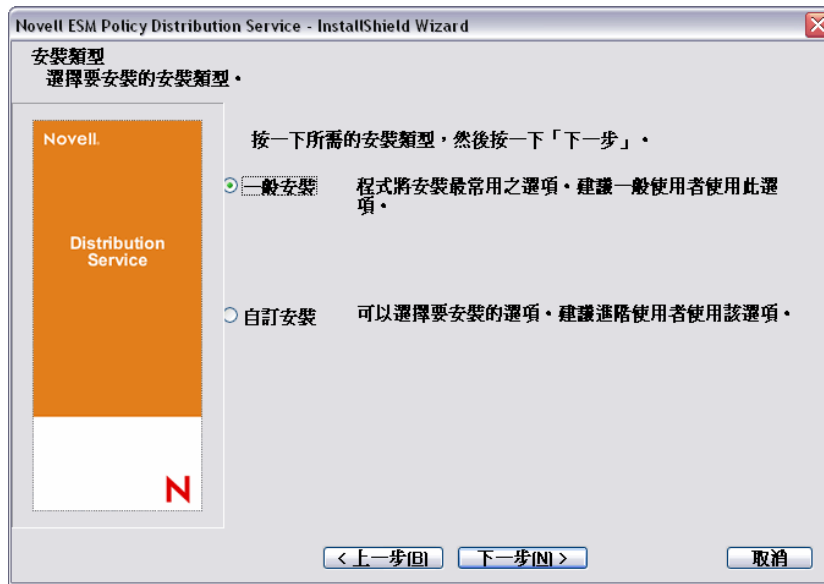
在啓動時，安裝程式會驗證所有必要的軟體是否皆位於伺服器中。若缺少任何軟體，安裝程式會在進入「歡迎畫面」之前自動安裝這些軟體 (必須接受附加軟體的授權合約)。若您需要安裝 Microsoft Data Access Components (MDAC) 2.8，則必須在安裝程序之後，將伺服器重新開機以繼續安裝 ZENworks Endpoint Security Management。若使用 Windows 2003 Server，則 ASP.NET 2.0 將設定為由安裝程式執行。

「規則配送服務」安裝開始後，請執行以下步驟：

附註：以下步驟將列出管理員完成安裝程序所需執行的動作。除非是成功完成安裝所需的特定動作或資訊，否則內部程序將會在整個安裝程序中顯示，而不會在此列出。

- 1 按一下「歡迎」畫面中的「下一步」以繼續。
- 2 接受授權合約，然後按一下「下一步」。
- 3 選取「典型」或「自訂」安裝。

圖 5-1 選取「典型」或「自訂」安裝



以下說明兩種安裝方式：

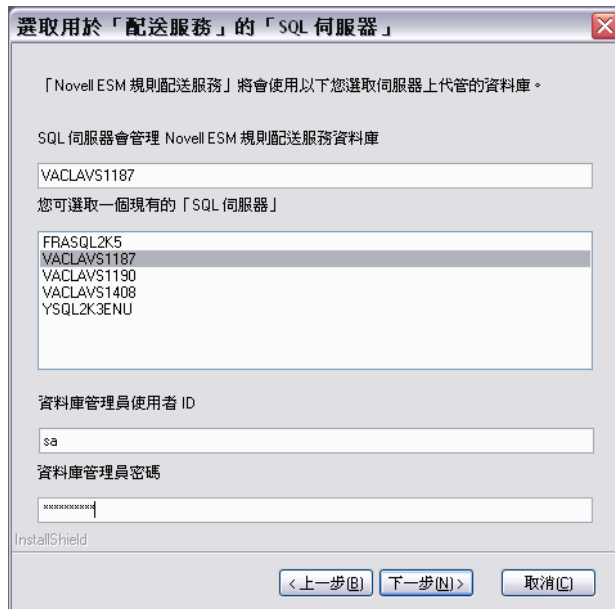
- 「典型安裝」(第 23 頁)
- 「自訂安裝」(第 25 頁)

5.1.1 典型安裝

典型安裝會將「規則配送服務」軟體檔案置於預設目錄中：`\Program Files\Novell\ESM Policy Distribution Service`。SQL 資料庫名稱將指定為 `STDSDB`。三種 SQL 資料庫檔案(資料、索引和記錄)將置於：`\Program Files\Microsoft SQL Server\mssql\Data`。

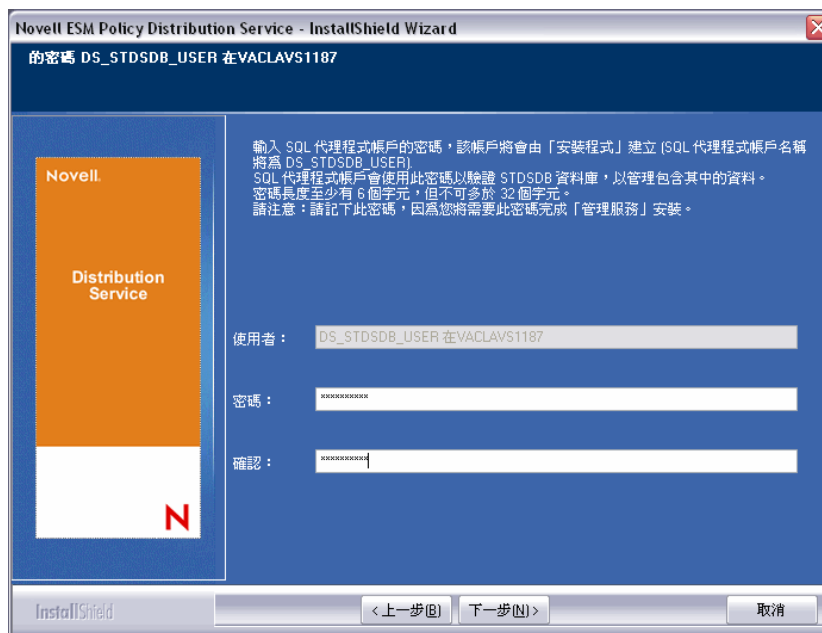
- 1 安裝程序中將會建立 Novell SSL 證書。如果您想要使用自己的 SSL 證書，請使用「自訂安裝」。這些證書必須配送給所有的使用者。
- 2 安裝程式將會偵測機器和網路上可用的 SQL 資料庫。選取「規則配送服務」的安全 SQL 資料庫，並輸入資料庫管理員名稱和密碼(如果密碼為零字元，安裝程式將會發出潛在的安全性問題警告)。使用者名稱和密碼不能是領域使用者；它必須是擁有 SysAdmin 權限的 SQL 使用者。

圖 5-2 選取 SQL 伺服器



- 3 指定「規則配送服務」代辦的密碼。這是服務登入其 SQL 資料庫時使用的使用者名稱和密碼。

圖 5-3 「配送服務」SQL 密碼



- 4 指定「規則配送服務」領域名稱。若伺服器的位置是在公司防火牆之外，則該名稱必須是完全合格的領域名稱。否則只需要伺服器的 NETBIOS 名稱。

圖 5-4 輸入「規則配送服務」領域名稱。



- 5 在「複製檔案」畫面中按一下「下一步」以開始安裝。
- 6 系統會在安裝目錄中建立一個 ESM Setup Files 資料夾。其中包含「管理服務」所需要的一個安裝 ID 檔案和 ESM-DS.cer 檔案 (Novell 自我簽署 SSL 證書)。您可以透過網路共享或將檔案儲存至磁碟片或隨身碟，然後以手動方式將其載入伺服器安裝目錄中，將該檔案複製至指定為「管理服務」主機的機器中。
- 7 現在您已安裝「規則配送服務」，請按一下「完成」關閉安裝程式，並啟動效能監看。

5.1.2 自訂安裝

自訂安裝將顯示在典型安裝中使用的預設值，並允許管理員指定或瀏覽不同的目錄，然後將軟體檔案置於該目錄中。

管理員可選擇安裝 Novell 自我簽署 SSL 證書，或使用他們自己的證書。

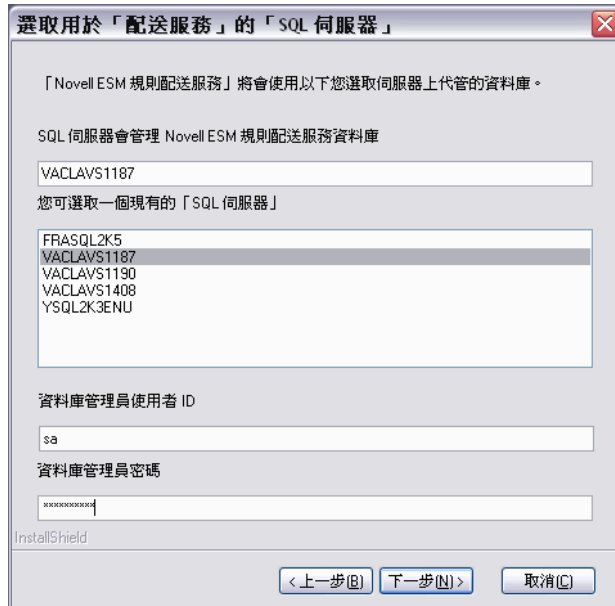
- 1 您需要 SSL 證書以保護「規則配送服務」和「管理服務」之間，以及 DS 和所有 Novell Security Clients 之間的通訊。如果您已經擁有證書權限，請按一下「請使用 IIS 設定的現有證書」。如果您需要證書，請按一下「允許 Novell 建立、安裝並使用自身的自我簽署根證書」。安裝程式將建立證書和簽署權限。無論證書的類型為何，這些證書都必須配送給所有的使用者。

圖 5-5 設定託管根部



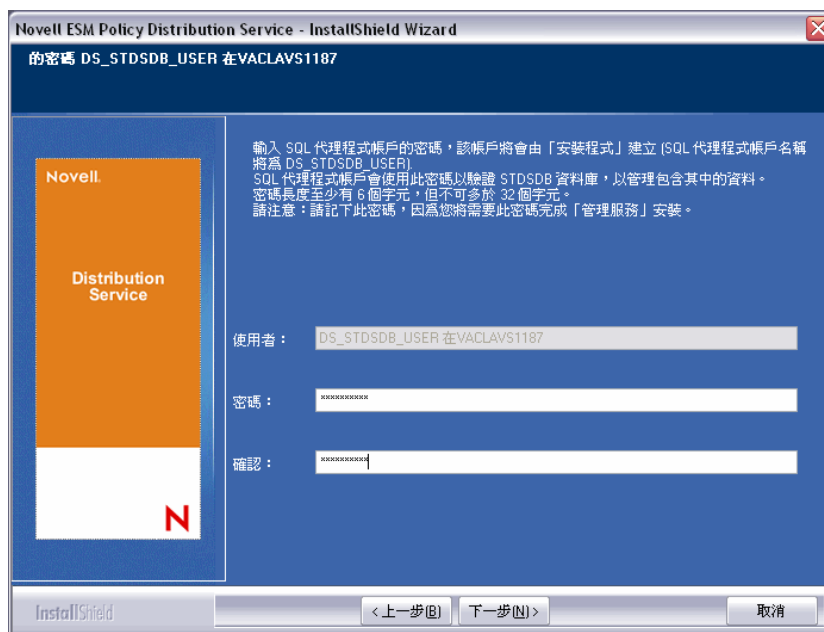
- 2 安裝程式將會偵測機器和網路上可用的 SQL 資料庫。選取「規則配送服務」的安全 SQL 資料庫，並輸入資料庫管理員名稱和密碼 (如果密碼為零字元，安裝程式將會發出潛在的安全性問題警告)。使用者名稱和密碼不能是領域使用者；它必須是擁有 SysAdmin 權限的 SQL 使用者。

圖 5-6 選取 SQL 伺服器



- 3 設定資料庫名稱 (預設輸入為 STDSDB)。
- 4 指定「規則配送服務」代辦的密碼。這是服務登入其 SQL 資料庫時使用的使用者名稱和密碼。

圖 5-7 「配送服務」 SQL 密碼



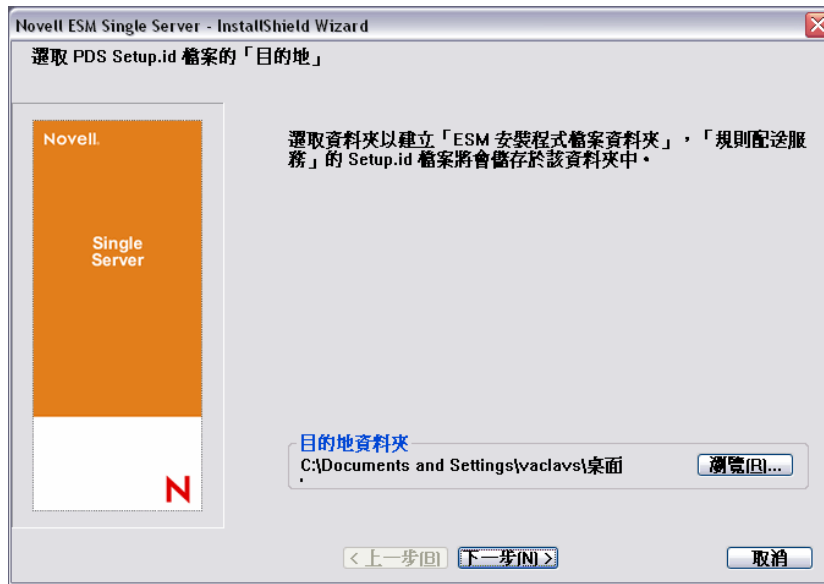
- 5 指定「規則配送服務」領域名稱。若伺服器的位置是在公司防火牆之外，則該名稱必須是完全合格的領域名稱。否則只需要伺服器的 NETBIOS 名稱。

圖 5-8 輸入「規則配送服務」領域名稱。



- 6 在「複製檔案」畫面中按一下「下一步」以開始安裝。
- 7 指定資料、索引和記錄檔的檔案路徑。
- 8 系統會在安裝目錄中建立一個 ESM Setup Files 資料夾。其中包含「管理服務」所需要的一個安裝 ID 檔案和 ESM-DS.cer 檔案 (如果先前已選取，則是 Novell 自我簽署 SSL 證書)。使用「瀏覽」指定檔案將儲存在伺服器上的位置 (預設值 = 安裝目錄)。

圖 5-9 儲存設定檔案



- 9 如果您選擇使用企業 SSL 證書，請將該檔案的複製至 ESM Setup Files 檔案資料夾。
- 10 您可以透過網路共享或將檔案儲存至磁碟或隨身碟，然後以手動方式將其載入伺服器安裝目錄中，將整個 ESM Setup Files 檔案直接複製至指定為「管理服務」主機的機器中。
- 11 現在您已安裝「規則配送服務」，請按一下「完成」關閉安裝程式，並啟動效能監看。

5.2 啟動服務

「規則配送服務」會在安裝後立即啟動，而不需將伺服器重新開機。您可以使用「管理主控台」中的「組態」工具來調整「配送服務」的上載時間。如需詳細資訊，請參閱《ZENworks Endpoint Security Management 管理指南》。

請繼續進行第 6 章「執行管理服務安裝」(第 29 頁)。

執行管理服務安裝

「管理服務」必須安裝在防火牆後的安全伺服器上，且無法與「規則配送服務」使用相同的伺服器（「單一伺服器」安裝則例外，請參閱 [第 3 章「執行單一伺服器安裝」](#)（第 17 頁））。基於安全性考量，「管理服務」不應安裝在網路防火牆之外。在選取伺服器之後，請注意伺服器名稱，包括 NETBIOS 和完整網域名稱 (FQDN)。基於安全性和功能性的原因，您無法將「管理服務」部署在主要領域控制器 (PDC) 上。

附註：我們建議您在設定（強化）SSI 伺服器時，停用所有的應用程式、服務、帳戶以及伺服器功能性所不需要的其他選項。執行此作業的步驟將視本機環境而定，因此無法預先說明。我們建議管理員參閱 [Microsoft Technet 安全性網頁](http://www.microsoft.com/technet/security/default.mspx) (<http://www.microsoft.com/technet/security/default.mspx>) 中適合的區段。《ZENworks Endpoint Security Management 管理指南》還提供其他的存取控制建議。

若要保護僅存取受信任的機器，可將虛擬目錄和 IIS 設定為具有 ACL。請參考以下文章：

- ◆ [Granting and Denying Access to Computers \(授予和拒絕電腦存取 \)](http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx) (<http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx>)
- ◆ [Restrict Site Access by IP Address or Domain Name \(透過 IP 位址和領域名稱限制網站存取 \)](http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066) (<http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066>)
- ◆ [IIS FAQ: 2000 IP address and domain name restrictions \(IIS FAQ：2000 個 IP 位址和領域名稱限制\)](http://www.iisfaq.com/default.aspx?View=A136&P=109) (<http://www.iisfaq.com/default.aspx?View=A136&P=109>)
- ◆ [Working With IIS Packet Filtering \(使用 IIS 封包篩選 \)](http://www.15seconds.com/issue/011227.htm) (<http://www.15seconds.com/issue/011227.htm>)

基於安全性考量，我們強烈建議您在任何的 IIS 安裝中移除以下預設資料夾：

- ◆ IISHelp
- ◆ IISAdmin
- ◆ Scripts
- ◆ Printers

我們也建議您使用 [microsoft.com](http://www.microsoft.com/technet/security/tools/locktool.mspx) (<http://www.microsoft.com/technet/security/tools/locktool.mspx>) 提供的 IIS Lockdown Tool 2.1。

2.1 版是由各大適用 IIS 相關 Microsoft 產品的範本所驅動。請選取最符合此伺服器角色的範本。如果您不確定，建議您使用動態 Web 伺服器範本。

在開始進行安裝「之前」，請確定已完成以下必要條件：

- 確認可存取已支援的目錄服務 (eDirectory、Active Directory 或 NT Domains*)。* = 只有當「管理服務」安裝在 Microsoft Windows 2000 Advanced Server (SP4) 上時才支援。
- 如果您使用 eDirectory™ 服務進行部署，請確定 Novell Client™ 已安裝在伺服器上，並可正確驗證至 eDirectory。請建立不會變更的帳戶密碼，可以供「管理主控台」驗證時使用（請參閱 [「新增 eDirectory 服務」](#)（第 43 頁））。
- 確定 Endpoint Security Client 至 MS 伺服器名稱解析：驗證目標電腦（已安裝 Endpoint Security Client）可 Ping MS 伺服器名稱。若能成功，這將會是在安裝中輸入的值。若不成功，則您必須在繼續進行安裝之前先將問題解決。

- 啓用或安裝 Microsoft Internet Information Services (IIS)，確定您已啓用 ASP.NET，並將其設定為接受保全插槽層 (SSL) 證書。

重要：請勿在「安全通訊」頁面選取「必須使用安全通道 (SSL)」核取方塊 (在「Microsoft 電腦管理」公用程式中，展開「服務和應用程式」>展開「Internet Information Services (IIS) 管理員」>展開「網站」>以滑鼠右鍵按一下「預設的網站」>按一下「內容」>按一下「目錄安全設定」索引標籤>按一下「安全通訊」群組方塊中的「編輯」按鈕)。選取此選項會中斷 ZENworks Endpoint Security Management 伺服器與端點上之 ZENworks Endpoint Security 用戶端之間的通訊。

- 如果您使用自己的 SSL 證書，請確定您已將根 CA 載入機器，且在之前步驟中驗證的伺服器名稱 (無論是 NETBIOS 或 FQDN) 符合在 IIS 中設定之證書的「發給」值。
- 如果您使用自己的證書，或者已安裝 Novell 自我簽署證書，您也可以已在安裝 Endpoint Security Client 的機器中嘗試使用以下 URL 來驗證 SSL：https://MS_SERVER_NAME/AuthenticationServer/UserService.asmx (其中 MS_SERVER_NAME 為伺服器名稱)。這將會傳回有效的資料 (html 頁面)，而不是證書警告。任何的證書警告都必須在安裝之前解決。
- 確定可存取支援的 RDBMS (Microsoft SQL Server 2000 SP4、SQL Server Standard、SQL Server Enterprise、SQL 2005)。將資料庫設為「混合」模式。
- 將包含「規則配送服務」安裝 ID 和「規則配送服務」根 SSL 證書的 ESM Setup Files 目錄複製至此伺服器的安裝目錄。

6.1 安裝步驟

按一下「安裝介面」功能表中的「管理服務安裝」。「管理服務」的安裝就會開始。

在啓動時，安裝程式會驗證所有必要的軟體是否皆位於伺服器中。若缺少任何軟體，安裝程式會在進入「歡迎畫面」之前自動安裝這些軟體 (必須接受附加軟體的授權合約)。若您需要安裝 Microsoft Data Access Components (MDAC) 2.8，則必須在安裝程序之後，將伺服器重新開機以繼續安裝 ZENworks Endpoint Security Management。若使用 Windows 2003 Server，則 ASP.NET 2.0 必須設定為由安裝程式執行。

「管理服務」安裝開始後，請執行以下步驟：

附註：以下步驟將列出管理員完成安裝程序所需執行的動作。除非是成功完成安裝所需的特定動作或資訊，否則內部程序將會在整個安裝程序中顯示，而不會在此列出。

- 1 按一下「歡迎」畫面中的「下一步」以繼續。
- 2 接受授權合約，然後按一下「下一步」。
- 3 選取「典型」或「自訂」安裝。

圖 6-1 選取「典型」或「自訂」



以下說明兩種安裝方式：

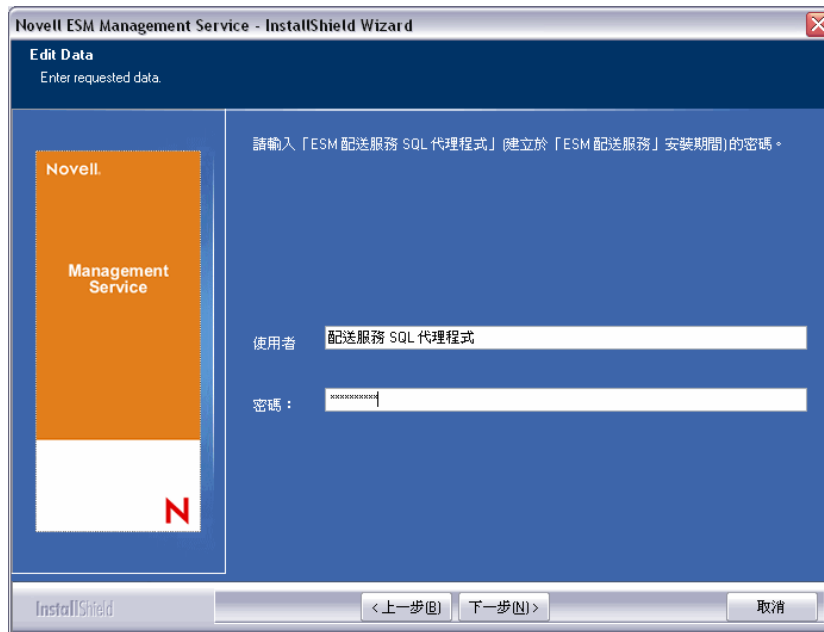
- 「典型安裝」(第 31 頁)
- 「自訂安裝」(第 35 頁)

6.1.1 典型安裝

典型安裝會將「管理服務」軟體檔案置於預設目錄中：`\Program Files\Novell\ESM Management Service`。SQL 資料庫名稱將指定為 `STMSDB`。三種 SQL 資料庫檔案(資料、索引和記錄)將置於：`\Program Files\Microsoft SQL Server\mssql\Data`。

- 1 指定在「規則配送」安裝期間建立的「規則配送服務」代辦密碼。

圖 6-2 輸入 SQL 密碼



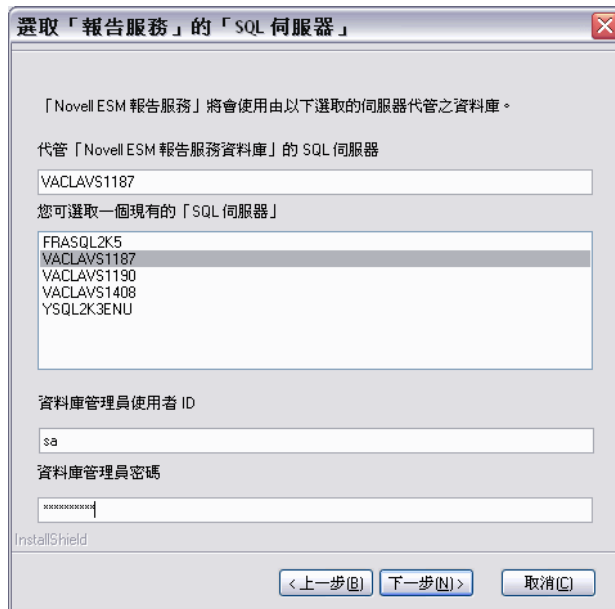
2 指定將代管「管理服務」的伺服器名稱。

圖 6-3 輸入 MS 伺服器名稱



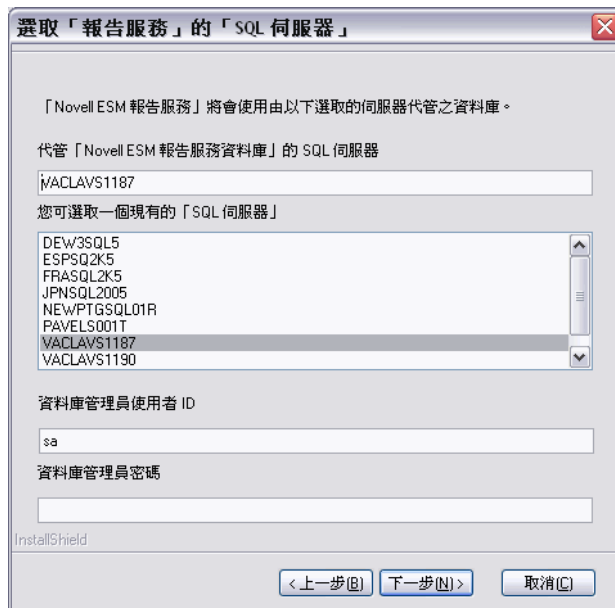
- 3 安裝程序中將會建立 Novell SSL 證書。如果您想要使用自己的 SSL 證書，請執行「**自訂安裝**」。這些證書必須配送給所有的使用者。
- 4 安裝程式將會偵測機器和網路上可用的 SQL 資料庫。選取「管理服務」的 SQL 資料庫，並指定資料庫管理員的使用者名稱和密碼(如果密碼為零字元，安裝程式將會發出潛在的安全性問題警告)。使用者名稱和密碼不能是領域使用者；它必須是擁有 SysAdmin 權限的 SQL 使用者。

圖 6-4 選取 MS SQL 資料庫



- 5 選取「報告服務」的 SQL 資料庫，並指定資料庫管理員在該資料庫的密碼。如果您想要擷取並儲存大量的報告，我們建議您在個別的 SQL 伺服器上建立「報告服務」資料庫。

圖 6-5 選取「報告服務」資料庫



- 6 如果您已購買 ZENworks Endpoint Security Management，您將會獲得個別的授權檔。將授權檔複製至此伺服器中並進行瀏覽（請參閱包含在授權檔案中的指示頁以取得詳細資訊）。如果您尚未購買 ZENworks Endpoint Security Management 授權，請選取「60 天試用授權」以繼續執行。

圖 6-6 瀏覽至 Novell 授權檔



- 7 在「複製檔案」畫面中按一下「下一步」以開始安裝。
- 8 「管理服務」將會執行 SQL 資料庫與「規則配送服務」的通訊檢查。如果通訊無法通過驗證，安裝程式會通知您該問題。所有方塊都必須勾選，安裝才能成功。

圖 6-7 通訊驗證



- 9 如果您將 eDirectory 安裝為目錄服務，請跳過 **步驟 10** 和 **步驟 11**。
- 10 如果您進行安裝的伺服器是執行 Active Directory 或 NT Domains 目錄服務的領域成員伺服器，則安裝程式將自動進行偵測，並使用安全且唯讀的連接將下列資料新增至安裝中：
 - ◆ 根部領域名稱或機器名稱
 - ◆ 領域管理員的名稱或具有適當讀取許可的資源帳戶
- 11 在空格中輸入管理員的密碼並按一下「**測試以驗證是否可以建立連接**」。如果測試成功，請按一下「**儲存**」。如果測試失敗，或無法偵測正確的領域，則必須透過「**管理主控台**」手動進行新增(請參閱「**新增 eDirectory 服務**」(第 43 頁))。

附註：所輸入的密碼應設定為不會過期，並且永遠都不停用此帳戶。

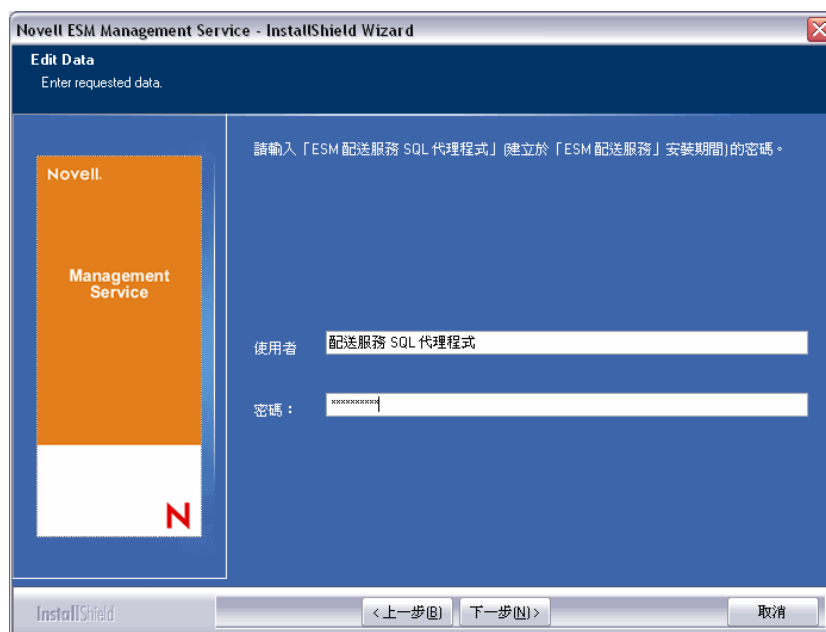
- 12 現在已安裝「管理服務」，按一下「結束」關閉通訊檢查，然後按一下「完成」關閉安裝程式。

6.1.2 自訂安裝

自訂安裝將顯示在典型安裝中使用的預設值，並允許管理員進入或瀏覽不同的位置。

- 1 指定在「規則配送」安裝期間建立的「規則配送服務」代辦密碼。

圖 6-8 輸入 SQL 密碼



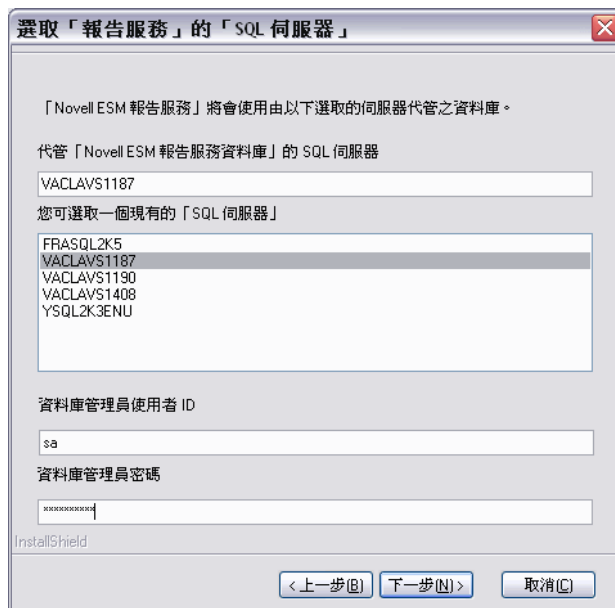
- 2 選取在「規則配送服務」安裝中使用的 SSL 證書類型。如果您使用現有的(企業)證書權限，請按一下：「Novell 配送服務使用已設定 IIS 的證書」。如果「配送服務」安裝程式已建立 Novell 證書，請按一下「Novell 配送服務已安裝 Novell 自我簽署根證書」。
- 3 指定將代管「管理服務」的伺服器名稱。

圖 6-9 輸入 MS 伺服器名稱



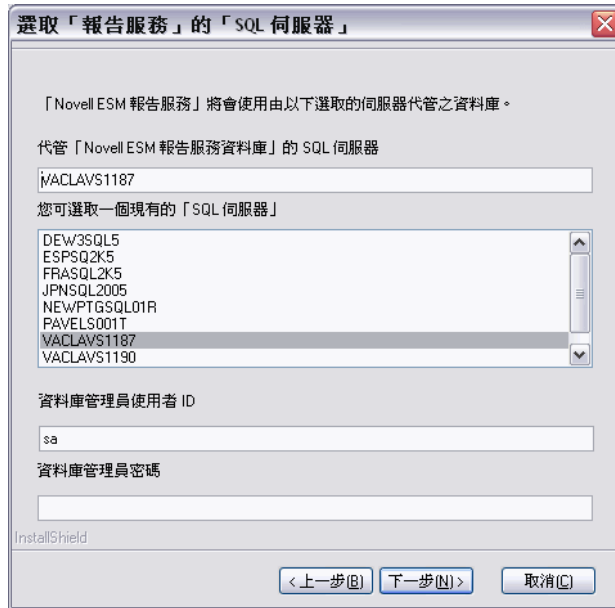
- 4 「管理服務」和所有 Endpoint Security Client 之間的安全通訊將需要 SSL 證書。如果您已經擁有證書權限，請按一下「使用 IIS 設定的現有證書」。如果您需要證書，請按一下「允許 Novell 建立、安裝與使用其自我簽署根部證書」。安裝程式將建立證書和簽署權限。無論證書的類型為何，這些證書都必須配送給所有的使用者。
- 5 當選取 Novell 證書時，請選取儲存證書的位置以方便配送 (預設值為安裝目錄)。
- 6 安裝程式將會偵測機器和網路上可用的 SQL 資料庫。選取「管理服務」的 SQL 資料庫，並指定資料庫管理員的使用者名稱和密碼 (如果密碼為零字元，安裝程式將會發出潛在的安全性問題警告)。使用者名稱和密碼不能是領域使用者；它必須是擁有 SysAdmin 權限的 SQL 使用者。

圖 6-10 選取 MS SQL 資料庫



- 7 設定資料庫名稱 (預設輸入為 STMSDB)。
- 8 選取「報告服務」的 SQL 資料庫，並指定資料庫管理員在該資料庫的密碼。

圖 6-11 選取「報告服務」資料庫



- 9 設定資料庫名稱 (預設輸入為 STRSDB)。
- 10 如果您已購買 ZENworks Endpoint Security Management，您將會獲得個別的授權檔。將授權檔複製至此伺服器中並進行瀏覽 (請參閱包含在授權檔案中的指示頁以取得詳細資訊)。如果您尚未購買 ZENworks Endpoint Security Management 授權，請選取「60 天試用授權」以繼續執行。

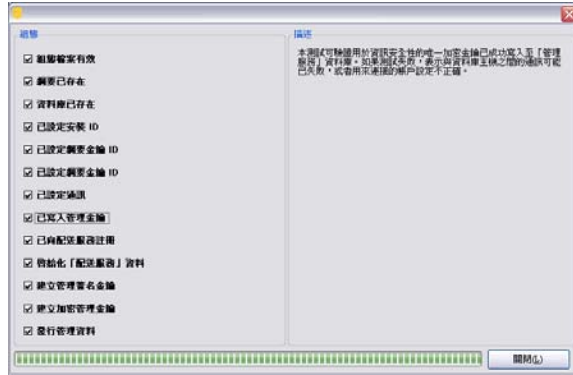
圖 6-12 瀏覽至 Novell 授權檔



- 11 在「複製檔案」畫面中按一下「下一步」以開始安裝。

- 12 選取「管理服務」資料庫之資料、索引和記錄檔的檔案路徑。
- 13 選取「報告服務」資料庫之資料、索引和記錄檔的檔案路徑。
- 14 「管理服務」將會執行 SQL 資料庫與「規則配送服務」的通訊檢查。如果通訊無法通過驗證，安裝程式會通知您該問題。所有方塊都必須勾選，安裝才能成功。

圖 6-13 通訊驗證



- 15 如果您將 eDirectory 安裝為目錄服務，請跳過 [步驟 16](#) 和 [步驟 17](#)。
- 16 如果您進行安裝的伺服器是執行 Active Directory 或 NT Domains 目錄服務的領域成員伺服器，則安裝程式將自動進行偵測，並使用安全且唯讀的連接將下列資料新增至安裝中：
 - ◆ 根部領域名稱或機器名稱
 - ◆ 領域管理員的名稱或具有適當讀取許可的資源帳戶
- 17 在空格中輸入管理員的密碼並按一下「[測試以驗證是否可以建立連接](#)」。如果測試成功，請按一下「[儲存](#)」。如果測試失敗，或無法偵測正確的領域，則必須透過「[管理主控台](#)」手動進行新增（請參閱「[新增 eDirectory 服務](#)」（[第 43 頁](#)））。

附註：所指定的密碼應設定為不會過期，並且永遠都不停用此帳戶。

- 18 現在已安裝「管理服務」，按一下「[結束](#)」關閉通訊檢查，然後按一下「[完成](#)」關閉安裝程式。

6.2 啓動服務

「管理服務」會在安裝後立即啓動，而不需將伺服器重新開機。管理主控台可用來管理「管理服務」中的資料（請參閱《[ZENworks Endpoint Security Management 管理指南](#)》）。

Novell 建議您在此伺服器上安裝「管理主控台」。若要將「管理主控台」安裝在個別的機器上，請透過網路共享或將檔案儲存至磁碟或隨身碟，將 ESM Setup Files 目錄複製至將代管「管理主控台」的機器上。

請繼續進行 [第 7 章](#)「[執行管理主控台安裝](#)」（[第 39 頁](#)）。

執行管理主控台安裝

「管理主控台」可安裝在「管理服務」伺服器上，也可以安裝在與「管理服務」伺服器直接通訊的安全 PC 上。您可以將多個「管理主控台」安裝設定為與單一「管理服務」進行通訊，但我們強烈建議您將「管理主控台」的存取權僅授予經選擇過後的使用者。

基於安全性考量，我們建議您將管理主控台直接安裝在「管理服務」的伺服器上。

如果您要在個別的工作站上安裝「管理主控台」，請確定在安裝之前完成以下必要條件：

- ❑ 請確定要安裝「管理主控台」的設備符合以下需求：
 - ◆ Windows XP SP1、Windows XP SP2 或 Windows 2000 SP4。
 - ◆ 建議使用 1.0 GHz 的處理器，以及最低 256 MB 的 RAM 和 100 MB 的可用磁碟空間。
- ❑ 將 ESM Setup Files 資料夾 (其中包含「規則配送服務」和「管理服務」的 SSL 根證書) 以及 STInstParam.id 檔案複製到 PC 中。
- ❑ 如果將「管理主控台」安裝在「管理服務」伺服器上，請確認 Microsoft Internet Explorer 為 5.5 或更高版本。

7.1 安裝步驟

按一下「安裝介面」功能表中的「管理主控台安裝」。

在啟動時，安裝程式將確認必要的 .NET Framework 3.5 和 WSE 2.0 SP2 已位於機器中。如果缺少其中一項或兩項，安裝程式會在進入「歡迎畫面」之前自動安裝這些軟體 (您必須接受 .NET 3.5 的授權合約)。

若要安裝管理主控台：

- 1 按一下「下一步」繼續。
- 2 接受授權合約，然後按一下「下一步」。
- 3 選取「典型」或「自訂」安裝。

圖 7-1 選取「典型」或「自訂」



以下說明兩種安裝方式：

- 「典型安裝」(第 40 頁)
- 「自訂安裝」(第 40 頁)

7.1.1 典型安裝

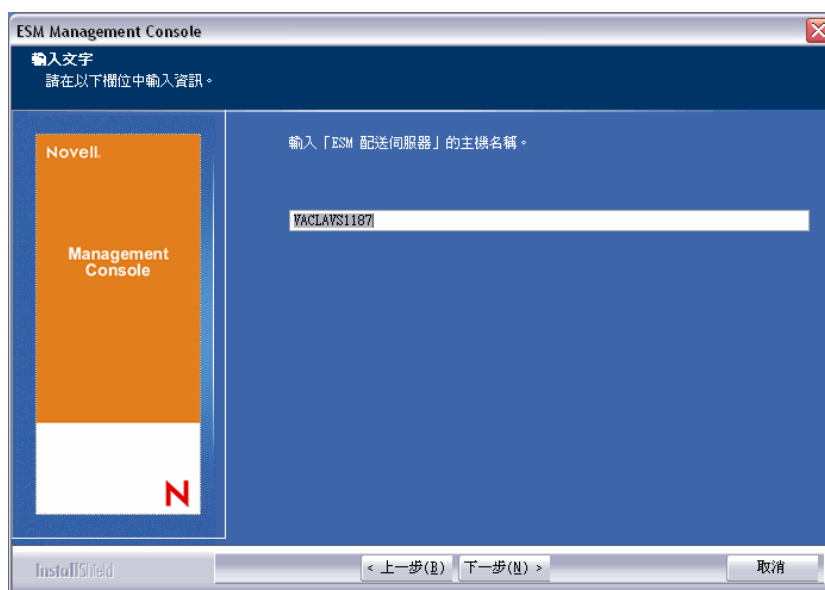
典型安裝將使用 STInstParam.id 檔案中的所有預設伺服器以及 SSL 資訊，並建立預設目錄：`\Program Files\Novell\ESM Management Console`。如果 ESM Setup Files 目錄已位於機器中，則「管理主控台」的安裝將不需要進行額外選定的項目。

7.1.2 自訂安裝

自訂安裝將顯示在典型安裝中使用的 STInstParam.id 預設值，並允許管理員變更該資訊。

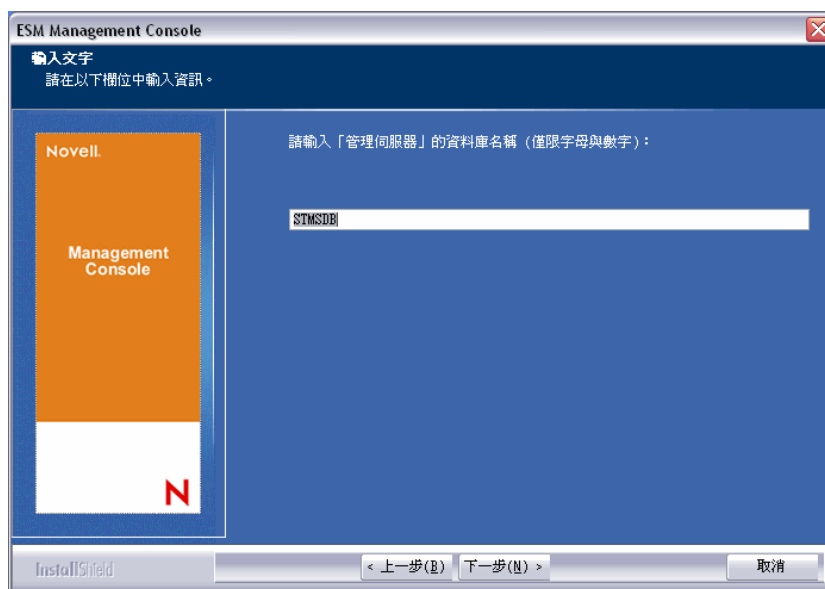
- 1 指定「規則配送服務」的主機名稱(若「配送」伺服器部署在公司防火牆之外，則該名稱必須是完全合格的領域名稱)。

圖 7-2 輸入「配送服務」主機名稱



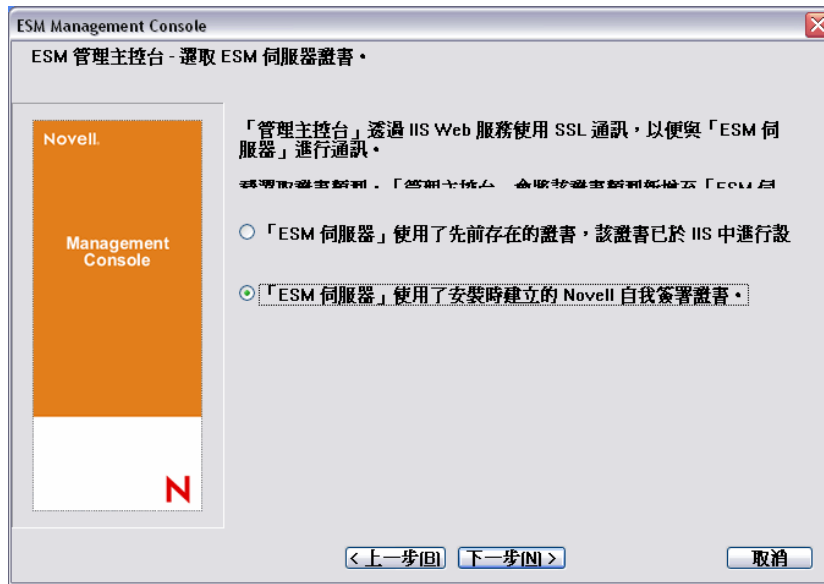
- 2 指定「管理服務」主機名稱。
- 3 指定「管理服務」SQL 資料庫主機名稱。
- 4 指定「管理服務」SQL 資料庫名稱。

圖 7-3 輸入 MS SQL 資料庫名稱



- 5 指定在「管理服務」安裝期間識別的 SQL SA 使用者名稱和密碼。
- 6 選取安裝在「規則配送服務」和「管理服務」上的 SSL 證書類型。

圖 7-4 選取伺服器證書



- 7 選取安裝「管理主控台」的目錄。預設位置為 \Program Files\Novell\ESM Management Console。

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」可讓您建立目錄服務組態，以定義 Endpoint Security Client 安裝的範圍。新組態會使用現有的目錄服務，以定義使用者為主和電腦為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」。如需關於建立與設定目錄服務的詳細資訊，請參閱《ZENworks Endpoint Security Management 管理指南》中的「設定目錄服務」。

7.2 啓動主控台

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」。

輸入管理員名稱及密碼，即可登入「管理主控台」。在輸入使用者名稱和密碼之前，您必須先連接至目錄伺服器的領域（請參閱「新增 eDirectory 服務」（第 43 頁））。輸入的使用者名稱必須是「管理服務」領域中的使用者。

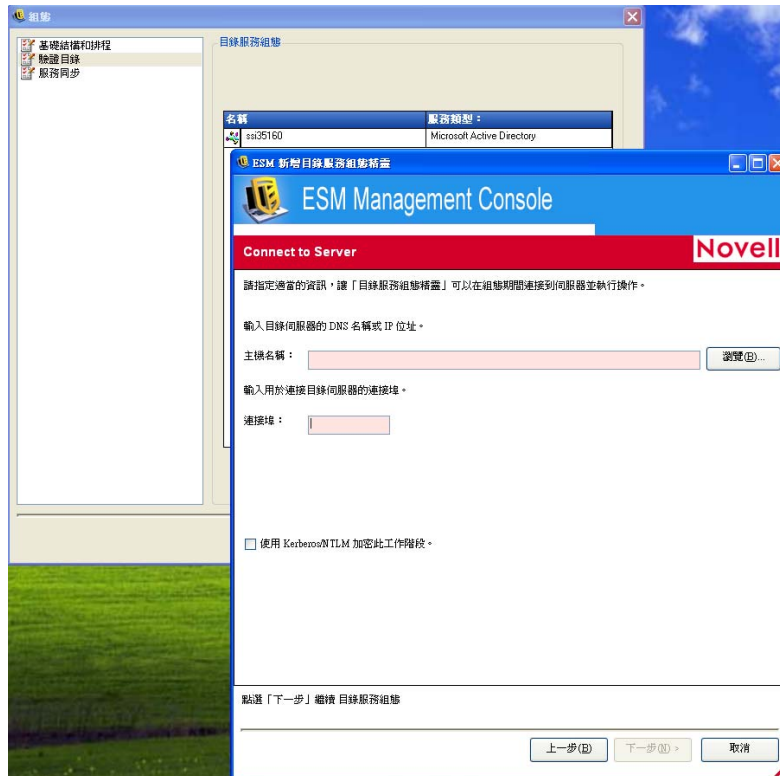
圖 7-5 登入 ZENworks Endpoint Security Management 管理主控台



7.2.1 新增 eDirectory 服務

- 1 按一下登入畫面上的「選項」按鈕，接著會顯示「組態」視窗。

圖 7-6 驗證目錄



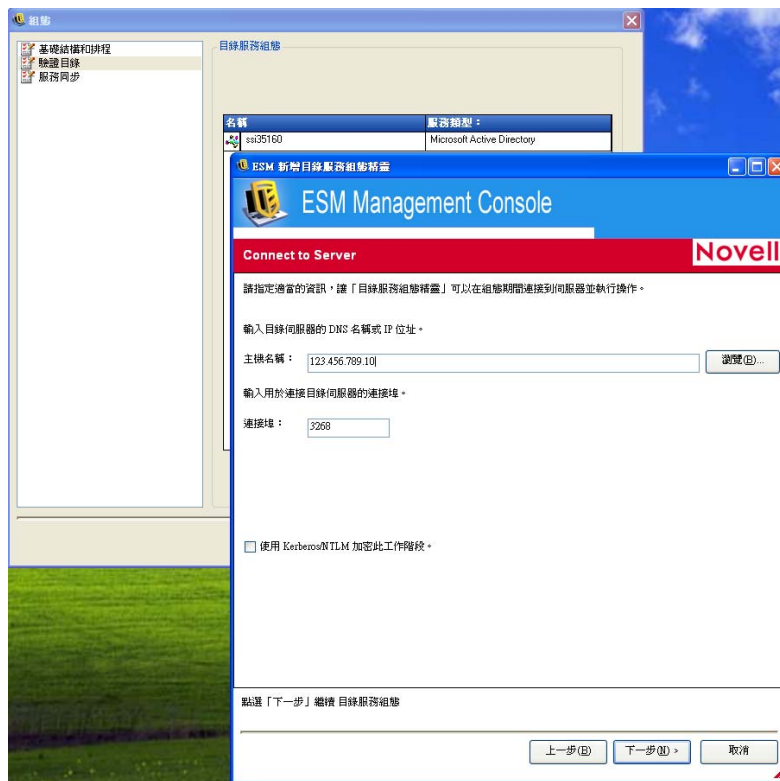
- 2 輸入 Directory Service 的易記名稱，並在「服務類型」下拉式清單中選取「eDirectory」。

- 3 在「主機/DN」方塊中輸入 eDirectory 伺服器的 IP 位址，並在「領域」網路樹之下指定網路樹名稱。
- 4 勾選「可用於使用者驗證」以在登入下拉式功能表中顯示網域。
- 5 在「服務連接」選項中取消勾選「安全驗證」。
- 6 指定 LDAP 格式輸入帳戶名稱。例如，"cn=admin,o=acmeserver" 中的 cn 為使用者，而 o 是儲存使用者帳戶的物件。
- 7 指定該帳戶的密碼。

附註：您不能將密碼設為過期，且不能停用此帳戶。

- 8 按一下「測試」，以驗證與此目錄服務的通訊。如果無法建立通訊，即會通知使用者此一錯誤。測試前間若發生任何錯誤資訊，則藉由介面修正。

圖 7-7 完成的目錄畫面



- 9 按一下「儲存」將此目錄服務新增至資料庫，然後按一下「新增」將其他目錄服務新增至資料庫。
- 10 按一下「確定」或「取消」，以結束「組態」視窗，並返回登入畫面。

請參閱《ZENworks Endpoint Security Management 管理指南》以瞭解如何設定額外目錄服務的監聽，包括支援的 Active Directory 和 NT Domains 服務。

7.2.2 設定管理主控台的許可設定

您可以在「管理主控台」的「工具」功能表中找到「許可」，而且只有「管理服務」的主要管理員和已由該管理員授予「許可」存取的任何人員可以存取。在執行獨立管理主控台時無法使用此控制（請參閱第 11 章「ZENworks Endpoint Security Management 安裝」（第 69 頁），以取得詳細資訊）。

許可設定會定義已允許哪些使用者或使用者群組可存取「管理主控台」、「發行規則」和「變更許可設定」。

在「管理伺服器」安裝期間，會在組態表單中輸入管理員或「資源帳戶」名稱。一旦測試已成功執行並儲存使用者資訊之後，系統會將許可自動授予該使用者。

在安裝「管理主控台」後，系統會將完整許可授予領域內的所有使用者。除了應具備存取權之群組和使用者外，資源使用者應移除其他所有群組和使用者之許可。資源使用者可針對指定的使用者設定其他許可。所授予的許可會產生下列結果：

- ◆ **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至指定的使用者和群組。
- ◆ **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，或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意規則。

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

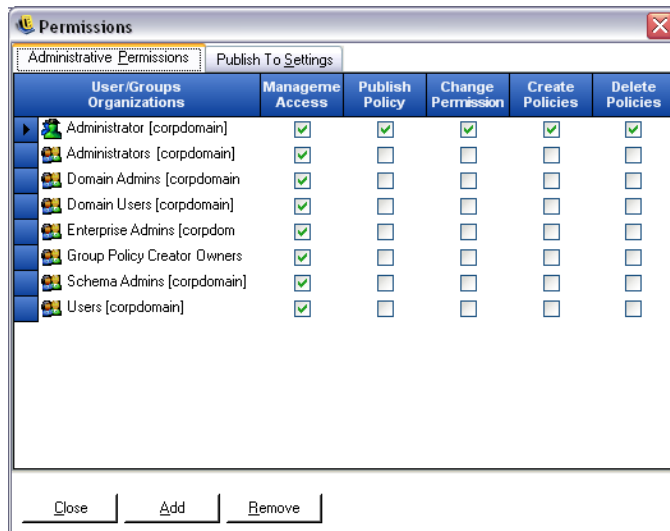
以下幾節中包含了更詳細的資訊：

- ◆ 「設定管理許可」（第 45 頁）
- ◆ 「變更「發行至」設定」（第 47 頁）

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。

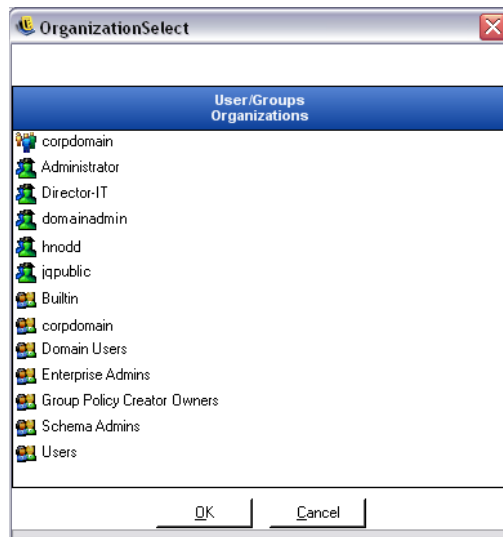
圖 7-8 管理主控台許可設定視窗



附註：依照預設值，「管理主控台」中的所有群組都可獲得完整許可。管理員必須立即取消勾選未獲授權群組的任何規則任務。您可以取消勾選許可，來移除主控台的存取權限。

- 2 (選擇性) 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」按鈕以顯示組織表。

圖 7-9 許可設定組織表格



- 2b 從清單中選取適當的使用者和群組。使用 Ctrl 或 Shift 鍵選取多個使用者。
 - 2c 選取所有的使用者和群組之後，按一下「確定」按鈕，將使用者和群組新增至「許可」表格中。
- 3 將許可指定給可用的使用者和群組。

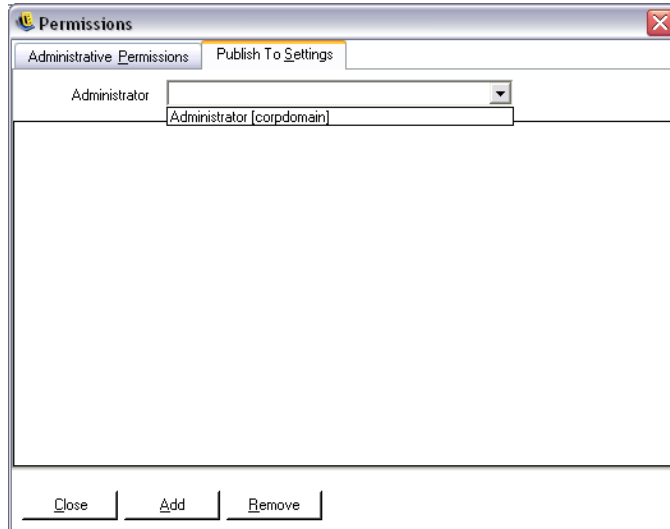
若要移除選取的使用者或群組，請將名稱反白後按一下「移除」。

變更「發行至」設定

您必須為已核取「發行規則」的使用者或群組指定發行規則的對象。若要設定「發行至」設定：

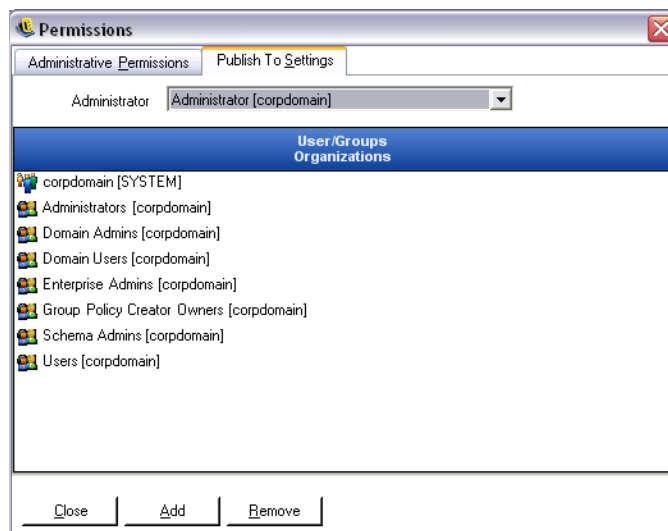
- 1 按一下「發行至設定」索引標籤。
- 2 在下拉式清單中選取授予「發行許可」的使用者和群組。

圖 7-10 發行設定



- 3 若要將使用者和群組指定給此使用者或群組：
 - 3a 按一下畫面底端的「新增」按鈕以顯示組織表。
 - 3b 從清單中選取適當的使用者和群組。使用 Ctrl 和 Shift 鍵選取多個使用者。
 - 3c 在選取所有使用者 / 群組之後，按一下「確定」按鈕。

圖 7-11 發行清單



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」。

系統會立即實作許可權設定，如此一來，管理員只需按一下「關閉」，並接受變更，以返回編輯器。

當新增新的目錄服務時，「資源帳戶」將獲得完整的許可設定，如以上所述。

7.2.3 發行規則

若要依預設設定發行安全性規則：

- 1 按一下「**建立新規則**」。
- 2 指定規則名稱，再按一下「**建立**」。
- 3 儲存規則並按一下「**發行**」索引標籤。
- 4 由於 Endpoint Security Client 使用者必須登入才能顯示在網路樹中，請選取左側之網路樹頂端，然後連按兩下將所有的群組和使用者填入發行欄位中。
- 5 按一下「**發行**」將規則傳送至「規則配送服務」。

以此方法產生的規則具有以下特性：

- ◆ 會建立單一位置（「不明」）。
- ◆ 允許使用 CD/DVD 光碟機。
- ◆ 允許使用可移除儲存設備。
- ◆ 允許所有的通訊連接埠（包括 Wi-Fi）。
- ◆ 「防火牆設定」包含「全部調整」（允許網路連接埠上的全部外傳流量；不允許網路連接埠上來路不明的內傳流量）。

如需瞭解如何建立更健全的安全性規則，請參閱《*ZENworks Endpoint Security Management 管理指南*》。

請繼續進行 [第 8 章「執行用戶端位置保證服務安裝」](#)（第 49 頁）。

7.3 安裝 USB Reader

包含在安裝套件內的 Novell USB Reader 可協助管理員建立允許的 USB 裝置清單。

若要安裝 Reader：

- 1 按一下「**安裝**」開始安裝。
- 2 在「歡迎畫面」中按一下「**下一步**」以繼續。
- 3 接受授權，然後按一下「**下一步**」。
- 4 在客戶資訊畫面中，指定適當的使用者名稱和組織資訊，並決定是否要讓此電腦上的所有使用者都可存取此軟體，或是只有指定的使用者才能存取。
- 5 按一下「**安裝**」。
- 6 按一下「**完成**」。

如需使用 USB Reader 的詳細資訊，請參閱《*ZENworks Endpoint Security Management 管理指南*》。

執行用戶端位置保證服務安裝

只有當使用者進入受控制的網路環境時才能存取此伺服器，這可用來確保其確實位於 ZENworks® Security Client 已識別的環境中。您可以在下方找到容錯移轉和重複性組態的指示。如有需要，您可以將「用戶端位置保證服務」(CLAS) 部署在代管「單一伺服器安裝」或「多重伺服器」「管理服務」安裝的伺服器上。

請將 CLAS 安裝在僅能由需要密碼驗證之網路環境中的端點所偵測到的端點上。

基於安全性和功能性的原因，您無法將 CLAS 部署在主要領域控制器 (Primary Domain Controller, PDC) 上。

附註：我們建議您在設定 (強化) SSI 伺服器時，停用所有的應用程式、服務、帳戶以及伺服器功能性所不需要的其他選項。執行此作業的步驟將視本機環境而定，因此無法預先說明。我們建議管理員參閱 [Microsoft Technet 安全性網頁 \(http://www.microsoft.com/technet/security/default.mspx\)](http://www.microsoft.com/technet/security/default.mspx) 中適合的區段。《ZENworks Endpoint Security Management 管理指南》還提供其他的存取控制建議。

若要保護僅存取受信任的機器，可將虛擬目錄和 IIS 設定為具有 ACL。請參考以下文章：

- ◆ [Granting and Denying Access to Computers \(授予和拒絕電腦存取 \) \(http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx\)](http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx)
- ◆ [Restrict Site Access by IP Address or Domain Name \(透過 IP 位址和領域名稱限制網站存取 \) \(http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066\)](http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)
- ◆ [IIS FAQ: 2000 IP address and domain name restrictions \(IIS FAQ：2000 個 IP 位址和領域名稱限制\) \(http://www.iisfaq.com/default.aspx?View=A136&P=109\)](http://www.iisfaq.com/default.aspx?View=A136&P=109)
- ◆ [Working With IIS Packet Filtering \(使用 IIS 封包篩選 \) \(http://www.15seconds.com/issue/011227.htm\)](http://www.15seconds.com/issue/011227.htm)

基於安全性考量，我們強烈建議您在任何的 IIS 安裝中移除以下預設資料夾：

- ◆ IISHelp
- ◆ IISAdmin
- ◆ Scripts
- ◆ Printers

我們也建議您使用 [microsoft.com \(http://www.microsoft.com/technet/security/tools/locktool.mspx\)](http://www.microsoft.com/technet/security/tools/locktool.mspx) 提供的 IIS Lockdown Tool 2.1。

2.1 版是由各大適用 IIS 相關 Microsoft 產品的範本所驅動。請選取最符合此伺服器角色的範本。如果您不確定，建議您使用動態 Web 伺服器範本。

在開始進行安裝之前，請確定已完成以下必要條件：

- 確定「管理服務」(MS) 至「規則配送服務」(DS) 的伺服器名稱解析：確定驗證目標電腦 (已安裝 MS) 可 Ping DS 伺服器名稱 (若是在網路防火牆內部設定 DS 則為 NETBIOS，若在 DMZ 外部安裝則為 FQDN)。
- 啓用或安裝 Microsoft Internet Information Services (IIS)，並確定已啓用 ASP.NET。

重要：請勿在「安全通訊」頁面選取「必須使用安全通道 (SSL)」核取方塊 (在「Microsoft 電腦管理」公用程式中，展開「服務和應用程式」>展開「Internet Information Services (IIS) 管理員」>展開「網站」>以滑鼠右鍵按一下「預設的網站」>按一下「內容」>按一下「目錄安全設定」索引標籤>按一下「安全通訊」群組方塊中的「編輯」按鈕)。選取此選項會中斷 ZENworks Endpoint Security Management 伺服器與端點上之 ZENworks Endpoint Security 用戶端之間的通訊。

按一下「安裝介面」功能表中的「用戶端位置保證服務安裝」。CLAS 安裝就會開始。

在啟動時，安裝程式會驗證所有必要的軟體是否皆位於伺服器中。若缺少任何軟體，安裝程式會在進入「歡迎畫面」之前自動安裝這些軟體 (必須接受附加軟體的授權合約)。若您尚未安裝 Microsoft Data Access Components 2.8，則必須在安裝程序之後，將伺服器重新開機以繼續安裝 ZENworks Endpoint Security Management。若使用 Windows 2003 Server，則 ASP.NET 2.0 將設定為由安裝程式執行。

8.1 安裝步驟

若要安裝並產生授權金鑰

- 1 按一下「歡迎」畫面中的「下一步」以繼續。
- 2 接受授權合約，然後按一下「下一步」。
- 3 安裝程式會將檔案複製至預設目錄：\Program Files\Novell\ESM CLAS。
- 4 「用戶端位置保證服務」的安裝將會產生兩種金鑰：私密金鑰和公開金鑰。您可將公開金鑰檔案儲存在桌面或不同的目錄中。如果您要將公開金鑰儲存在不同的目錄中，請按一下「是」，並瀏覽至想要的資料夾。按一下「否」以接受預設值，將公開金鑰檔案與私密金鑰檔案儲存在一起。
- 5 按一下「完成」關閉安裝程式。

「管理服務」必須能存取公開金鑰。

8.2 CLAS 容錯移轉安裝

您可以將多重 CLAS 重複安裝在整個企業中的伺服器上，如此將能以密碼方式確保多個企業位置，或者在主要 CLAS 伺服器故障時，仍可正常確保該位置。

若發生第二種情況，私密金鑰的位置將會根據 URL 而不是 IP 位址。因此您可將整個區塊的伺服器設定為共享一個單一 URL。您可以將 CLAS 安裝在單一伺服器中，如此可將該伺服器的複本複製到其他的伺服器，或者您也可以將其個別安裝在每個伺服器中，而將私密和公開金鑰將複製至其他的伺服器。位於 URL 區塊中的所有伺服器都必須有相同的私密和公開金鑰。

8.3 將公用金鑰傳送至管理服務

在安裝完成之後，產生的公用金鑰將會經由安全性規則傳送至 Endpoint Security Client，該金鑰位於伺服器的 \Program Files\Novell\Novell ESM CLAS 目錄中。您可由檔案名稱 publickey 辨識公開金鑰。您可以將檔案名稱變更為任何名稱。

之後系統會複製公開金鑰並傳送至「管理服務」(位於服務的任何位置上)，這可讓「管理主控台」存取該金鑰，並經由安全性規則將其配送至所有的 Endpoint Security Client。您也可以將 publickey 檔案載入執行「ZENworks Endpoint Security Management 管理主控台」的電腦中。

請繼續進行 [第 9 章「Endpoint Security Client 3.5 安裝」\(第 53 頁\)](#)。

Endpoint Security Client 3.5 安裝

9

為 Windows XP (SP1 與 SP2) 與 Windows 2000 SP4 用戶端使用 Novell ZENworks Endpoint Security Client 3.5。按一下「安裝介面」功能表中的適當 *ZENworks Security Client* 安裝程式。Endpoint Security Client 安裝就會開始。以下各頁將簡介基本安裝和 MSI 安裝的安裝程序。

- ◆ 「基本安裝」只會將 Endpoint Security Client 3.5 安裝在目前的機器上。
- ◆ MSI 安裝程序將會在「管理」模式 (/a) 中啟動安裝程式，並建立軟體的 MSI 套件。您可以將此套件向下傳遞，或者在預先設定必要的使用者輸入後，在特定的網路環境中發佈。這可讓個別的使用者以預先定義的伺服器值安裝軟體。

9.1 基本 Endpoint Security Client 3.5 安裝

此程序只會在目前的機器上安裝 Endpoint Security Client 3.5。

確認已安裝所有最新版的 Microsoft 安全性修補和防毒軟體。

將「管理服務」SSL 根證書安裝至本地機器 (ESM-MS.cer 或企業證書)

附註：我們建議您在安裝 Endpoint Security Client 3.5 期間，關閉與有效登錄功能進行互動的防毒 / 防間諜軟體。

- 1 按一下「歡迎」畫面中的「下一步」以繼續。
- 2 接受授權合約，然後按一下「下一步」。
- 3 輸入安裝密碼。這可避免使用者透過「新增 / 移除程式」解除安裝 Endpoint Security Client 3.5 (建議使用)。

圖 9-1 解除安裝密碼



- 4 選取接收規則的方法 (受管理的用戶端從「配送服務」，不受管理組態則在本機取回 [請參閱 第 11 章「ZENworks Endpoint Security Management 安裝」(第 69 頁) 瞭解不受管理的詳細資訊])。

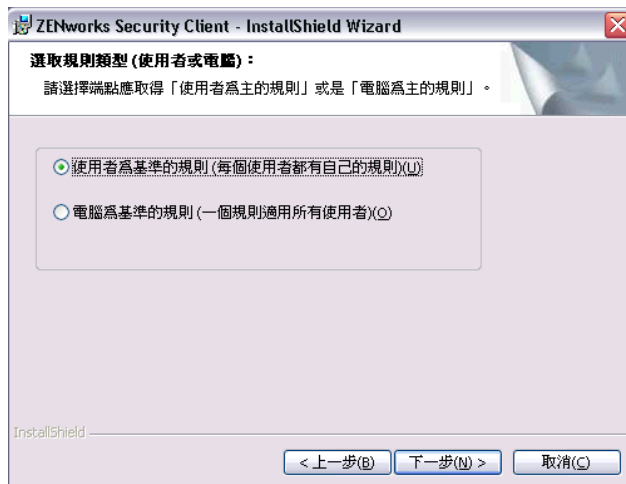
圖 9-2 管理設定



5 指定「管理服務」資訊。

6 選擇要為使用者或機器 (以機器為基礎的規則) 接收規則。

圖 9-3 以使用者或機器為基礎的規則



7 按一下「安裝」。

在安裝軟體之後，系統將提示使用者重新啟動機器。

附註：您可以選擇在執行安裝前，將「管理服務」證書複製至與 setup.exe 位置相同的資料夾。這會自動將證書安裝至機器 (例如，全部使用者)。您也可以對 Novell license.dat 檔案進行相同的程序。

9.2 MSI 安裝

此程序會為 Endpoint Security Client 3.5 建立 MSI 套件。系統管理員可使用此套件透過 Active Directory 規則或其他軟體配送方法將安裝發佈到使用者群組。

若要建立 MSI 套件：

如果您要從 CD 或 ISO 主安裝程式進行安裝，且不需要執行任何指令行變數 (請參閱「[指令行變數](#)」(第 57 頁))：

- 1 插入 CD 並等待主安裝程式啟動。
- 2 按一下「[產品安裝](#)」。
- 3 按一下「[Security Client](#)」。
- 4 按一下「[建立 ZSC MSI 套件](#)」。

若只要使用 setup.exe 檔案進行安裝 (您可以在 CD 上找到此可執行檔，路徑是 D:\ESM32\ZSC)，請執行以下步驟：

- 1 在 setup.exe 上按一下滑鼠右鍵。
- 2 選取「[建立捷徑](#)」。
- 3 在捷徑上按一下滑鼠右鍵，然後按一下「[內容](#)」。
- 4 在「目標」欄位結尾的引號之後按一下空格鍵，然後鍵入 /a。

例如："C:\Documents and Settings\user\Desktop\CL-Release-3.2.455\setup.exe" /a

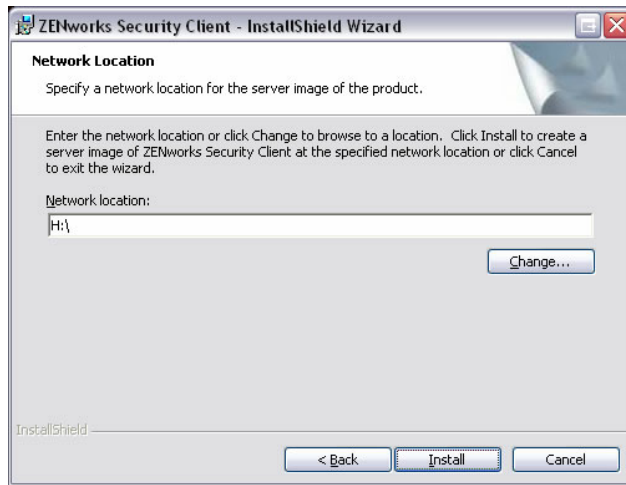
您可以使用多個指令行變數進行 MSI 安裝，請參閱「[指令行變數](#)」(第 57 頁)取得詳細資訊。

- 5 按一下「[確定](#)」。
- 6 連按兩下捷徑以啟動 MSI 安裝程式。

當開始安裝時：

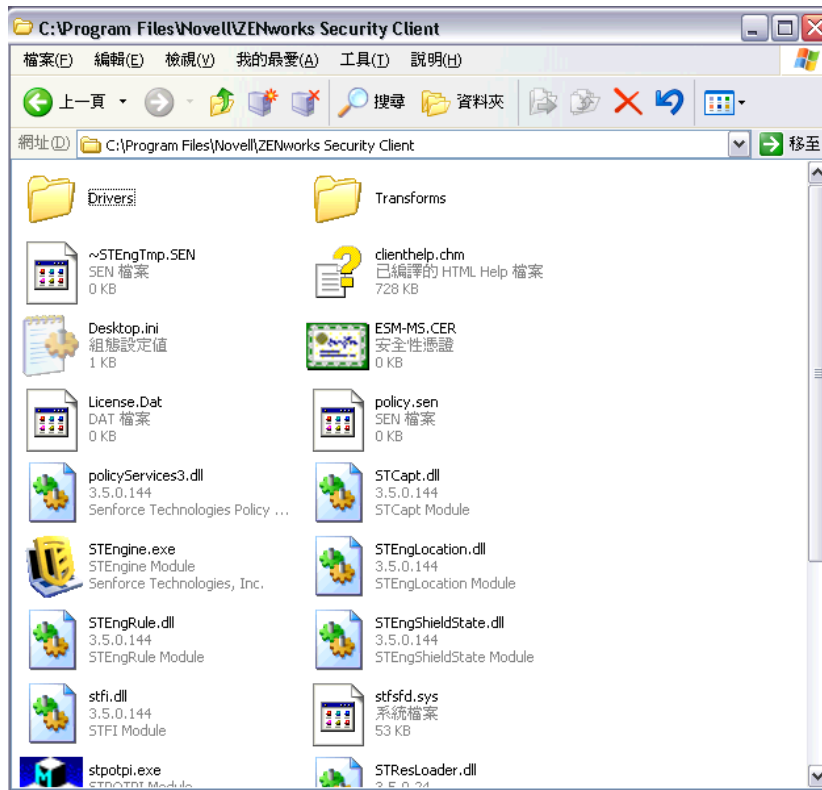
- 1 按一下「[歡迎](#)」畫面中的「[下一步](#)」以繼續。
- 2 接受授權合約，然後按一下「[下一步](#)」。
- 3 選擇是否需要「[解除安裝密碼](#)」(建議使用)並輸入密碼。
- 4 選取接收規則的方法 (受管理的用戶端從「[配送服務](#)」，不受管理組態則在本機取回)。
若選取不受管理：
 - ◆ 指定「[管理服務](#)」資訊 (視在「[管理服務](#)」安裝期間輸入的內容而定，輸入 FQDN 或 NETBIOS)。
 - ◆ 選取以使用者為基礎或以機器為基礎的規則。
- 5 (選擇性) 在提供的欄位中輸入電子郵件地址，以在安裝失敗時通知您。
- 6 指定要建立 MSI 複本的網路位置，或按一下「[變更](#)」按鈕以瀏覽至該位置。

圖 9-4 選取 MSI 複本的網路位置



- 7 按一下「安裝」建立 MSI 複本。
- 8 瀏覽至已建立的 MSI 複本，並開啓 "\program files\Novell\ZENworks Security Client\" 資料夾
- 9 將「管理服務」SSL 證書 (ESM-MS.cer 或企業證書) 和 Novell 授權金鑰複製至此資料夾，以取代目前位於資料夾中的預設 0 KB 檔案。ESM-MS SSL 證書位於 ZENworks Endpoint Security Management Setup Files 資料夾中。授權金鑰將另行以電子郵件寄發 (若使用 30 天試用版，則目前不需要授權金鑰)。

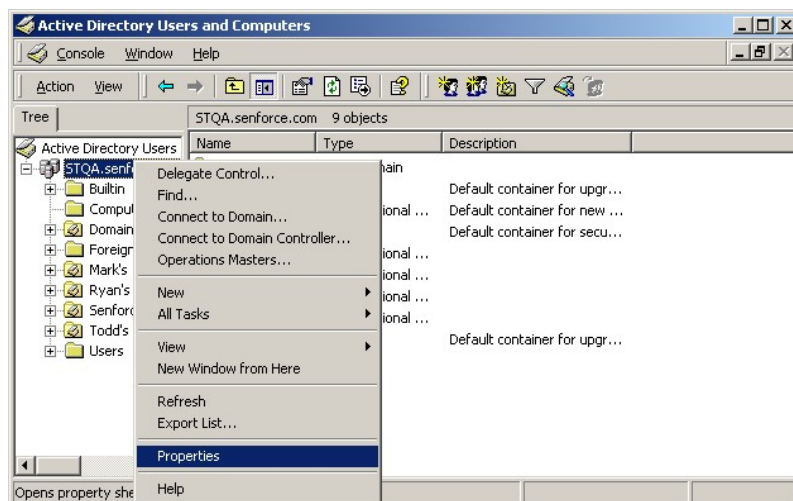
圖 9-5 取代 MSI 套件中的預設檔案



若要將 MSI 套件設為向下傳遞至使用者群組 (如「群組規則」)：

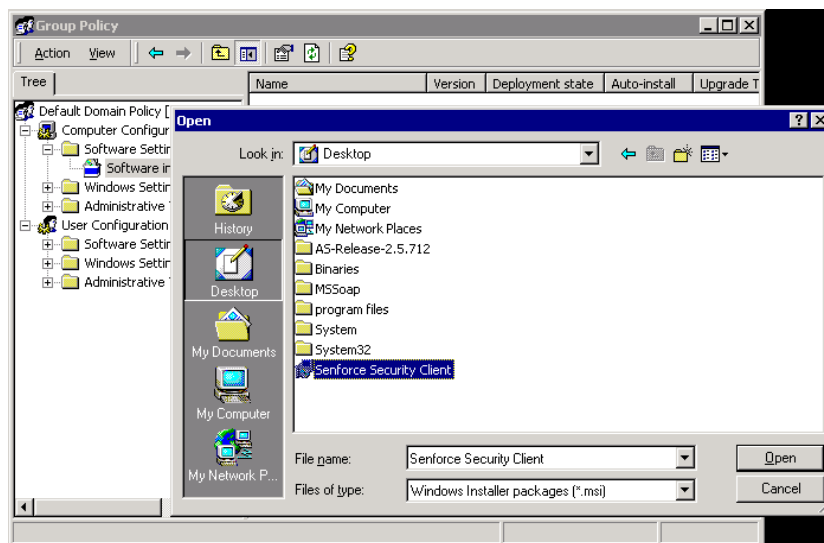
- 1 開啓「系統管理工具 - Active Directory 使用者和電腦」，並開啓「根領域」或「OU 內容」。

圖 9-6 開啓「根領域內容」或「OU 內容」



- 2 按一下「群組規則」索引標籤並按一下「編輯」。
- 3 將 MSI 套件新增至「電腦組態」。

圖 9-7 選取要新增的 MSI 套件



9.2.1 指令行變數

MSI 安裝可使用指令行變數選項。您必須在可執行捷徑中設定這些變數，並設為在管理員模式中執行。若要使用變數，您必須在 MSI 捷徑中輸入以下指令行：

“...\\setup.exe” /a /V“variables”。在兩個引號之間輸入以下任何指令。請使用單個空格分隔多個變數。

範例：setup.exe /a /V"STDRV=stateful STBGL=1" 會建立一個 MSI 套件，其中 Endpoint Security Client 3.5 將以「所有可設定狀態的」進行開機，並強制執行嚴格的白名單 (Whitelisting)。

附註：以可設定狀態進行開機將引起某些互通性問題 (DHCP 位址延遲、Novel 網路互通性問題等)。

可使用以下指令行變數：

表格 9-1 指令行變數

指令行變數	描述	註
STDRV=stateful	NDIS 驅動程式在開機時處於全部可設定狀態。	將 NDIS 驅動程式的預設狀態從「所有開啓的」變更為「所有可設定狀態的」，在開機時允許全部網路流量，直到 Endpoint Security Client 3.5 決定其位置為止。
/qn	無訊息安裝。	使用該變數以隱藏典型 MSI 安裝程序。Endpoint Security Client 3.5 將在下次使用者重新開機時啓動。
STRBR=ReallySuppress	安裝完成後不重新開機。	在第一次重新開機前，安全性強制執行和用戶端自我防禦功能無法完全運作。
STBGL=1	應用程式控制的嚴格白名單強制執行。	您必須建立識別白名單上應用程式的規則，並且與規則一併配送名單。
STUPGRADE=1	升級 Endpoint Security Client 3.5。	在升級 Endpoint Security Client 3.5 時使用。
STUNINSTALL=1	解除安裝 Endpoint Security Client 3.5。	在解除安裝 Endpoint Security Client 3.5 時使用。
STUIP="the password"	使用密碼解除安裝	在啓用解除安裝密碼時使用。
STNMS="MS Name"	變更「管理服務」名稱。	變更 Endpoint Security Client 3.5 的「管理服務」名稱。
POLICYTYPE=1	將 Endpoint Security Client 3.5 變更為以機器為基礎的規則。	使用此變數將 MSI 安裝的 Endpoint Security Client 變更為接受以機器為基礎，而不是以使用者為基礎的規則。
POLICYTYPE=2	將 Endpoint Security Client 3.5 變更為以使用者為基礎的規則。	使用此變數將 MSI 安裝的 Endpoint Security Client 變更為接受以使用者為基礎，而不是以機器為基礎的規則。
STVA="Adapter name"	新增虛擬介面卡。	使用此變數啓動虛擬介面卡上的規則控制
/L *v c:\log.txt	開啓記錄。	使用此變數啓動安裝時的記錄。否則需要透過 Endpoint Security Client 診斷工具完成 (請參閱《管理員手冊》)。

9.2.2 與 MSI 套件一同配送規則

您可以使用企業設定的規則來取代包含在 MSI 安裝中的預設規則。若要使用 MSI 複本下推特定規則：

- 1 建立一個透過管理主控台配送給所有使用者的規則 (請參閱 《*ZENworks Endpoint Security Management 管理指南*》, 以取得與規則建立有關的詳細資訊) 。
- 2 輸出規則, 並將其儲存為 `policy.sen` 。

附註：所有使用此方法 (不受管理) 配送的規則都必須命名為 `policy.sen`, Endpoint Security Client 3.5 才會接受這些規則。Endpoint Security Client 3.5 將不會執行未以 `policy.sen` 命名的規則。

- 3 開啓規則輸出至的資料夾, 並複製 `policy.sen` 和 `setup.sen` 檔案。
- 4 瀏覽已建立的 MSI 複本並開啓 "`program files\Novell\ZENworks Security Client\`" 資料夾。
- 5 將 `policy.sen` 和 `setup.sen` 檔案貼至資料夾中。這將會取代預設的 `policy.sen` 和 `setup.sen` 檔案。

9.2.3 從 MSI 進行 Endpoint Security Client 3.5 的使用者安裝

當使用者重新驗證至領域時 (透過機器的重新開機), MSI 安裝套件將在登入之前執行。在完成 MSI 安裝之後, 系統會將機器重新開機並允許使用者登入機器。Endpoint Security Client 3.5 現已安裝並執行。

9.3 執行 Endpoint Security Client 3.5

Endpoint Security Client 3.5 會在系統啓動時自動執行。如需關於 Endpoint Security Client 3.5 的詳細資訊, 請參閱 《*ZENworks Endpoint Security Client 3.5 使用者指南*》。

您可以將 《使用者指南》 配送給所有的使用者, 以協助他們更加瞭解新端點安全性軟體的操作。

ZENworks Endpoint Security Client 4.0 安裝

10

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。您現在可以使用 3.5 版用戶端來管理 Windows XP，並用 4.0 版用戶端來管理 Windows Vista。

以下各頁將簡介基本安裝和 MSI 安裝的安裝程序。

「基本安裝」只會將 Endpoint Security Client 4.0 安裝在目前的機器上。

MSI 安裝程序將會在「管理」模式 (/a) 中啟動安裝程式，並建立軟體的 MSI 套件。您可以將此套件向下傳遞，或者在預先設定必要的使用者輸入後，在特定的網路環境中發佈。這可讓個別的使用者以預先定義的伺服器值安裝軟體。

- ◆ 「基本 Endpoint Security Client 4.0 安裝」 (第 61 頁)
- ◆ 「MSI 安裝」 (第 64 頁)
- ◆ 「執行 Endpoint Security Client 4.0」 (第 67 頁)
- ◆ 「Endpoint Security Client 4.0 中不支援的功能」 (第 67 頁)

10.1 基本 Endpoint Security Client 4.0 安裝

此程序只會在目前的機器上安裝 ZENworks Endpoint Security Client 4.0。

開始之前：

- ◆ 確認已安裝所有最新版的 Microsoft 安全性修補和防毒軟體。Endpoint Security Client 4.0 軟體可安裝在以 32 位元模式執行的 Windows Vista (執行 Support Pack 1) 與 Windows Server 2008 上。
- ◆ Novell 建議您在安裝 Endpoint Security Client 4.0 期間，關閉與有效登錄功能進行互動的防毒 / 防間諜軟體。
- ◆ 受管理的 Endpoint Security Client 需要與「ZENworks Endpoint Security 管理服務」元件進行 SSL 通訊。若在「管理服務」或「單一伺服器」安裝期間選取「自我簽署證書」，執行 Security Client 的端點必須在適當的網路位置 (最好是在本機電腦網路位置) 安裝證書。

若要自動執行此作業，請將 ESM-MS.cer 檔案放在 Endpoint Security Client 安裝程式 Setup.exe 檔案所在的資料夾。或者，您可以將整個 ESM Setup Files 資料夾從「管理服務」安裝 (或「單一伺服器」安裝) 複製到 Endpoint Security Client 安裝程式 Setup.exe 所在資料夾 (確定 ESM-MS.cert 位於 ESM Setup Files 資料夾，且資料夾名稱為 ESM Setup Files)。這會自動將證書安裝至機器 (例如，全部使用者)。您也可以對 Novell license.dat 檔案進行相同的程序。

選取「安裝介面」功能表中的適當 ZENworks Security Client 安裝程式目錄。

- 1 連按兩下 Setup.exe 開始執行安裝程序。

2 選擇安裝語言，然後按一下「確定」。

語言選項包括：

- ◆ 簡體中文
- ◆ 繁體中文
- ◆ 英文(預設值)
- ◆ 法文
- ◆ 德文
- ◆ 義大利文
- ◆ 日文
- ◆ 葡萄牙文
- ◆ 西班牙文(傳統)

3 Endpoint Security Client 4.0 要求電腦上必須安裝 Microsoft Web Services Enhancements (WSE) 2.0 (含 Service Pack 3) 與 Microsoft Visual C++ 2008，才能安裝用戶端。若安裝程序未偵測到這些元件，您將會看到此畫面。按一下「安裝」安裝這些必要元件。

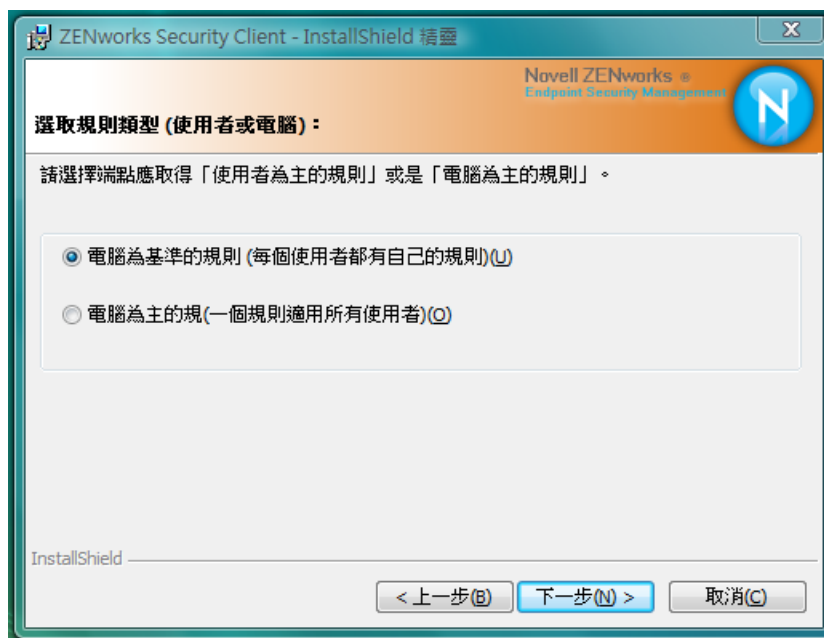
4 若尚未執行此動作，請先關閉防毒軟體與防間諜軟體，然後再按一下「歡迎」畫面上的「下一步」。

5 接受授權合約，然後按一下「下一步」。



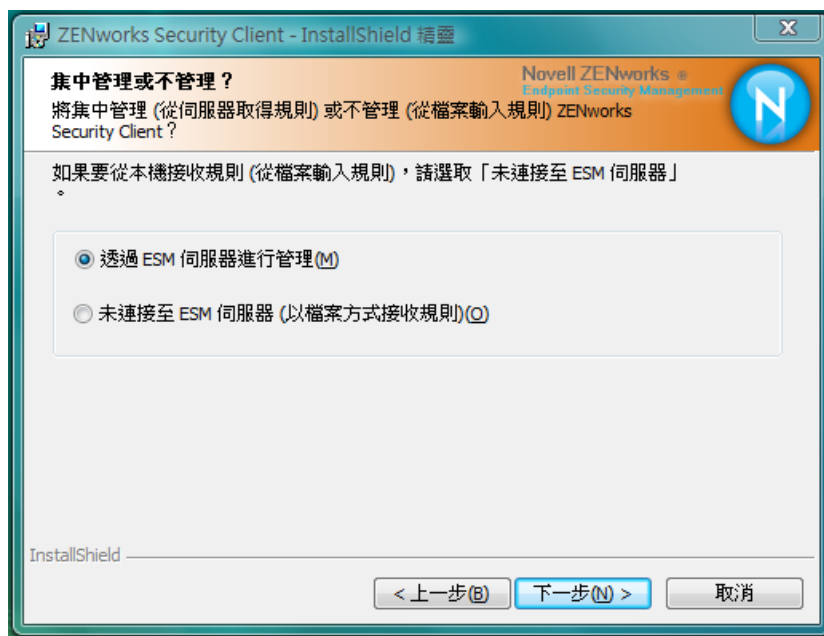
6 選取「需要解除安裝密碼」。這可避免使用者解除安裝 Endpoint Security Client 4.0 (建議使用)。

7 新增解除安裝密碼並確認密碼，然後按一下「下一步」。



- 8 選取規則類型 (「使用者為基準的規則」，其中每個使用者都有個別的規則；或「電腦為基準的規則」，其中每個規則適用於所有使用者)。按一下「下一步」。

附註：如果您的網路使用 eDirectory 做為「目錄服務」，請選取「使用者為基準的規則」。eDirectory 不支援以電腦為基準的規則。



- 9 選取如何接收規則 (受管理方式是對於受管理用戶端透過 ESM 伺服器接收，或對於未受管理 (獨立) 組態則從本機取回)。按一下「下一步」。

如需未受管理安裝的詳細資訊，請參閱第 11 章「ZENworks Endpoint Security Management 安裝」(第 69 頁)。

- 10 (選擇性) 若選取**步驟 9** 中的「*透過ESM 伺服器管理*」，請輸入支援「管理」服務之伺服器的名稱。

您輸入的伺服器名稱必須符合在信任的根證書 (用於安裝「ZENworks Endpoint 管理服務」或「單一伺服器」的伺服器) 提供的「發給」名稱。這可以是執行「ZENworks Endpoint 管理服務」元件之伺服器的 NETBIOS 名稱或完全合格的領域名稱 (FQDN)。輸入後，請按一下「*下一步*」。

- 11 按一下「*安裝*」開始安裝。

- 12 安裝軟體之後，當系統提示時請重新啓動機器。

如需 4.0 Client for Vista 不支援之功能的清單，請參閱「**Endpoint Security Client 4.0 中不支援的功能**」(第 67 頁)。

10.2 MSI 安裝

此程序會為 Endpoint Security Client 4.0 建立 MSI 套件。系統管理員可使用此套件透過 Active Directory 規則或其他軟體配送方法將安裝發佈到使用者群組。

- 「**使用主安裝程式**」(第 64 頁)
- 「**使用 Setup.exe 檔案**」(第 64 頁)
- 「**完成安裝**」(第 65 頁)
- 「**指令行變數**」(第 66 頁)
- 「**與 MSI 套件一同配送規則**」(第 67 頁)

10.2.1 使用主安裝程式

如果您要從 CD 或 ISO 主安裝程式進行安裝，且不需要執行任何指令行變數：

- 1 插入 CD 並等待主安裝程式啓動。
- 2 按一下「*產品安裝*」。
- 3 按一下「*Security Client*」。
- 4 按一下「*建立 ZSC MSI 套件*」。
- 5 請繼續執行「**完成安裝**」(第 65 頁)。

10.2.2 使用 Setup.exe 檔案

若只使用 setup.exe 檔案來安裝：

- 1 在 setup.exe 上按一下滑鼠右鍵。
您可以在 CD 的 D:\ESM32\ZSC 下找到這個可執行檔：
- 2 選取「*建立捷徑*」。
- 3 在捷徑上按一下滑鼠右鍵，然後按一下「*內容*」。
- 4 在「*目標*」欄位結尾的引號後方，按下空白鍵插入空格，然後輸入 /a。
例如："C:\Documents and Settings\user\Desktop\CL-Release-3.2.455\setup.exe" /a
有數個指令行變數可用於 MSI 安裝。請參閱「**指令行變數**」(第 57 頁)，以取得詳細資料。

- 5 按一下「確定」。
- 6 連按兩下捷徑以啟動 MSI 安裝程式。
- 7 請繼續執行「完成安裝」(第 65 頁)。

10.2.3 完成安裝

完成 [使用主安裝程式](#) 或 [使用 Setup.exe 檔案](#)，然後使用此程序來完成用戶端安裝。

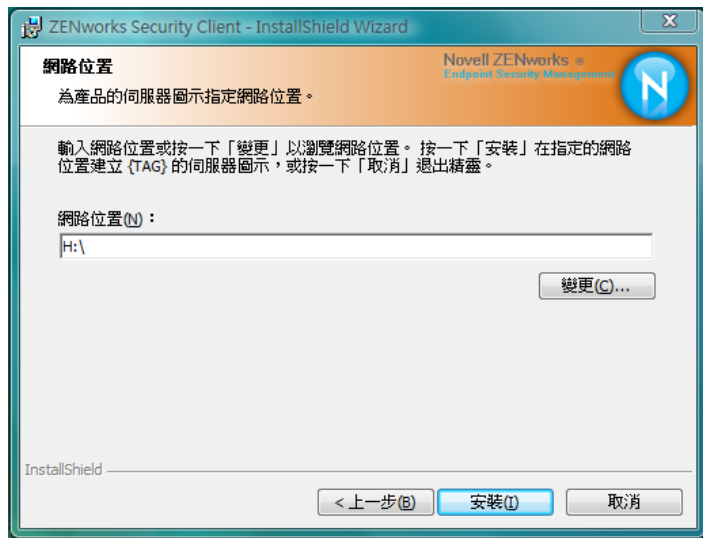
- 1 按一下「歡迎」畫面中的「下一步」以繼續。
- 2 選取「需要解除安裝密碼」(建議)，並輸入密碼。按一下「下一步」。

附註：若透過 MSI 套件解除安裝 Endpoint Security Client，您必須透過 MSI 屬性指定解除安裝密碼(請參閱[表格 10-1 頁上 66](#))。

- 3 選取規則類型(「使用者為基準的規則」，其中每個使用者都有個別的規則；或「電腦為基準的規則」，其中每個規則適用於所有使用者)。按一下「下一步」。

附註：如果您的網路使用 eDirectory 做為「目錄服務」，請選取「使用者為基準的規則」。eDirectory 不支援以電腦為基準的規則。

- 4 選取如何接收規則(受管理方式是對於受管理用戶端透過 ESM 伺服器接收，或對於未受管理(獨立)組態則從本機取回)。
- 5 (選擇性)若選取[步驟 4](#)中的「透過 ESM 伺服器進行管理」：
 - 您輸入的伺服器名稱必須符合在信任的根證書(用於安裝「ZENworks Endpoint 管理服務」或「單一伺服器」的伺服器)提供的「發給」名稱。這可以是執行「ZENworks Endpoint 管理服務」元件之伺服器的 NETBIOS 名稱或完全合格的領域名稱(FQDN)。
- 6 (選擇性)在提供的欄位中輸入電子郵件地址，以在安裝失敗時通知您。
- 7 指定要建立 MSI 複本的網路位置，或按一下「變更」按鈕瀏覽並選取位置。



- 8 按一下「安裝」建立 MSI 複本。按一下「完成」關閉安裝程式。

- 9 瀏覽至已建立 MSI 複本的位置，並開啓 \Program Files\Novell ZENworks\Endpoint Security Client\ 資料夾。
- 10 將「管理服務」SSL 證書 (ESM-MS.cer 或企業證書) 和 Novell 授權金鑰複製至此資料夾，以取代目前位於資料夾中的預設 0 KB 檔案。
- ESM-MS SSL 證書位於 ZENworks Endpoint Security Management Setup Files 資料夾中。授權金鑰是以電子郵件個別寄發。若您使用 60 天試用版，則目前不需要授權金鑰。

10.2.4 指令行變數

指令行變數選項可用於 MSI 安裝。可執行檔捷徑是設為在管理員模式中執行，而這些變數必須在其中進行設定。若要使用變數，您必須在 MSI 捷徑中輸入以下指令行：

"...\setup.exe" /a /V"variables"。在兩個引號之間輸入以下任何指令。請使用單個空格分隔多個變數。

可使用以下指令行變數：

表格 10-1 指令行變數

指令行變數	描述	註
/qn	無訊息安裝。	隱藏典型 MSI 安裝程序。Endpoint Security Client 將在下次使用者重新開機時啟動。
SESMMSG=1	顯示訊息通知終端使用者若已部署「加密規則」，則「安全庇護」中的檔案無法自動移除加密。	預設值是 0 (不顯示訊息)，讓解除安裝程序以「靜音」模式進行。
STRBR=ReallySuppress	安裝完成後不重新開機。	在第一次重新開機前，安全性強制執行和用戶端自我防禦功能無法完全運作。
STUPGRADE=1	升級 Endpoint Security Client 4.0。	升級 Endpoint Security Client 4.0。
STUNINSTALL=1	解除安裝 Endpoint Security Client 4.0。	解除安裝 Endpoint Security Client 4.0。
STUIP="the password"	使用密碼解除安裝	在啟用解除安裝密碼時使用此變數。
STNMS="MS Name"	變更「管理服務」名稱。	變更 Endpoint Security Client 4.0 的「管理服務」名稱。
POLICYTYPE=1	將 Endpoint Security Client 4.0 變更為以機器為基礎的規則。	變更以 MSI 方式安裝的 Endpoint Security Client，接受以機器為基礎的規則，而非以使用者為基礎的規則。
POLICYTYPE=2	將 Endpoint Security Client 4.0 變更為以使用者為基礎的規則。	變更以 MSI 方式安裝的 ZENworks Security 4.0 Clients for Vista，接受以使用者為基礎的規則，而非以機器為基礎的規則。
STVA="Adapter name"	新增虛擬介面卡。	啟動虛擬介面卡上的規則控制
/L *v c:\log.txt	開啓記錄。	啟動安裝記錄功能。若未使用此變數，則必須透過 Endpoint Security Client 診斷工具來進行記錄。

10.2.5 與 MSI 套件一同配送規則

您可以使用企業設定的規則來取代包含在 MSI 安裝中的預設規則。若要使用 MSI 複本下推特定規則：

- 1 建立一個透過管理主控台配送給所有使用者的規則 (請參閱 《*ZENworks Endpoint Security Management 管理指南*》, 以取得與規則建立有關的詳細資訊)。
- 2 輸出規則, 然後將它重新命名為 policy.sen。
所有使用此方法 (不受管理) 配送的規則都必須命名為 policy.sen, Endpoint Security Client 4.0 才會接受這些規則。Endpoint Security Client 4.0 將不會執行未以 policy.sen 命名的規則。
- 3 開啓規則輸出至的資料夾, 並複製 policy.sen 和 setup.sen 檔案。
- 4 瀏覽已建立的 MSI 複本, 並開啓 \Program Files\Novell ZENworks\Endpoint Security Client\ 資料夾。
- 5 將 policy.sen 和 setup.sen 檔案貼至資料夾中。這將會取代預設的 policy.sen 和 setup.sen 檔案。

10.3 執行 Endpoint Security Client 4.0

Endpoint Security Client 4.0 會在系統啓動時自動執行。如需關於 Endpoint Security Client 4.0 的詳細資訊, 請參閱 《*ZENworks Endpoint Security Client 4.0 使用者指南*》。

您可以將 《使用者指南》 配送給所有的使用者, 以協助他們更加瞭解新端點安全性軟體的操作。

10.4 Endpoint Security Client 4.0 中不支援的功能

Endpoint Security Client 4.0 不支援的功能或部分支援的功能包括：

- ◆ 用戶端自我防禦。
- ◆ 數據機支援。
- ◆ 程序檔。
- ◆ 手動變更某位置的防火牆。
- ◆ 讓某位置可看到多個防火牆。只有預設防火牆可以使用。
- ◆ 完整性規則。
- ◆ 封鎖應用程式。
- ◆ 滑鼠移到通知區域圖示上顯示的資訊已變更。圖示只會顯示「規則」與「位置」資訊。
- ◆ USB 連接性。
- ◆ Wi-Fi 金鑰管理。
- ◆ 有線連線的評價沒有比無線連線的評價高。
- ◆ Endpoint Security Client 更新 (依規則)。
- ◆ VPN 驗證逾時。

- ◆ 儲存裝置的自動播放控制。
- ◆ 網路環境中的電話簿項目。

ZENworks Endpoint Security Management 安裝

11

企業可以在「不受管理」的模式中執行 ZENworks® Security Client 和「管理主控台」（不需要連接「規則配送服務」或「管理服務」）。此安裝選項主要目的在於設定簡易評估。此選項也適用於伺服器空間不足，或只需要基本安全性的企業。不過此組態將無法使用快速規則更新和「規範報告」。

11.1 不受管理的 Endpoint Security Client 安裝

若要安裝不受管理的 Endpoint Security Client，請遵循 [第 9 章「Endpoint Security Client 3.5 安裝」](#)（第 53 頁）中的指示，並選取「未連接至 ZENworks Endpoint Security Management 伺服器（以檔案方式接收規則）」選項。此安裝會略過關於伺服器名稱的問題，並將 Endpoint Security Client 安裝在此機器上（系統也會建立不受管理 Endpoint Security Client 的 MSI 套件）。

圖 11-1 選取「未連接至 ZENworks Endpoint Security Management 伺服器」



11.2 獨立管理主控台

此組態可讓您不需要連接外部「管理服務」，或透過「規則配送服務」配送規則，便可安裝「ZENworks Endpoint Security Management 管理主控台」並建立規則。請在主安裝程式功能表中選取「獨立管理主控台安裝」，並遵循 [第 7 章「執行管理主控台安裝」](#)（第 39 頁）的指示以進行安裝。

在安裝程序開始時，會先安裝 SQL 資料庫（如果機器上已存在資料庫，安裝程式將設定適當的資料庫）。在安裝資料庫後，安裝將會停止。您必須將機器重新開機以啟動 SQL 資料庫。在重新開機後，請再次啟動安裝程序以繼續執行。

除了「報告」功能以外，您可以使用大部分的規則功能進行部署。您必須將輸出的規則檔案配送至 Endpoint Security Client 的 \Program Files\Novell\ZENworks Security Client\ 目錄。

11.3 配送不受管理的規則

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《*ZENworks Endpoint Security Management 管理指南*》）。
- 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為 `policy.sen`，Endpoint Security Client 才會接受這些規則。
- 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。
`Setup.sen` 只需要與第一個規則一起複製到不受管理的設備中。之後只需要配送新的規則。

如果不受管理的 Endpoint Security Client 安裝在與「獨立管理主控台」相同的機器中，則 `Setup.sen` 檔案也必須複製至 `\Program Files\Novell\ZENworks Security Client\` 目錄中。如果機器上的不受管理 Endpoint Security Client 是在「獨立編輯器」之後安裝，則必須依照上述手動傳送該檔案。

按一下「發行」按鈕會立即將規則發行至該機器的不受管理 Endpoint Security Client。若要將規則提供給多個不受管理的使用者，請依照上述說明，使用「輸出」功能。

文件更新

A

本節包含 3.5 版初版之後此《Novell ZENworks Endpoint Security Management 安裝指南》之文件內容變更的相關資訊。變更是依發行日期列出。

本產品的文件以 HTML 和 PDF 兩種格式提供，可從網路上下載。HTML 和 PDF 文件將保持最新，因此也包含本節所列之變更。

若想知道您所使用的 PDF 文件是否最新，可以查看標題頁上的發佈日期。

文件已在下列日期更新：

- 「2009 年 1 月 5 日」(第 71 頁)

A.1 2009 年 1 月 5 日

對以下小節進行了更新：

位置	更新
所有章節	整份指南中的用戶端名稱已變更。現在它的正式名稱是 Novell ZENworks Endpoint Security Client。在其對應的章節中，用戶端稱為 Endpoint Security Client 3.5 (適用於 Windows XP) 與 Endpoint Security Client 4.0 (適用於 Windows Vista)。
「系統需求」(第 10 頁)	加入新 Vista 用戶端與獨立型「管理主控台」的系統需求。
第 9 章「Endpoint Security Client 3.5 安裝」(第 53 頁)	加入資訊與名稱變更，指示 Endpoint Security Client 3.5 是適用於 Windows XP。
第 10 章「ZENworks Endpoint Security Client 4.0 安裝」(第 61 頁)	加入 Endpoint Security Client 4.0 (適用於 Windows Vista) 章節。