

NOD32 防病毒系統企業版

安裝及使用手冊



目錄

序言	2
安裝	3
1 · 安裝更新伺服器	4
2 · 安裝遠端管理伺服器	14
3 · 創建安裝包	22
4 · 推送安裝示例	25
5 · 推送安裝問題解析	32
6 · 其他安裝方法示例	38
7 · 如何把單機加入管理	42
配置	
8. 大型電腦網路與同步	49
9. 連接到 RAS 伺服器	50
10 RAS 伺服器設置	51
11. RAC 控制台設置	53
12. 網路活動總覽	55
RAC 控制台的具體細節	58
13. 任務	60
14. 報告	62



序言

NOD32 企業版包括四個部分：遠端管理伺服器，遠端管理控制台，局域網絡更新伺服器，NOD32 防毒系統工作站。NOD32 遠端管理伺服器與 NOD32 遠端管理控制台是為了在大型電腦網絡環境下管理 NOD32 防病毒解決方案而設計的專用工具。通過 NOD32 遠端管理伺服器與 NOD32 遠端管理控制台，你可以觀察到每一個工作站上 NOD32 防病毒活動、病毒入侵情況以及你的網絡上所有電腦的 NOD32 系統更新情況。NOD32 遠端管理伺服器（以下簡稱 RAS）記錄了網絡上所有電腦中的 NOD32 防病毒系統的所有資訊，而且這些資訊可以通過 NOD32 遠端管理控制台（以下簡稱 RAC）獲得。通過 RAC 與網絡上工作站和伺服器中的 NOD32 防病毒系統互動，使得管理員可以使用網絡上的個人電腦遠端操作 NOD32 管理工具。



安裝

遠端安裝可以讓你通過自己的工作站在遠端工作站上安裝 NOD32 防病毒系統，而無須在遠端工作站上進行手動安裝。

基本來說，有兩類 Windows 作業系統。第一種包括 Windows 95、98 和 Me，第二種包括 Windows NT 4.0、2000、XP 和 Windows 2003 server。針對上述兩種 Windows 作業系統，有不同的遠端安裝程式。在 Windows NT 4.0、2000、XP 和 2003 server 中安裝 NOD32 防病毒系統，需要採用“推送安裝”程式。

假設我們面對一個由 50 台個人電腦(PC)組成的單一區域網路，每台機器裝有 Windows 98、Windows 2000 或 Windows XP 作業系統，並且沒有任何防病毒系統。我們希望從零開始，在上述電腦上安裝 NOD32 防病毒系統。本章節將示範如何安裝 NOD32 中央管理安裝包 (企業版)，內容主要包含 7 部份：

- 1． 如何建立更新伺服器
- 2． 如何建立遠端管理伺服器
- 3． 如何建立安裝包
- 4． 推送安裝示例
- 5． 推送安裝問題解析
- 6． 其他安裝方法示例
- 7． 如何把單機加入管理

注意：1.除非你有特殊原因，否則建議你使用本文所述的安裝順序。

2.本手冊全部以 NOD32 繁體中文 2.7 版為示例，如果你使用的是其他版本，請做出相應更改。

安裝更新伺服器

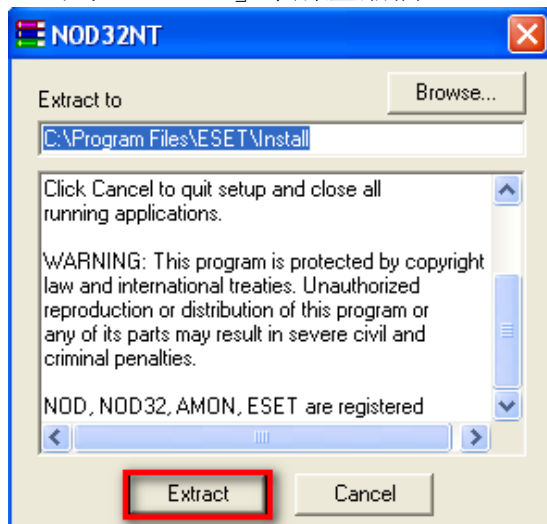
關於更新伺服器:

1. 更新伺服器可以安裝於 windows 95 或以上系統, 不一定要安裝在伺服器版本的 windows 上。
2. 更新伺服器已包含防毒模組, 故更新伺服器無需另外安裝 NOD32 標準用戶版本。
3. 更新伺服器本身必須能連接到互聯網, 從 NOD32 的伺服器下載病毒定義檔後, 可以將病毒定義分發給你的網絡上的其他電腦。

1. 雙擊光碟中的 **ndntcsad.exe** 檔來安裝。



2. 點擊「**Extract**」來解壓縮檔。

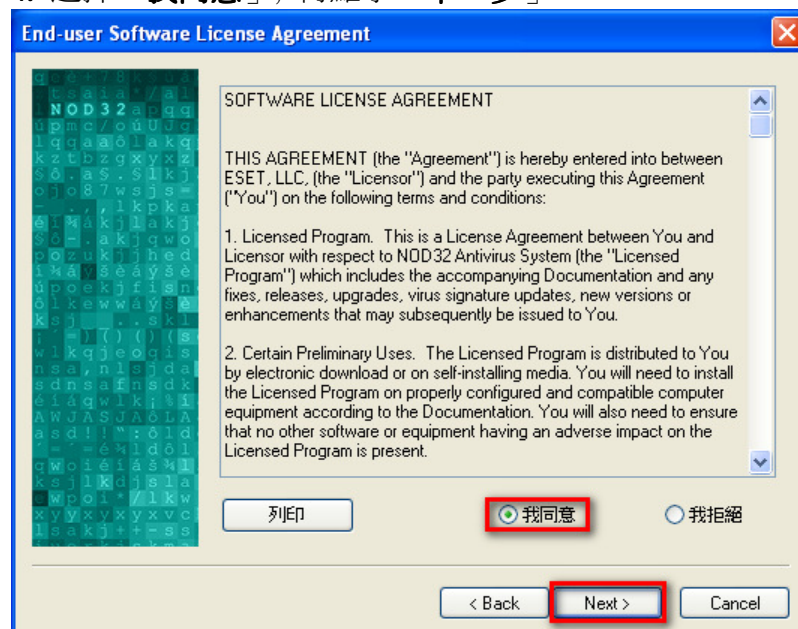




3. 點擊「下一步」



4. 選擇「我同意」，再點擊「下一步」





5. 輸入你的使用者名稱和密碼，再點擊「下一步」

自動更新設定

NOD32防毒系統自動更新需要正確的使用者名稱及密碼。請於網上登記或諮詢零售商/代理商

伺服器:
<自動選擇>

使用者名稱: AV-1234567 密碼:

以後再輸入使用者及密碼(不建議使用), 選擇以下方格

☐ 以後再設定更新參數

< Back Next > Cancel

6. 點擊「下一步」

網際網絡連線

請根據你的網際網絡連線設定代理伺服器和使用名稱, 或詢問系統管理員

☐ 我使用撥號連線(數據機)

代理伺服器

☒ 我不知道有沒有使用代理伺服器。我希望使用與Internet Explorer相同的設定。

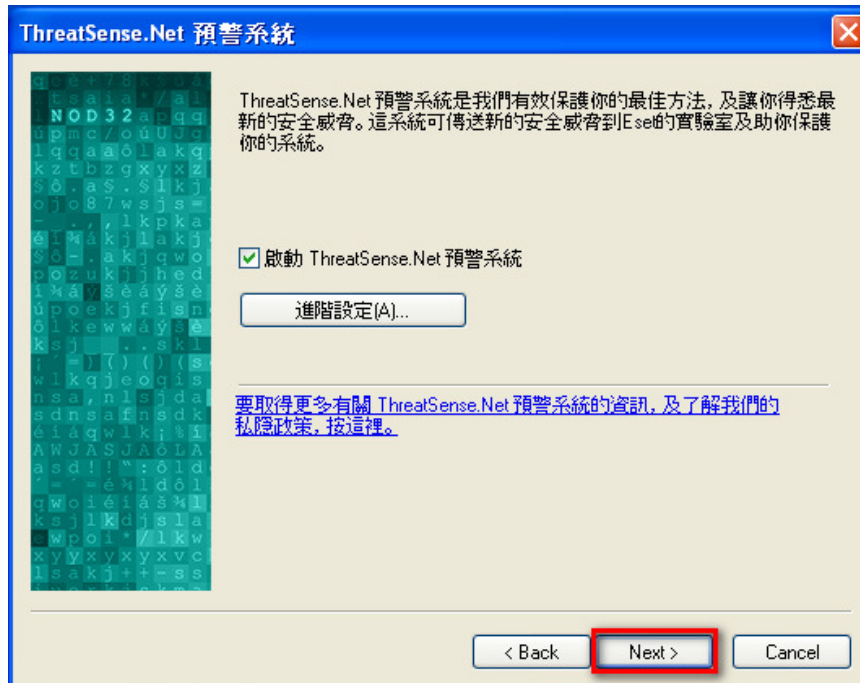
☐ 我不使用代理伺服器

☐ 我使用代理伺服器

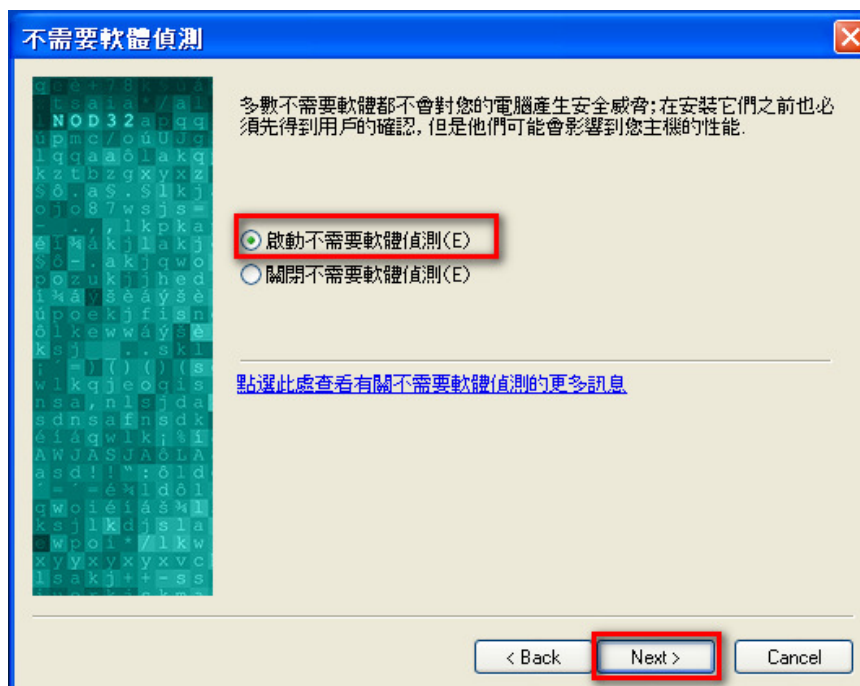
< Back Next > Cancel



7. 點擊「下一步」

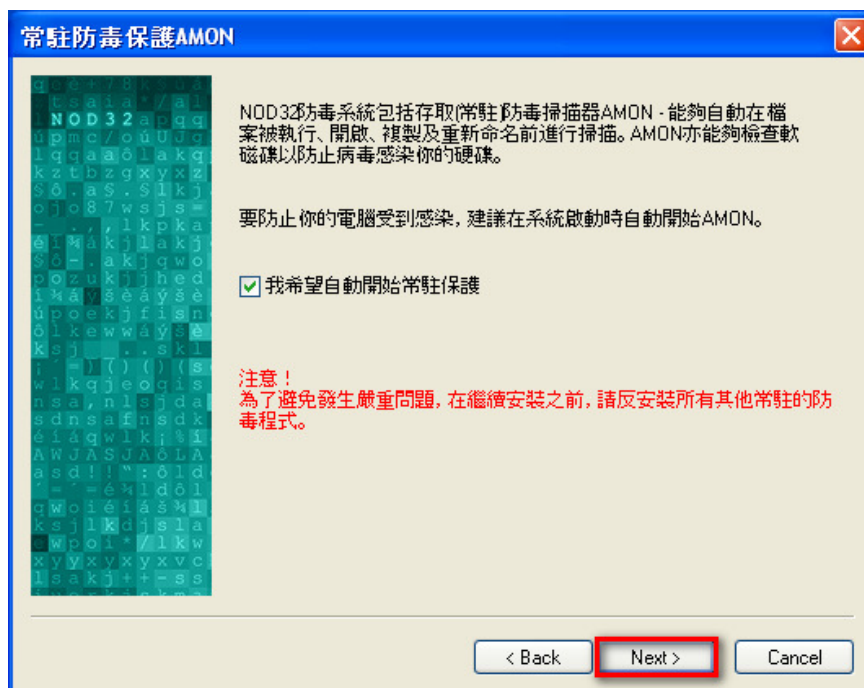


8. 我們會建議選擇**啟動不需要軟體偵測**，點擊「下一步」





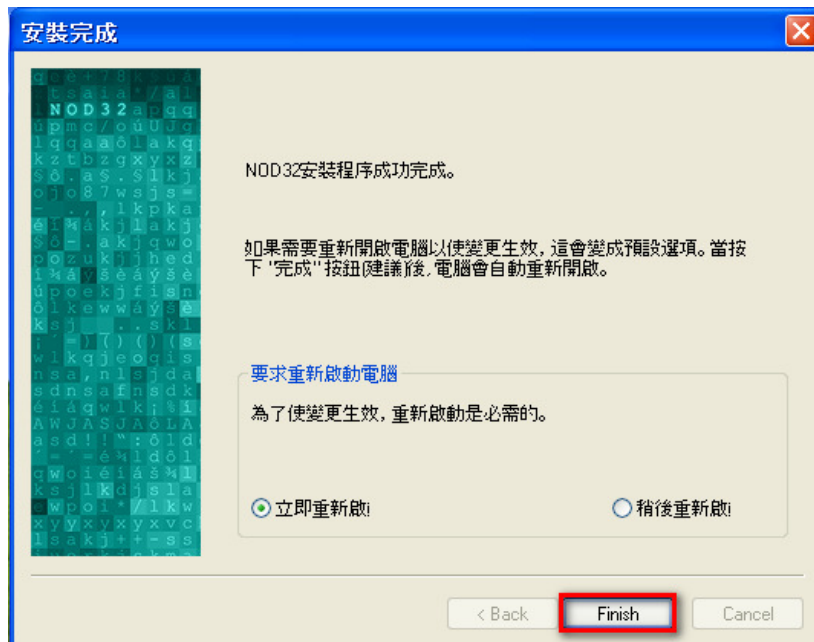
9. 點擊「下一步」



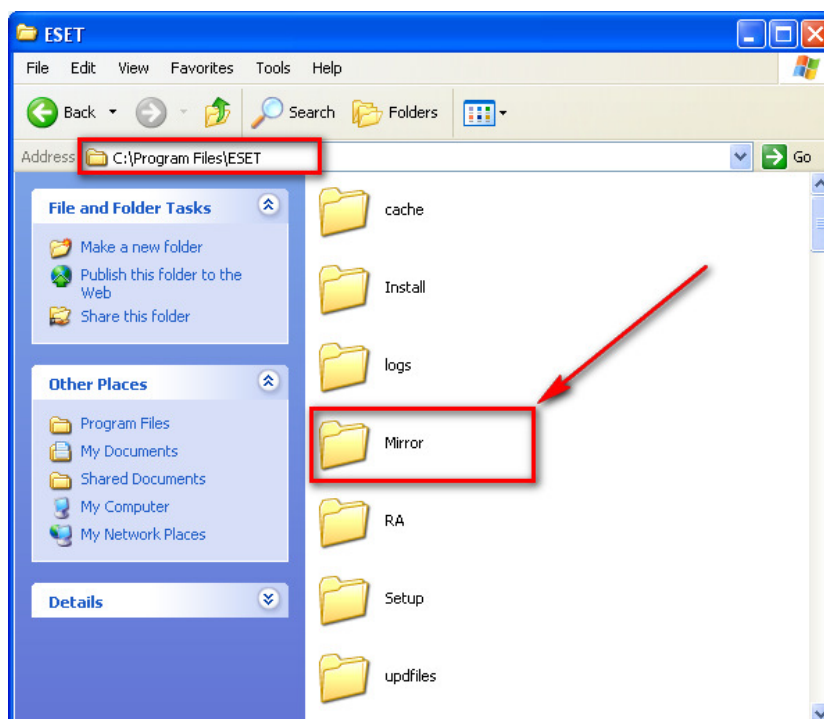
10. 點擊「下一步」



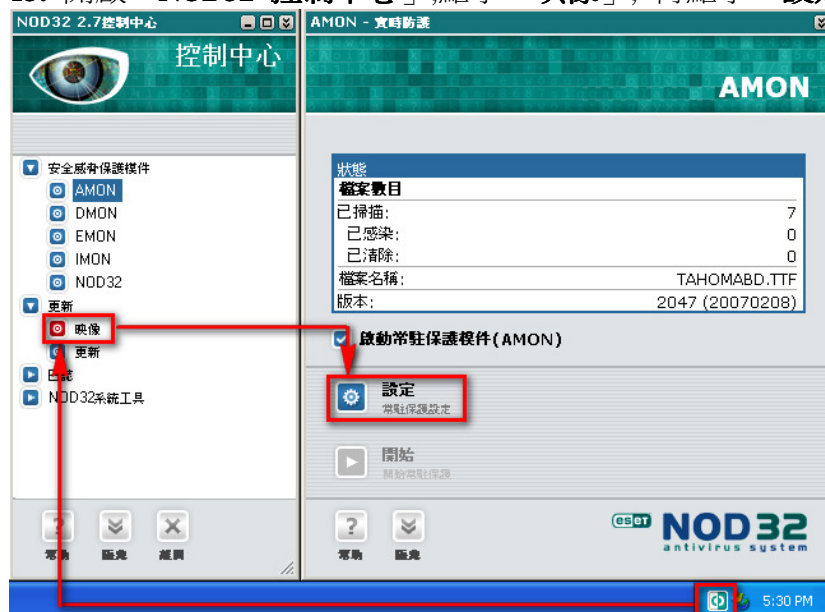
11. 點擊「完成」來重新啟動電腦



12. 在「C:\Program Files\ESET」新建一個「Mirror」檔夾



13. 開啟「NOD32 控制中心」, 點擊「映像」, 再點擊「設定」



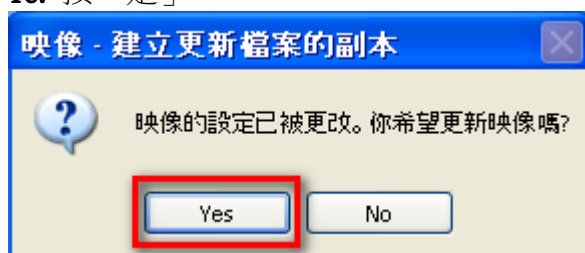
14. 先勾選「建立更新映像」, 再按圖作設定



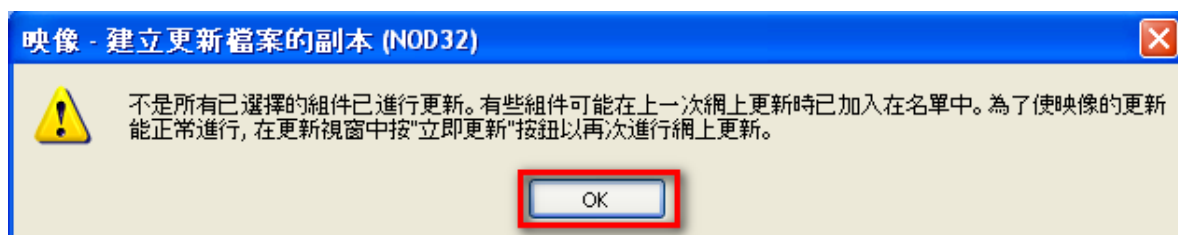
15. 如果你的網絡中安裝了英文版的 NOD32, 請按「顯示所有語言版本」, 並勾選相應的語言版本。



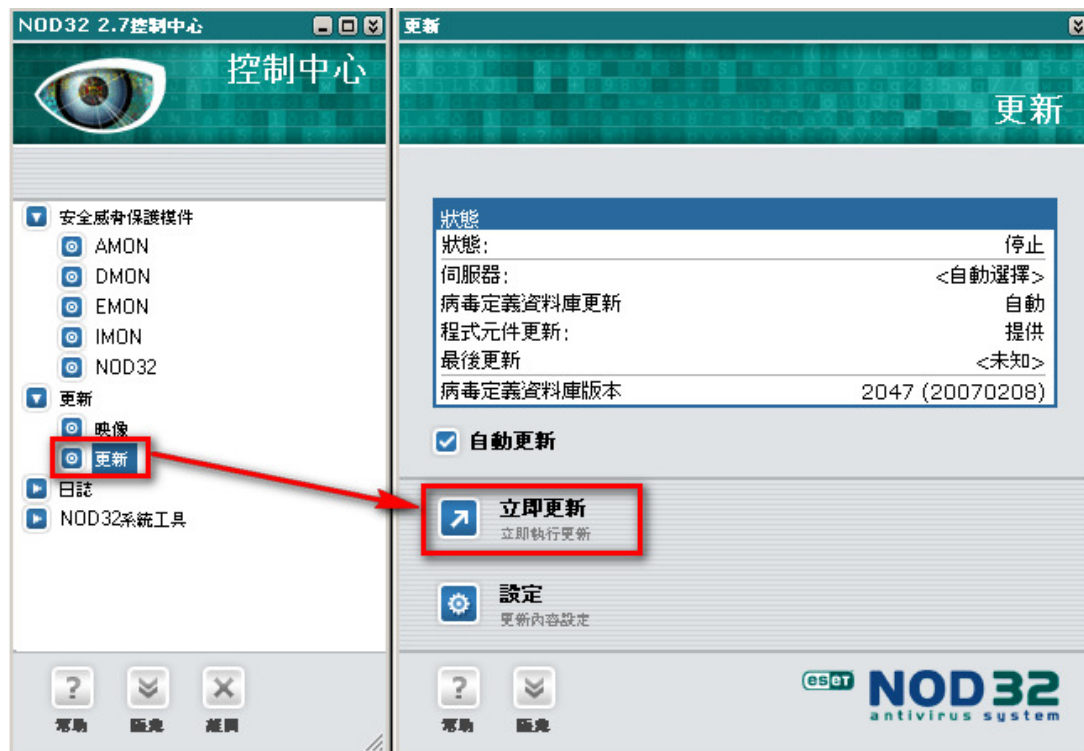
16. 按「是」



17. 按「確定」



18. 按「更新」，再按「立即更新」

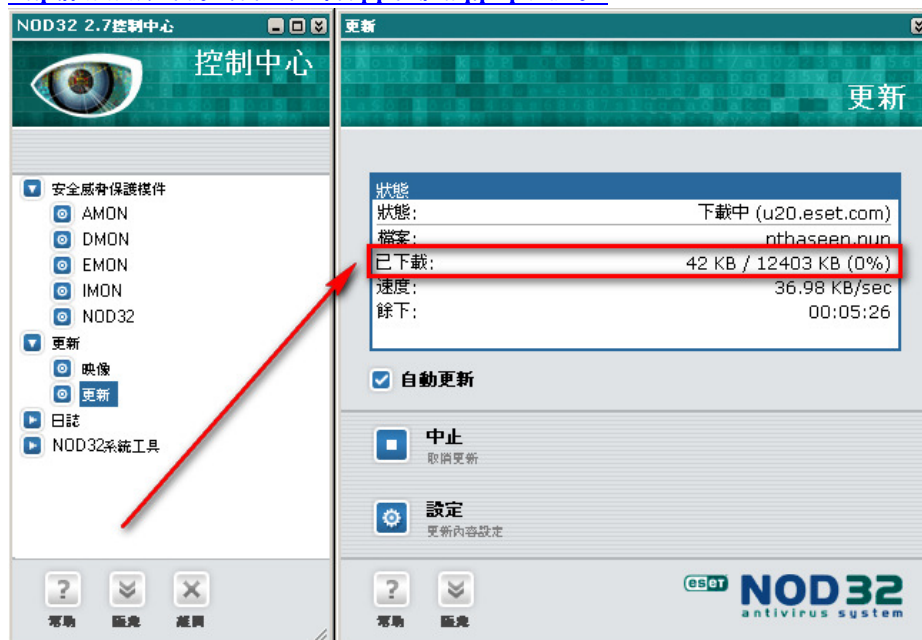


19. 按「是」，為其他作業系統下載模組更新

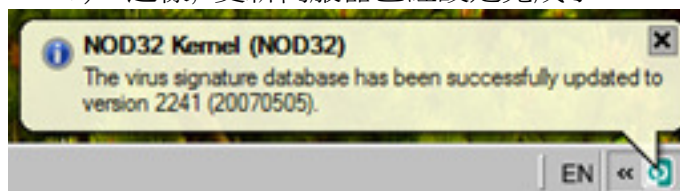


20. 如果你輸入了正確的使用者名稱和密碼，會看見下載進度。如果你發現彈出提示輸入使用者名稱和密碼，請參閱

<http://www.nod32.com.hk/support/faq.php?id=32>



21. 等一會兒，你會看到更新完成通知(例:病毒定義資料已成功更新到 Version 2241.)。這樣，更新伺服器已經設定完成了。



到此,我們已經成功建立了更新伺服器,請繼續閱讀下一章節完成企業版的安裝



安裝遠端管理伺服器

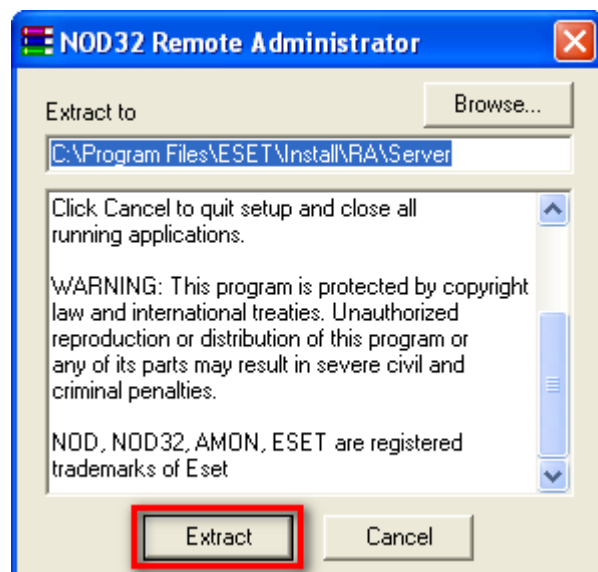
關於遠端管理伺服器:

1. 除非你有特殊原因, 否則建議你把遠端管理伺服器, 遠端管理控制台及更新伺服器的安裝在同一台電腦上, 以方便日後的管理。
2. 遠端管理伺服器可以讓你同時把 NOD32 安裝到多台電腦、修改多台電腦的設定及監視多台電腦的狀態, 可以大大增加系統管理員的效率。

1. 請先安裝遠端管理伺服器, 雙擊其安裝文件 (**rasrvnten.exe**) 開始安裝。

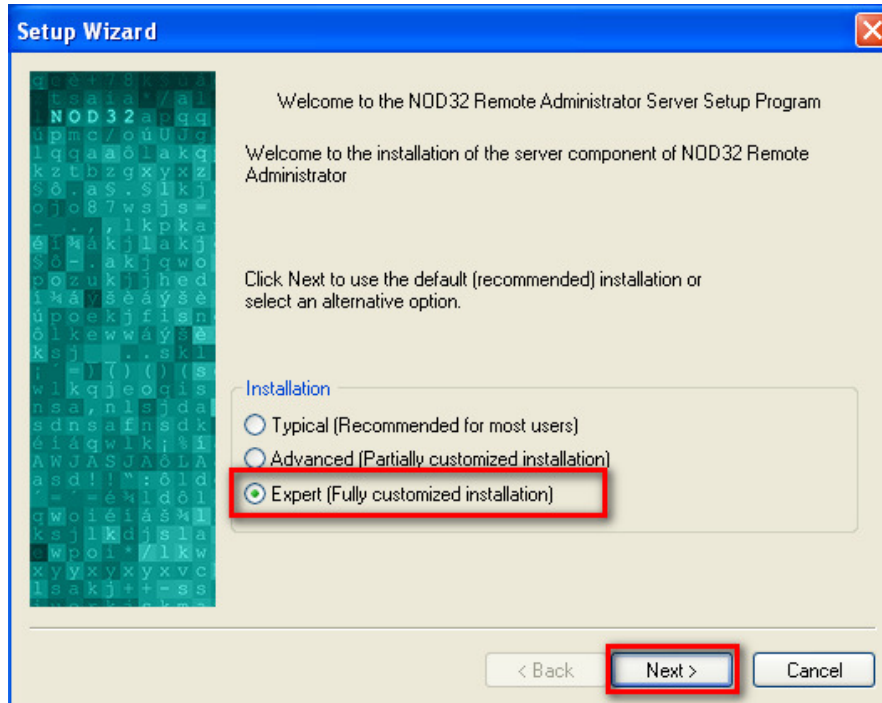


2. 按「Extract」來解壓縮檔案

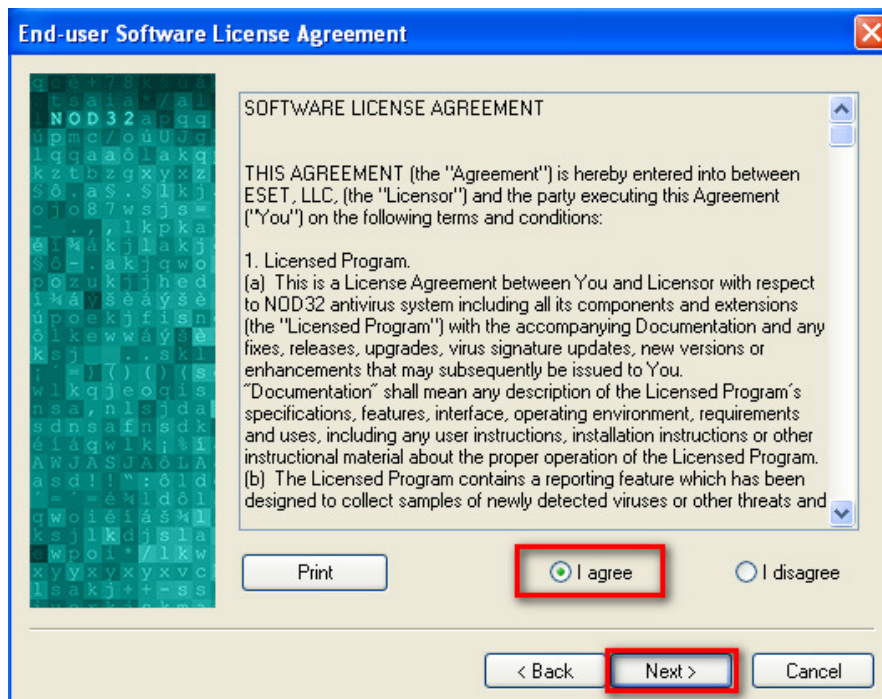




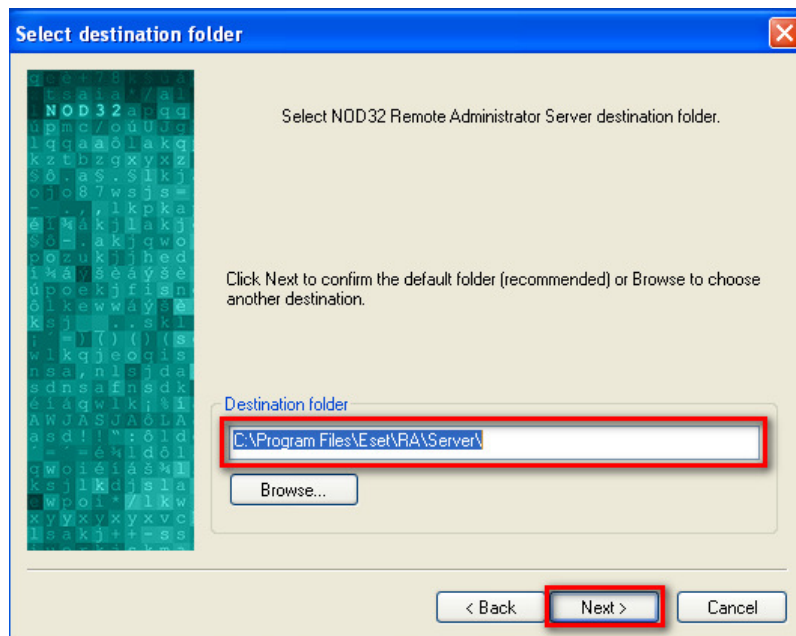
3. 選擇「Expert (Fully customized installation)」(專家), 按「下一步」



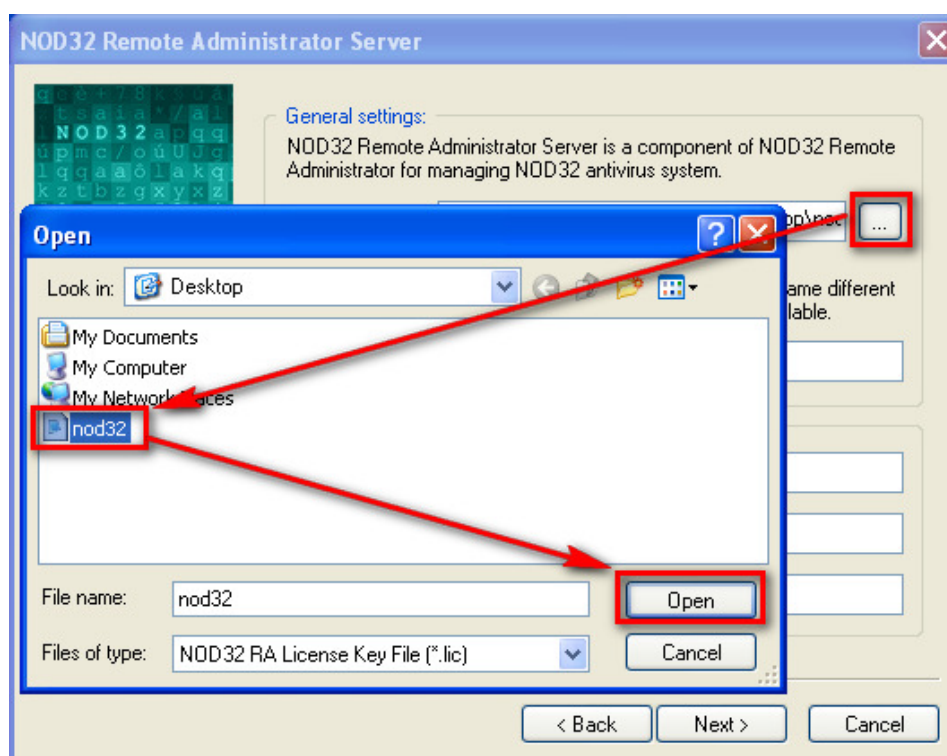
4. 選擇「I agree」, 按「下一步」



5. 安裝位置選擇 ,按「下一步」



6. 選擇使用權證檔案, 它可能在你的 NOD32 光碟中, 也可能是我們電郵給你的。注意該檔案的副檔名是「.lic」, 至於檔案名稱並不重要。





7. 請輸入遠端管理伺服器的「IP 地址」，而不是「電腦名稱」，否則遠端管理伺服器可能不能正常運作。

NOD32 Remote Administrator Server

General settings:
NOD32 Remote Administrator Server is a component of NOD32 Remote Administrator for managing NOD32 antivirus system.

License key file: Documents and Settings\user\Desktop\nod32.lic

Warning: Specify a server name only if you need to use a name different from hostname. In this case, some features may not be available.

Server name: 192.168.2.123

SMTP settings:

Server:

Sender address:

User name: Password:

< Back Next > Cancel

8. 請按「下一步」。

NOD32 Remote Administrator Server

Automatic database cleanup

Clean up unrelated data every 20 minutes

Default

Perform automatic compression and repair of main database:

☒ Periodically, every 30 Days

Start at: 23:00

While compressing database, the server switches to maintenance mode and does not serve the clients in the meantime. This task is therefore usually scheduled during the night.

☒ Enable automatic compact & repair

Default

< Back Next > Cancel



9. 請按「下一步」

NOD32 Remote Administrator Server

There are several tasks that can be performed by regular database maintenance.

☐ Only keep the last 1000 alerts for each client warning: this may affect report statistics

☐ Only keep the last 10 events for each client

☐ Only keep the last 10 scan logs for each client

☒ Delete clients when not connected for 6 Months

This setting enables you to delete clients, fulfilling specified criteria, from the list.

☒ Delete alert logs older than 6 Months

☒ Delete event logs older than 6 Months

☒ Delete scan logs older than 6 Months

Default

< Back **Next >** Cancel

10. 請按「下一步」

NOD32 Remote Administrator Server

Replication "to" settings:

Check replicate "to" if you want to replicate this server to replicate to some upper server. Check replicate "from" and set allowed servers if you want to allow some servers to replicate data to this server.

☐ Enable "to" replication Port 2846

Upper server

Replicate every 10 minutes

☒ Replicate alert log ☐ Including details

☒ Replicate event log ☐ Including details

☒ Replicate scan log ☐ Including details

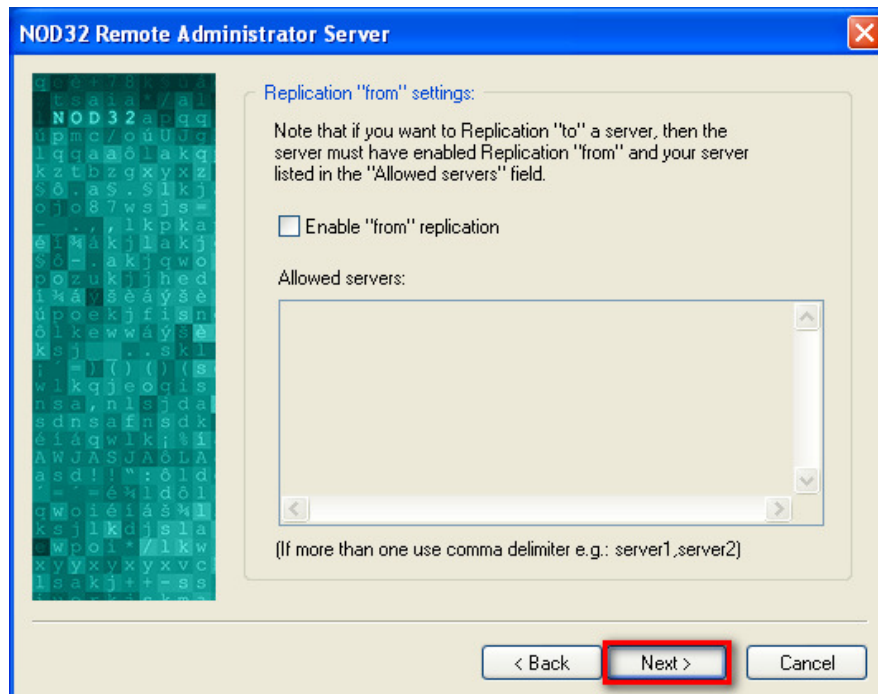
☒ Automatically replicate client configuration

Default

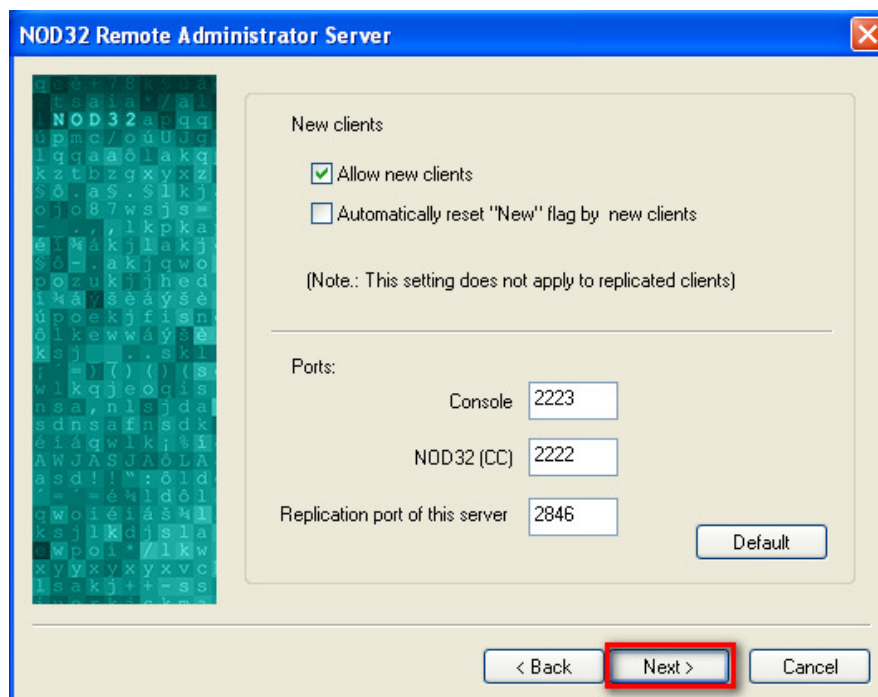
< Back **Next >** Cancel



11. 請按「下一步」



12. 這裡是設置埠位設定, 但一般會根據原先的設定.然後請按「下一步」





13. 請按「下一步」

NOD32 Remote Administrator Server

☒ Enable logging

☒ Log to Text file

Text Log Filename:

Text Log verbosity:

Rotate when larger than: MB

☐ Log to OS Application Log

Application Log verbosity:

☐ Database Debug Log (recommended is off)

Database Log Filename:

Rotate when larger than: MB

Default

< Back **Next >** Cancel

14. 要完成設置及儲存所有設定，請按「下一步」

Setup configuration complete

The setup configuration is now complete.

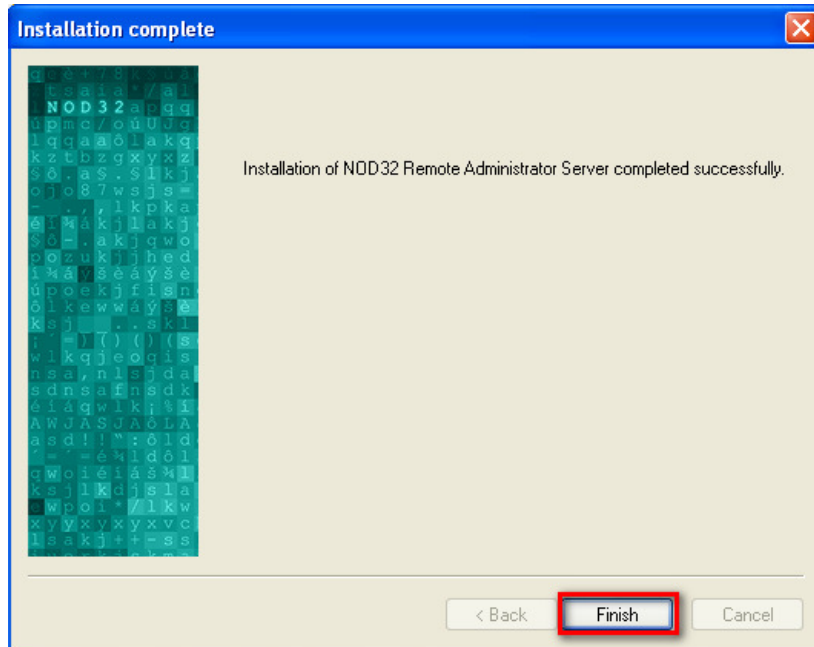
To change the configuration, click Back.

If you are happy with the configuration click Next to complete installation.

< Back **Next >** Cancel



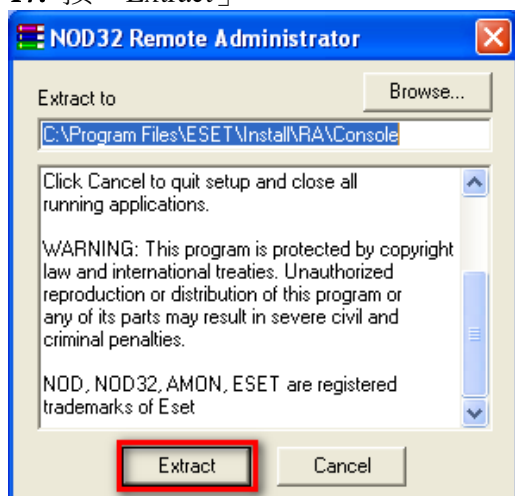
15. 按「完成」



16. 現在，我們將安裝遠端管理控制台(**raconsnten.exe**)，它是遠端伺服器的控制面板。如果你有需要，也可在其他電腦（例如是系統管理員的筆記本電腦）安裝遠端管理控制台。

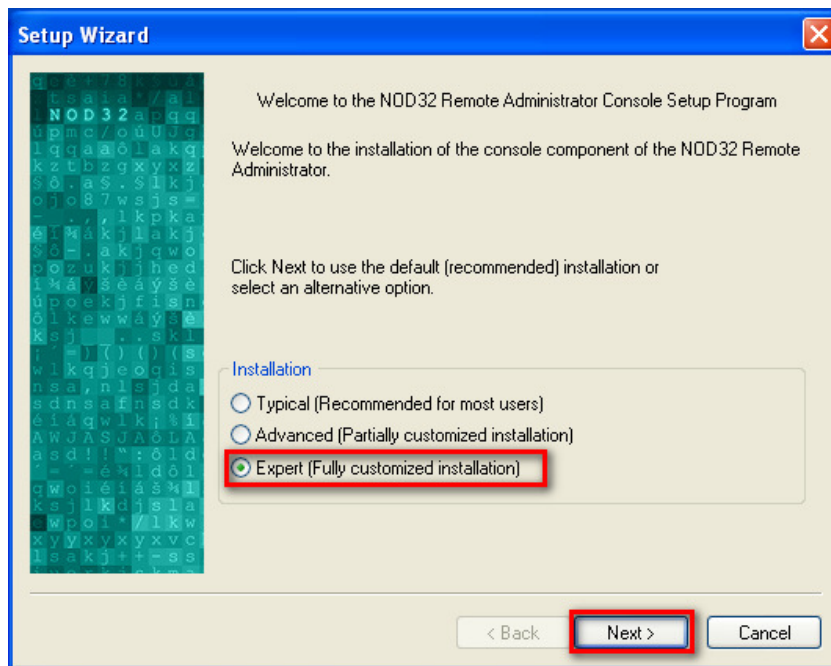


17. 按「Extract」

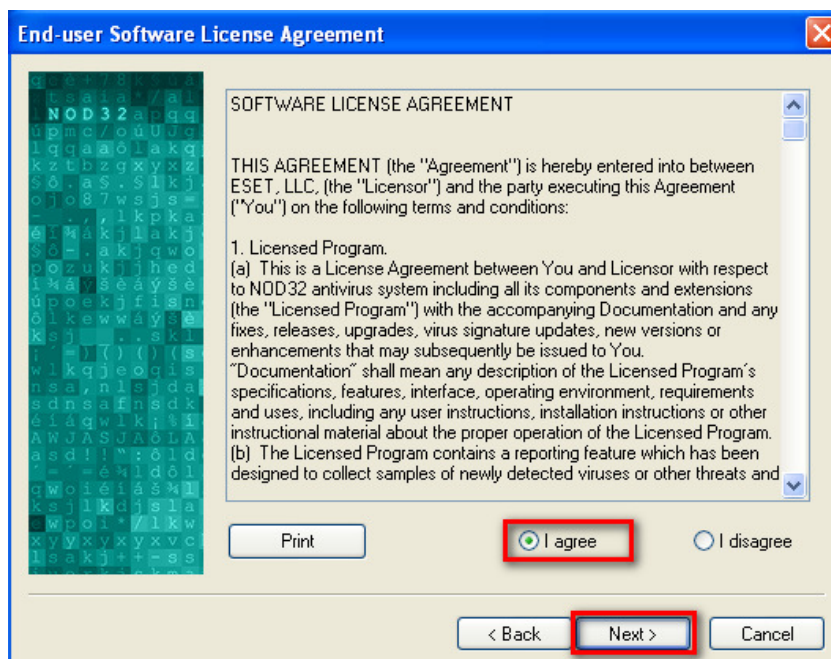




18. 選擇「Expert (Fully customized installation)」(專家), 再按「下一步」

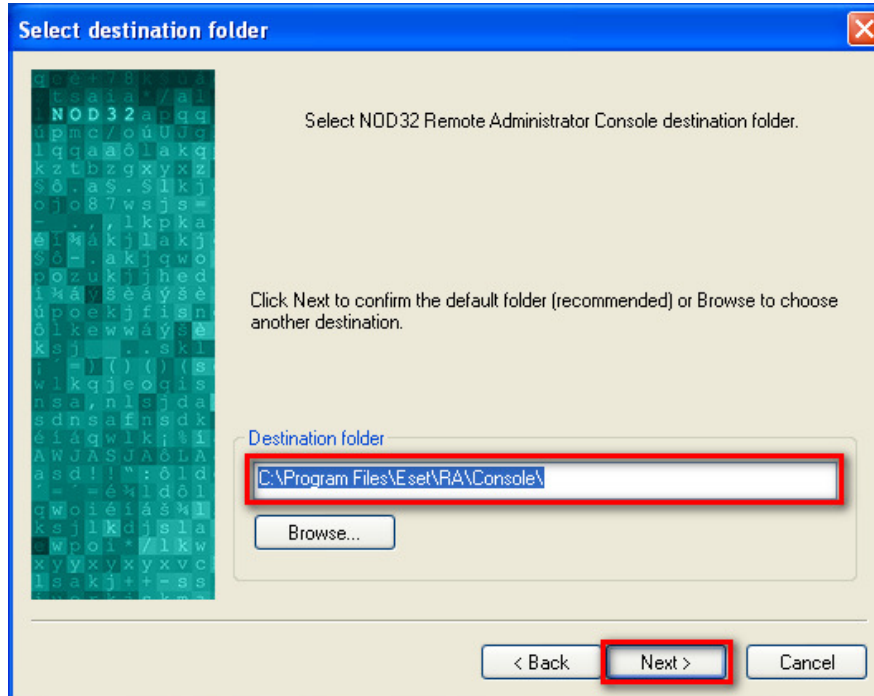


19. 選擇「I agree」, 再按「下一步」

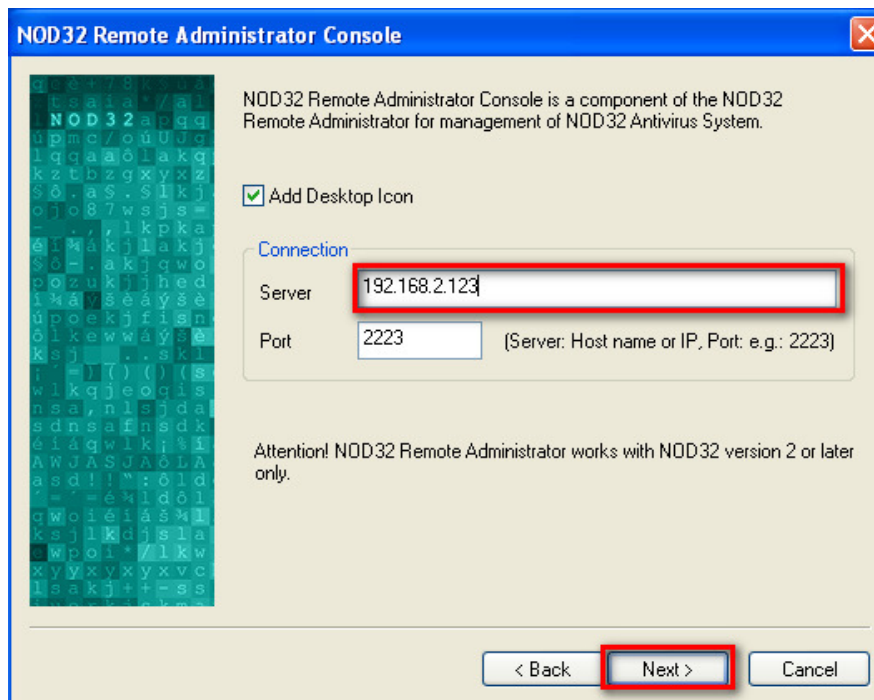




20. 按「下一步」

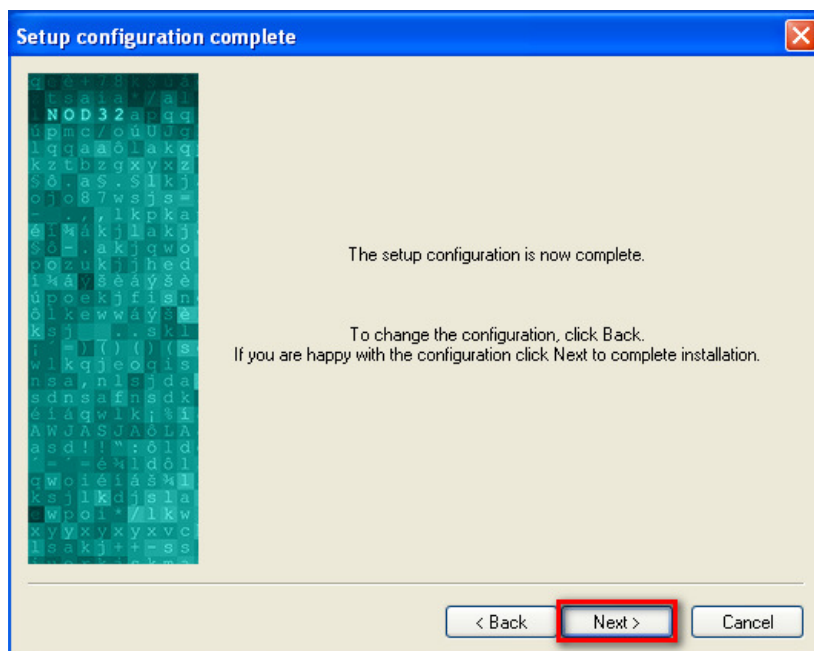


21. 請輸入遠端管理伺服器的「IP 地址」，而不是「電腦名稱」，否則遠端管理伺服器可能不能正常運作。

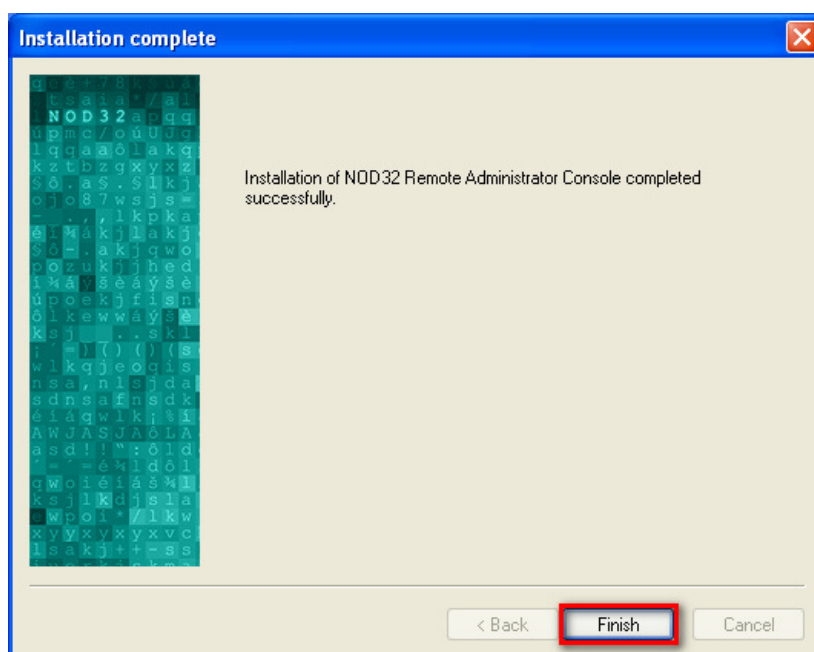




22. 按「下一步」



23. 按「完成」

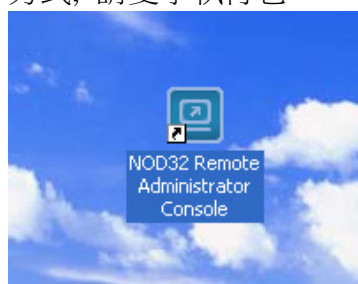


到此,你已經成功安裝了更新伺服器,遠端管理控制台及伺服器,在下一章節中,我們將指導你如何通過控制台來遠端控制及設定網路中其他用戶端上的 NOD32 .

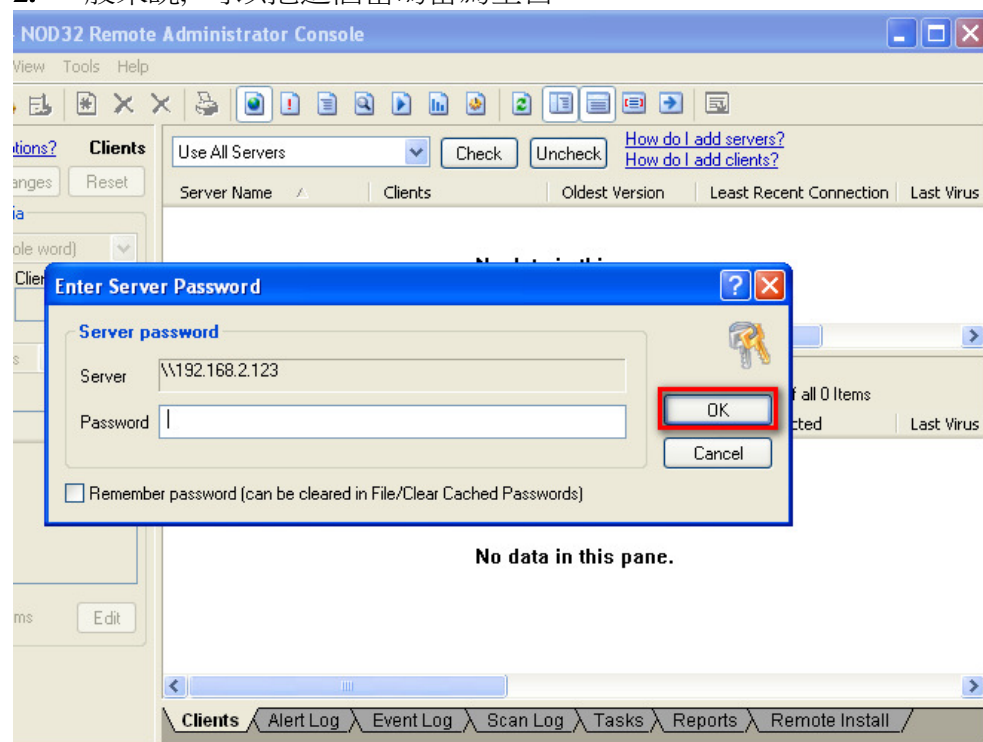
創建安裝包

我們可以利用遠端管理控制台來控制遠端管理伺服器，並通過它來完成對網路中所有機器的安裝，配置，更新，殺毒，病毒統計等工作。首先，我們將介紹如何通過管理控制台來完成網路中所有用戶端機器的 NOD32 安裝。

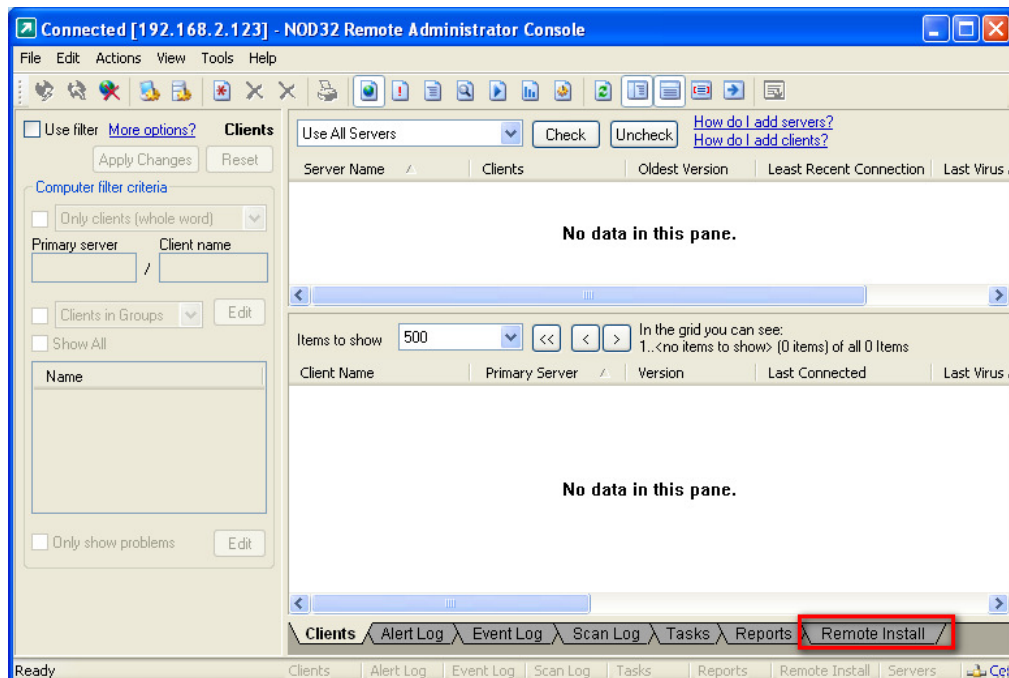
1. 如果你已經按照根據之前章節安裝**遠端管理控制台**，你的桌面會有這個快捷方式，請雙擊執行它。



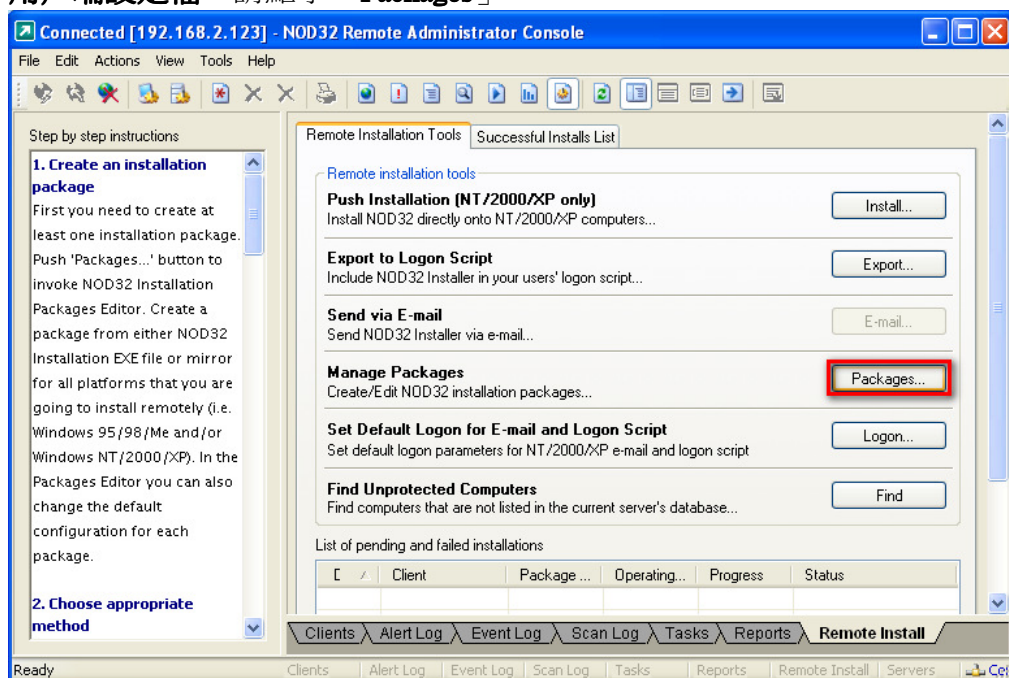
2. 一般來說，可以把這個密碼留為空白。



3. 遠端管理的第一件事，是把 NOD32 安裝到用戶端上。請點擊「Remote Install」

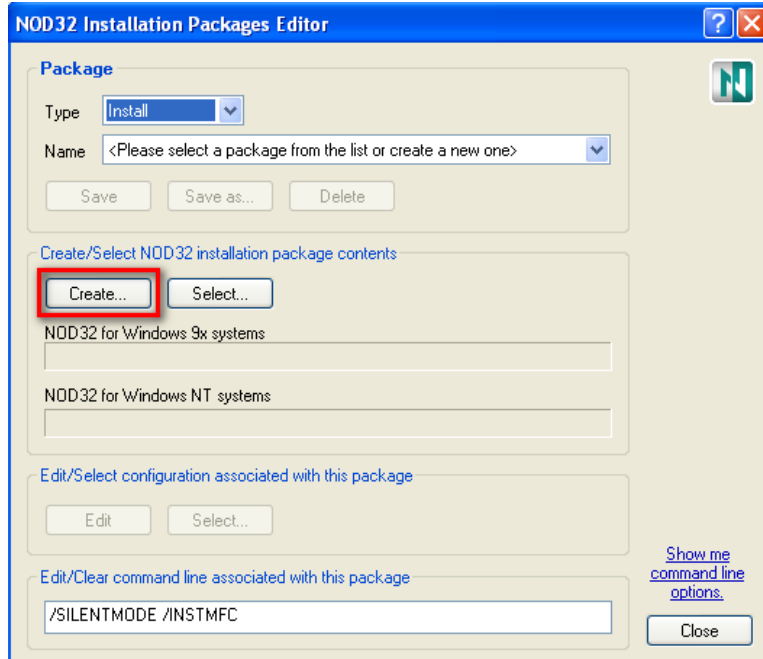


4. 我們要為安裝建立一個安裝包 (package)，這個安裝包含用戶端安裝檔以及用戶端設定檔。請點擊「Packages」

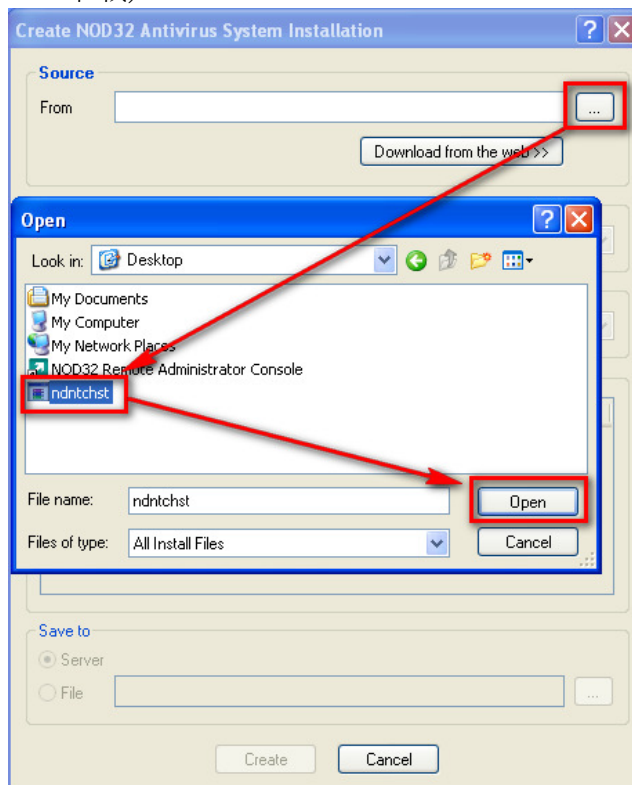




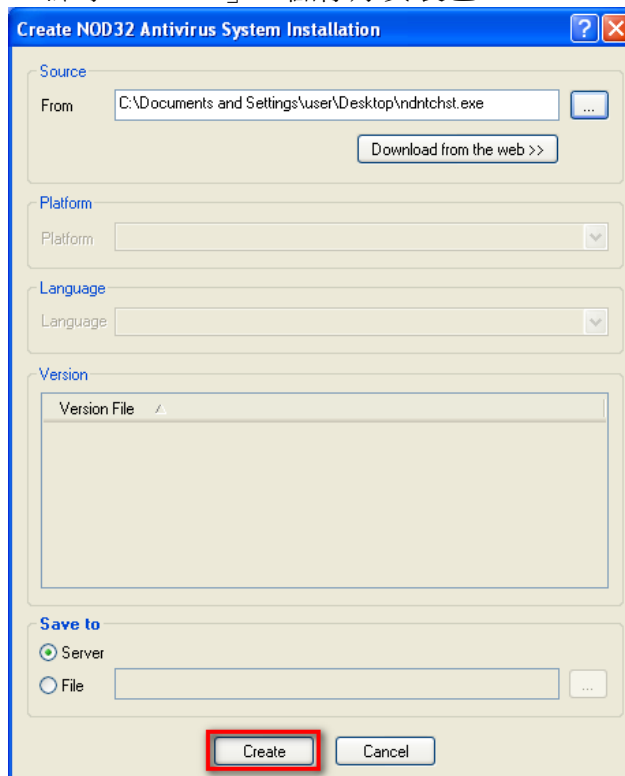
5. 點擊「Create」,建立一個將要安裝到用戶端的 NOD32 安裝程式。



6. 點擊「…」並選擇用戶端安裝檔 (你也可以點擊「Download from the web」來下載)



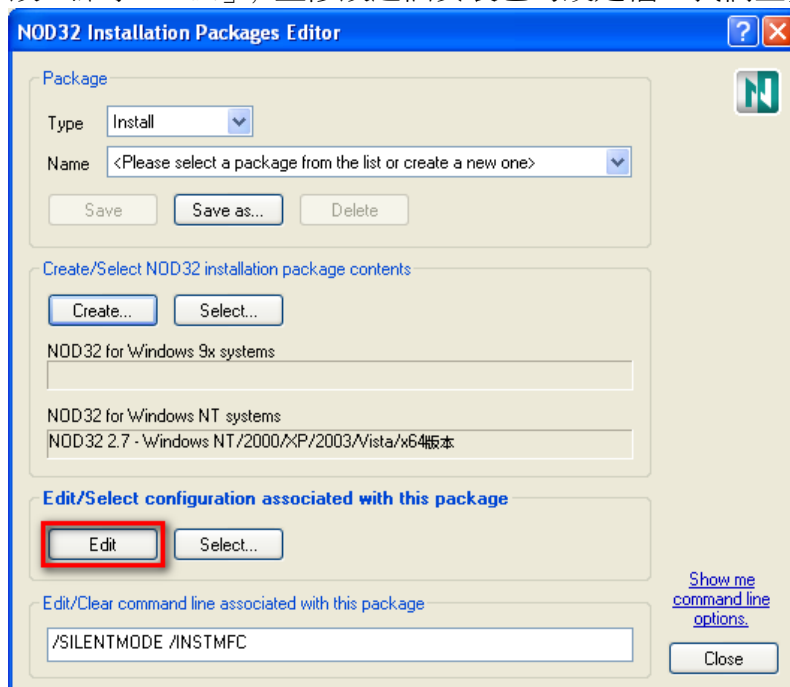
7. 點擊「Create」，儲存好安裝包



The dialog box titled "Create NOD32 Antivirus System Installation" contains the following sections:

- Source:** A "From" text field with the path "C:\Documents and Settings\user\Desktop\ndntchst.exe" and a "Download from the web >>" button.
- Platform:** A dropdown menu labeled "Platform".
- Language:** A dropdown menu labeled "Language".
- Version:** A text area labeled "Version File".
- Save to:** Radio buttons for "Server" (selected) and "File", followed by a text field and a browse button.
- Buttons:** "Create" and "Cancel" buttons at the bottom, with "Create" highlighted by a red rectangle.

8. 在上一步，你已經成功應用了範本，但是你需要根據你的具體情況做一些修改。點擊「Edit」，並修改這個安裝包的設定檔。我們主要修改三個設定。

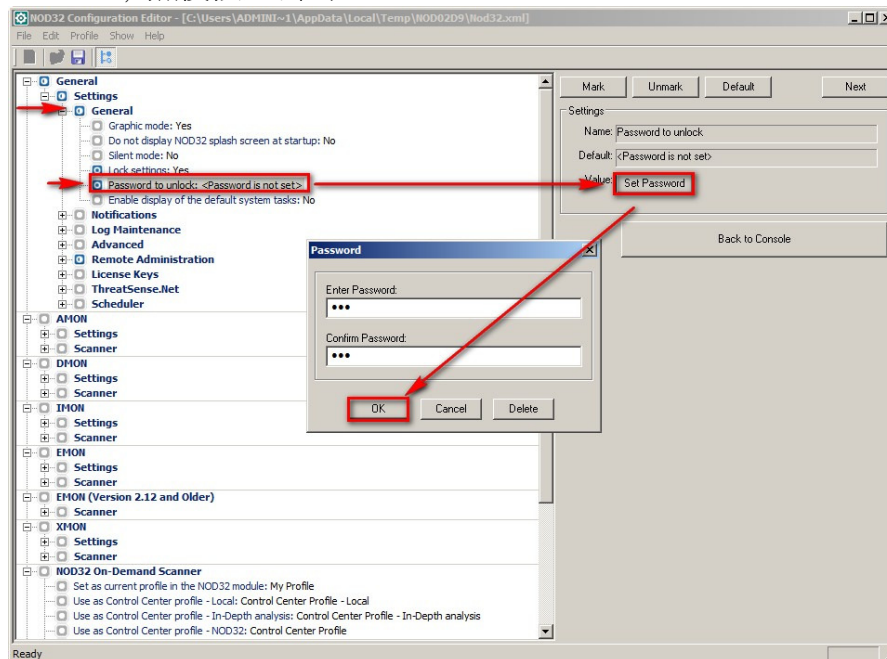


The "NOD32 Installation Packages Editor" dialog box contains the following sections:

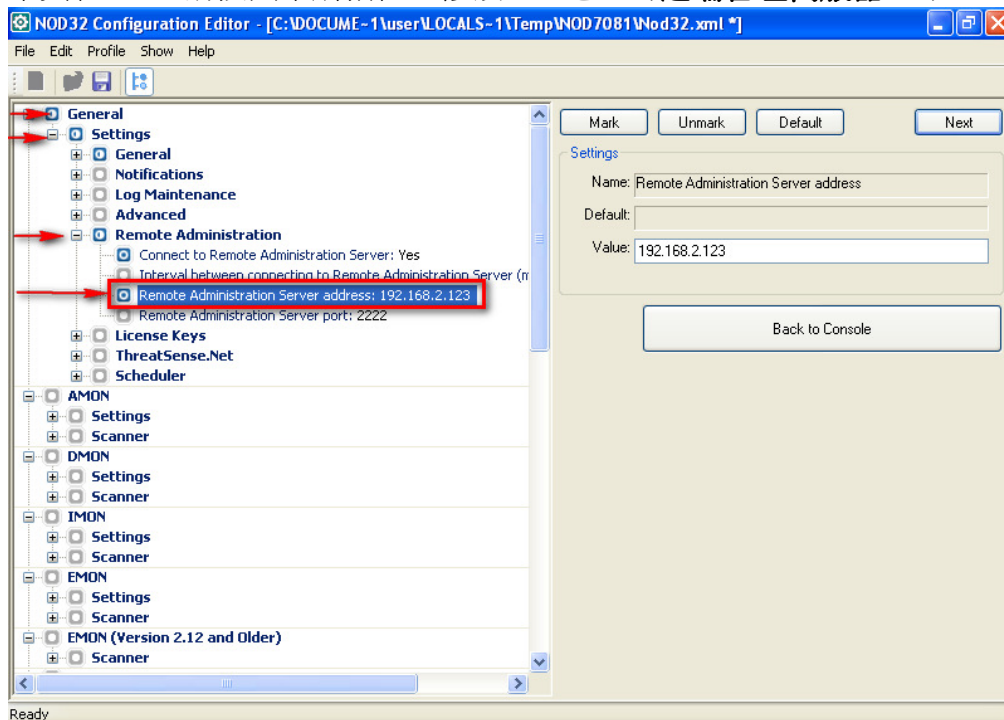
- Package:** A "Type" dropdown set to "Install", a "Name" dropdown with the text "<Please select a package from the list or create a new one>", and "Save", "Save as...", and "Delete" buttons.
- Create/Select NOD32 installation package contents:** "Create..." and "Select..." buttons, followed by three text fields containing:
 - NOD32 for Windows 9x systems
 - NOD32 for Windows NT systems
 - NOD32 2.7 - Windows NT/2000/XP/2003/Vista/x64版本
- Edit/Select configuration associated with this package:** An "Edit" button (highlighted with a red rectangle) and a "Select..." button.
- Edit/Clear command line associated with this package:** A text field containing "/SILENTMODE /INSTMF" and a "Close" button.
- Additional elements:** A "Show me command line options." link and a small NOD32 logo in the top right corner.



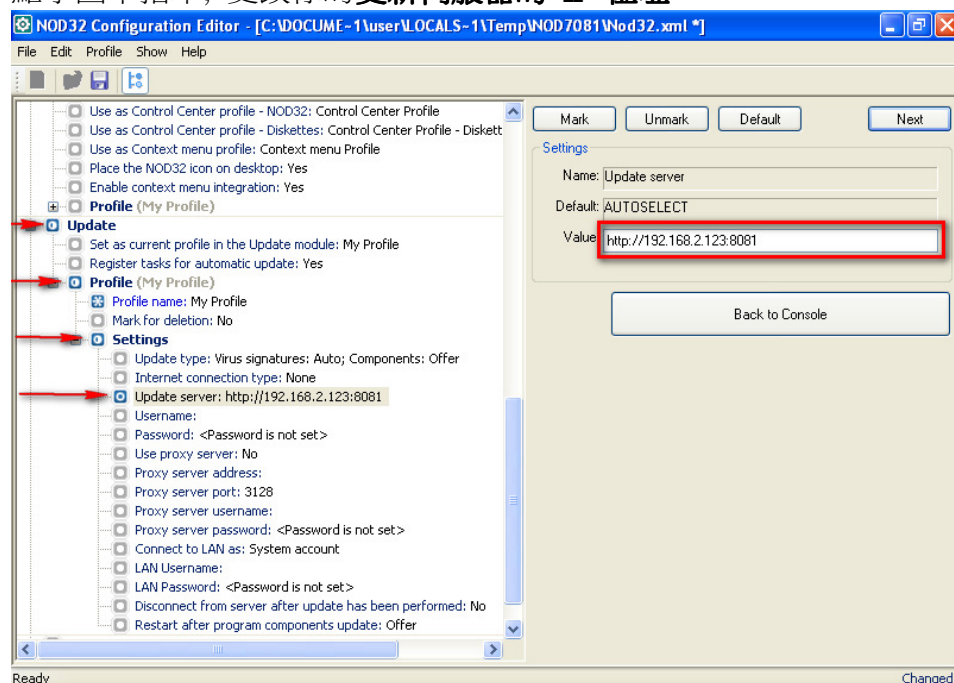
9. 在這裏設定用戶端 NOD32 的**密碼保護**，可以防止其他用戶修改 NOD32 的配置，或者卸載 NOD32。請按 Lock Settings: 別起是，請按 Password to unlock-> Set Password, 然後按入密碼。



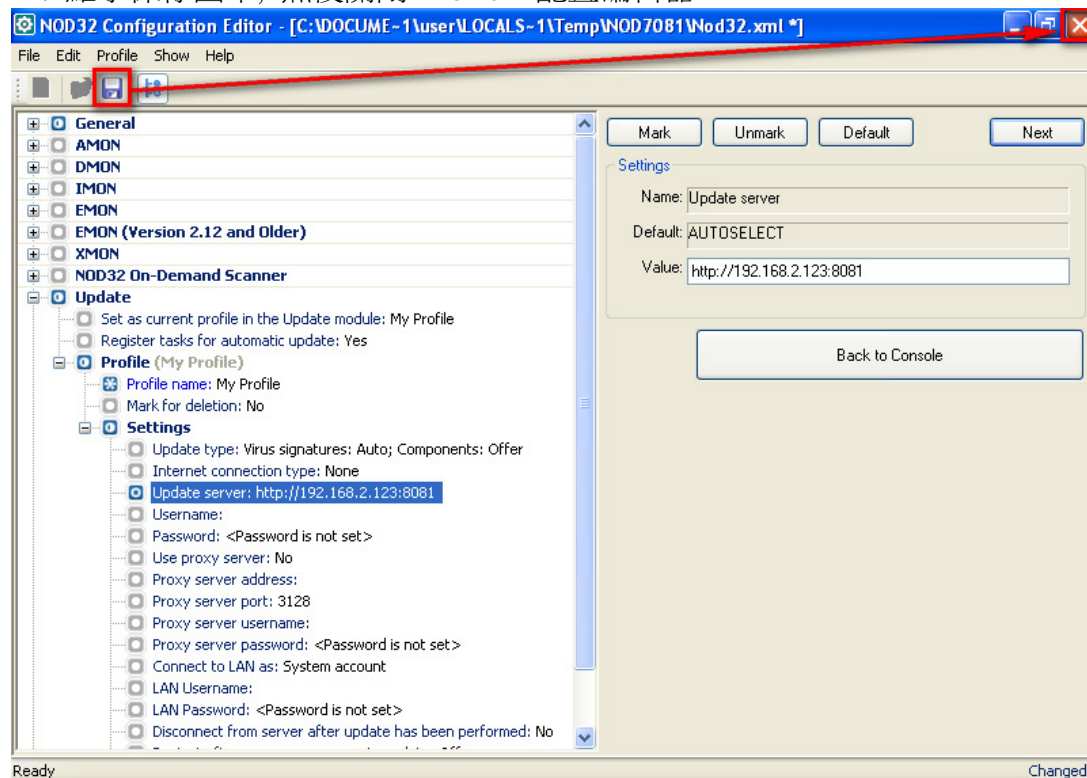
10. 第二個要修改的設定，是讓用戶端定期連接到遠端管理伺服器，以便日後的中央管理。請按圖中所指位置修改 IP 地址（**遠端管理伺服器 IP**）



11. 第三個設定，是讓用戶端同過我們剛建立的更新伺服器來更新病毒定義。請點擊圖中指示，更改你的**更新伺服器的 IP 位址**。

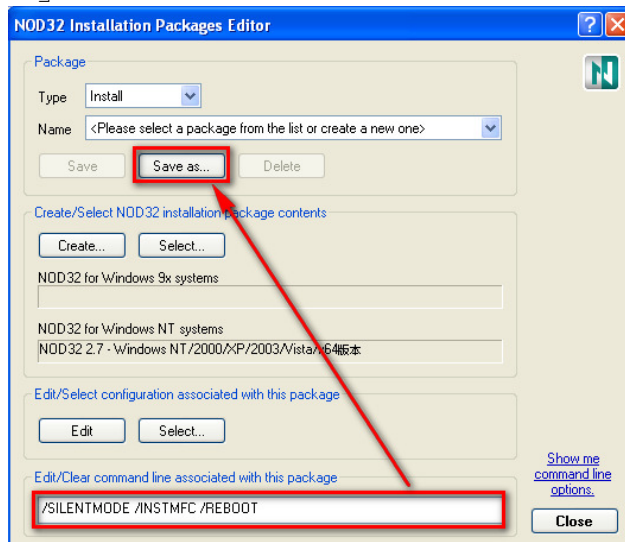


12. 點擊保存圖示，然後關閉 NOD32 配置編輯器。

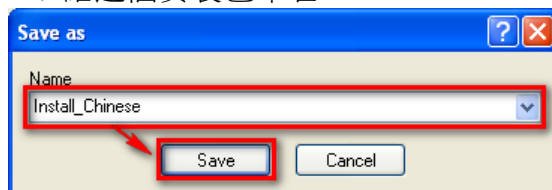




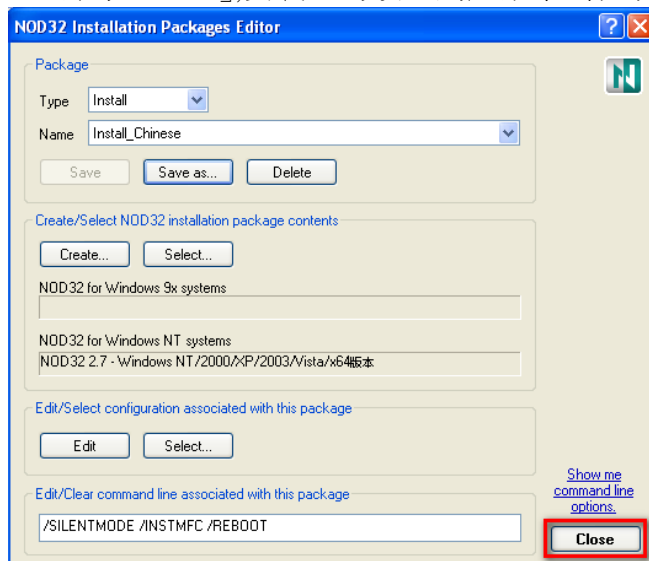
13. 用戶端 NOD32 安裝後需要重新啟動電腦來生效，如果你用戶端在安裝 NOD32 自動重新啟動，請點擊圖所示作設定加入 **reboot** 命令。然後點擊「**Save as**」。



14. 給這個安裝包命名



15. 點擊「**Close**」,安裝包的設置到此結束，你可以根據你的需要設定多個安裝包。

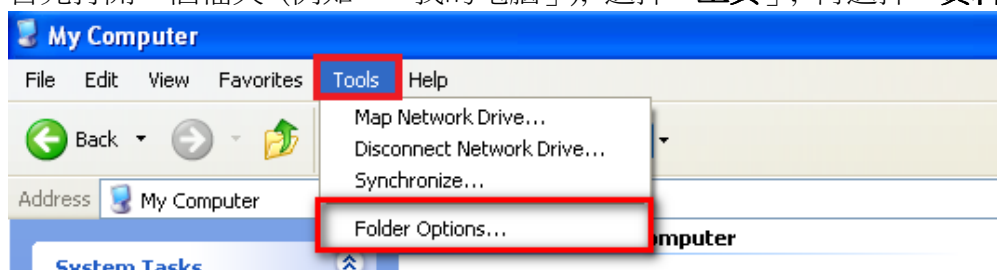


推送安裝示例

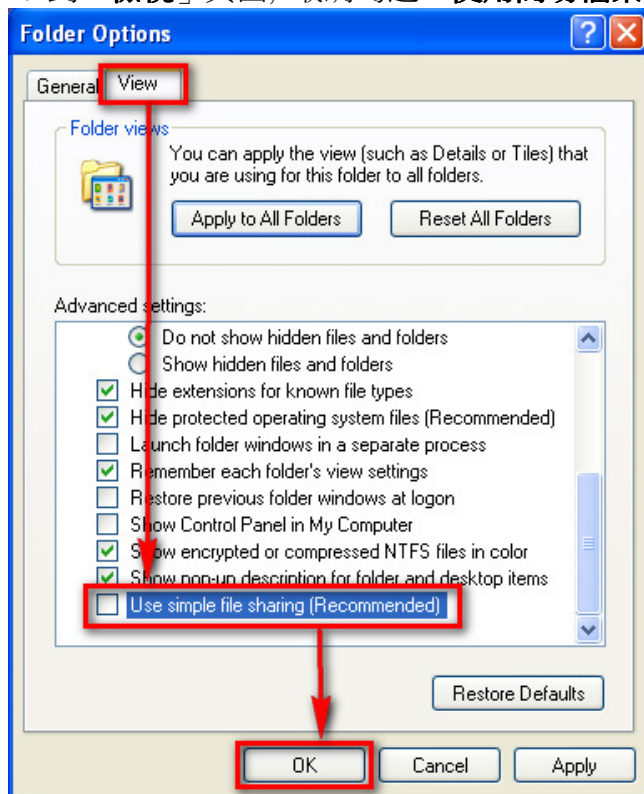
NOD32 遠端安裝有基本的三種方法，腳本安裝，**共用檔夾安裝**，和推送安裝。**共用檔夾安裝**需要有域的環境。在進行這三種安裝前都需要預先做好安裝包。本章節將示範最常用的推送安裝。

1. 要使用推送安裝，用戶端必須是 **Windows NT/2000/XP**，並且須要關閉「**使用簡易檔案共用**」，方法如下：

首先打開一個檔夾（例如：「我的電腦」），選擇「**工具**」，再選擇「**資料夾選項**」

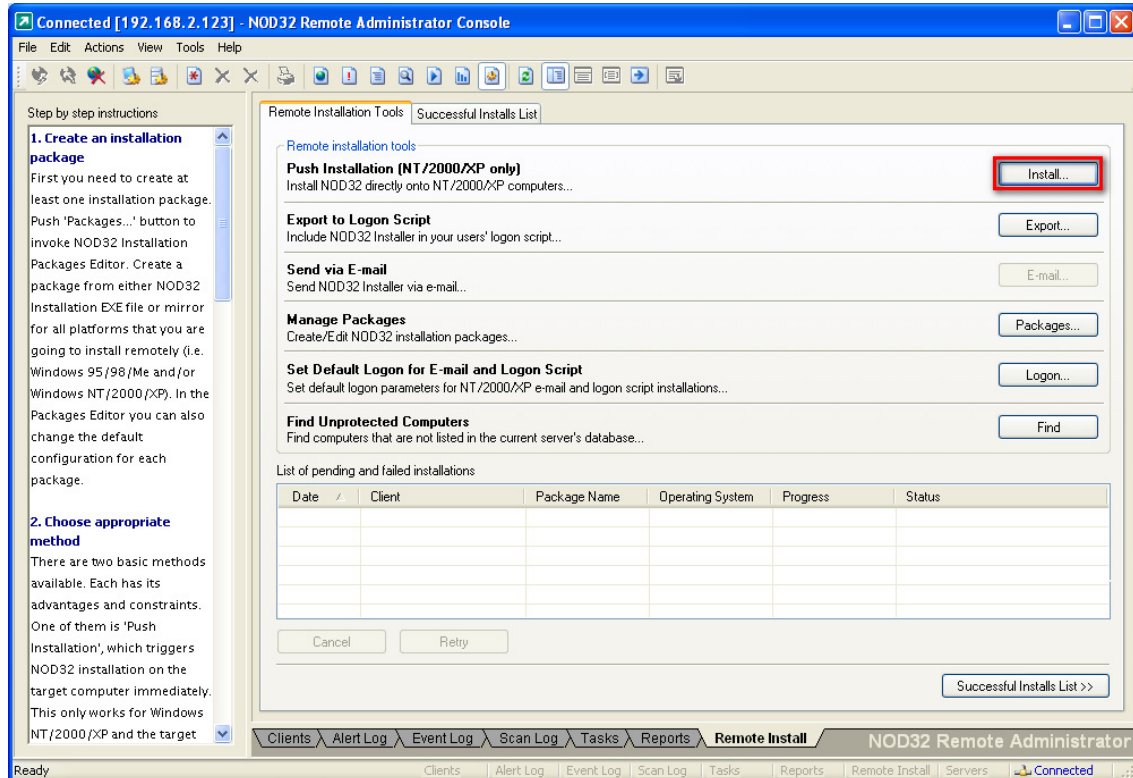


2. 到「**檢視**」頁面，取消勾選「**使用簡易檔案共用(建議使用)**」，再點擊「**確定**」

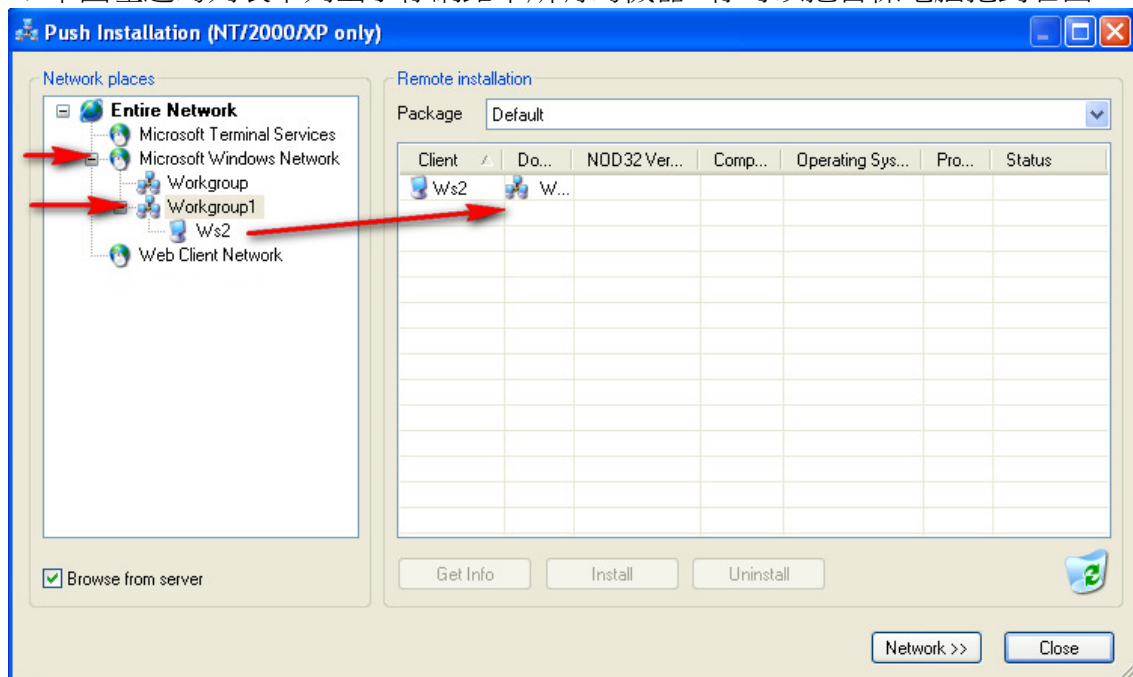




3. 確保用戶端沒有開啟“使用簡易檔案共用”及任何防火牆後，點擊「Install」開始安裝。



4. 下圖左邊的列表中列出了你網路中所有的機器，你可以把目標電腦拖到右面。

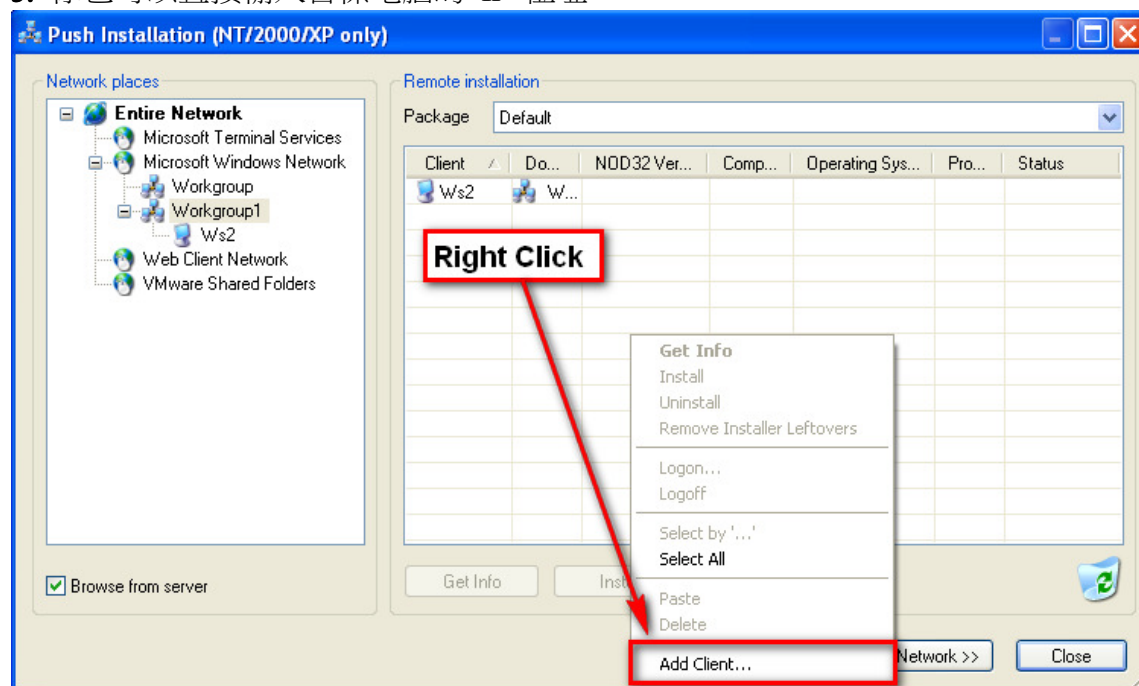


Version 2 Limited

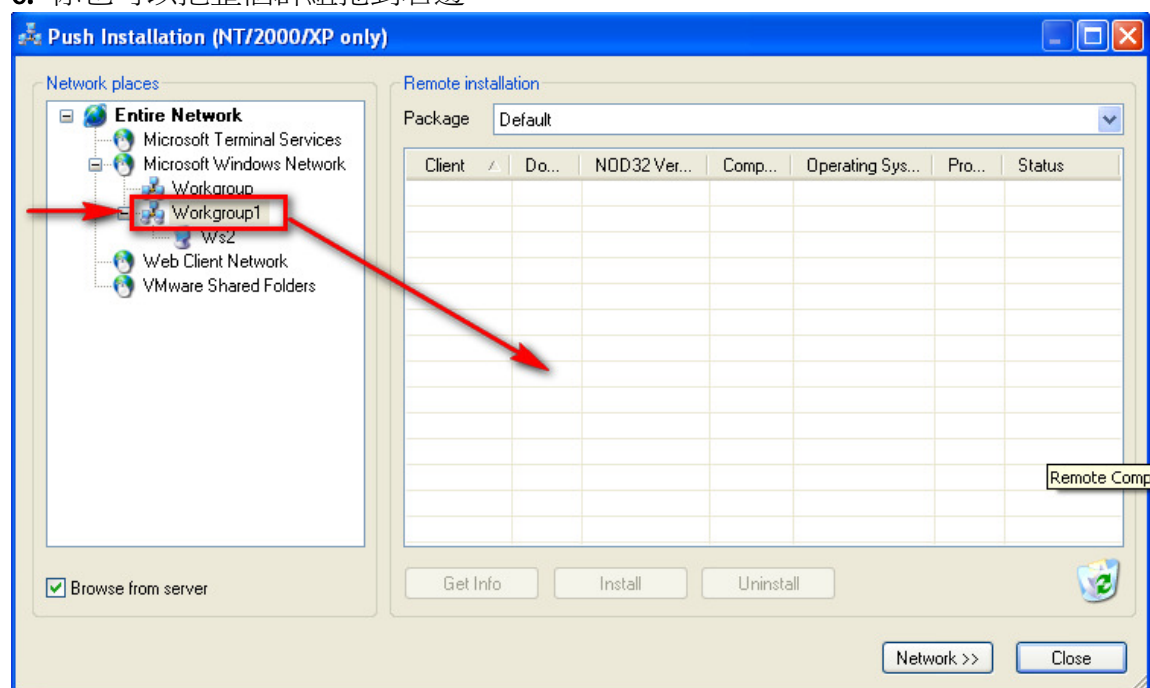
33

Mong Kok Office: 18/F, Go-up Commercial Building, 998 Canton Road, Mong Kok, Hong Kong
Sales Hotline: (852) 2893 8860 Support Hotline: (852) 2893 8186 Fax: (852) 2148-0323
Support FAQ: <http://www.nod32.com.hk/faq>

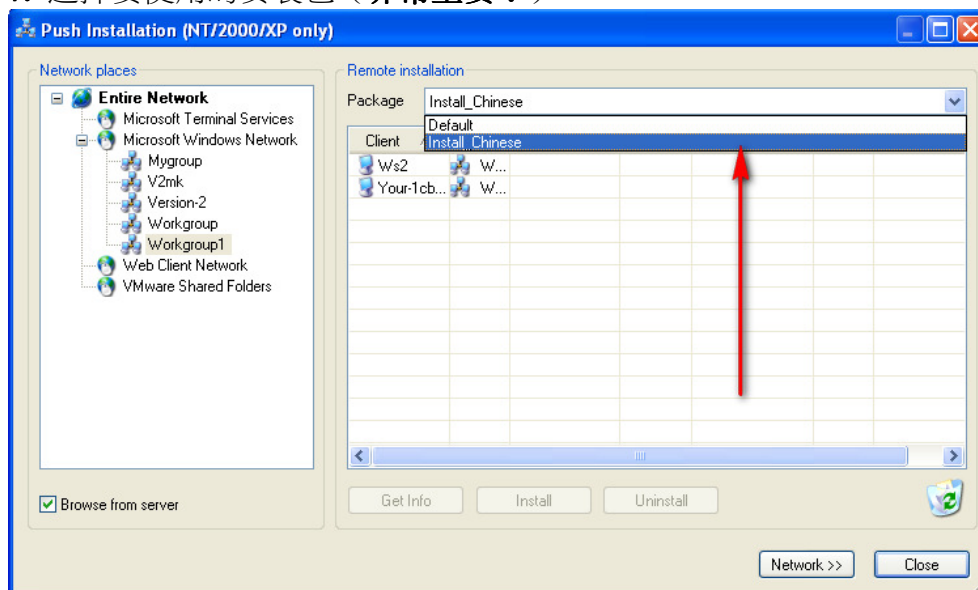
5. 你也可以直接輸入目標電腦的 IP 位址。



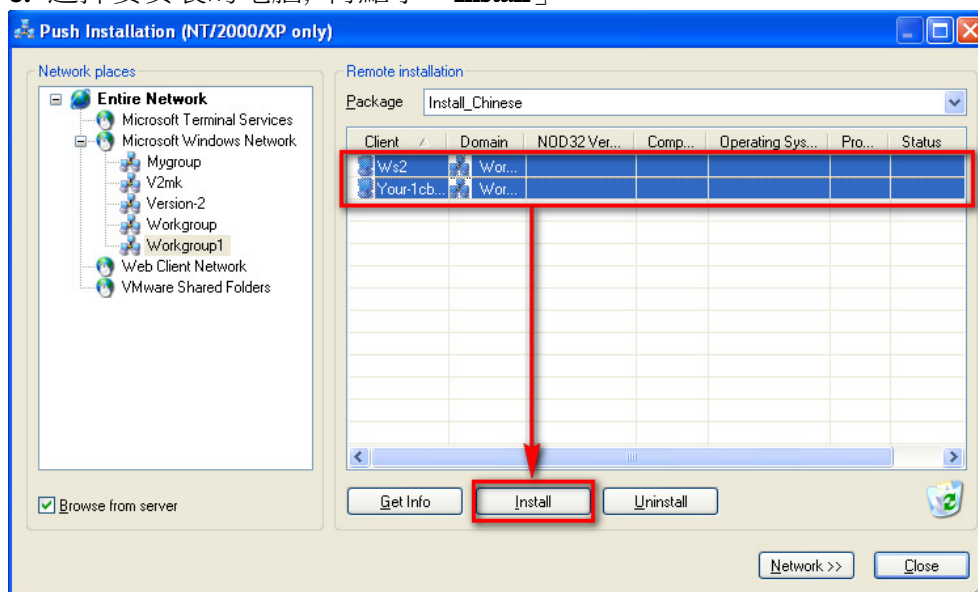
6. 你也可以把整個群組拖到右邊



7. 選擇要使用的安裝包（非常重要！）

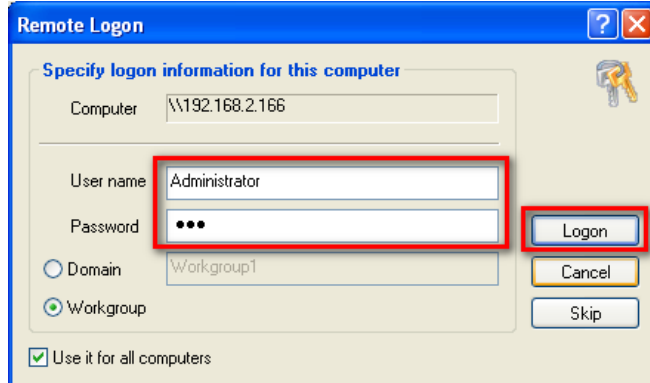


8. 選擇要安裝的電腦，再點擊「Install」

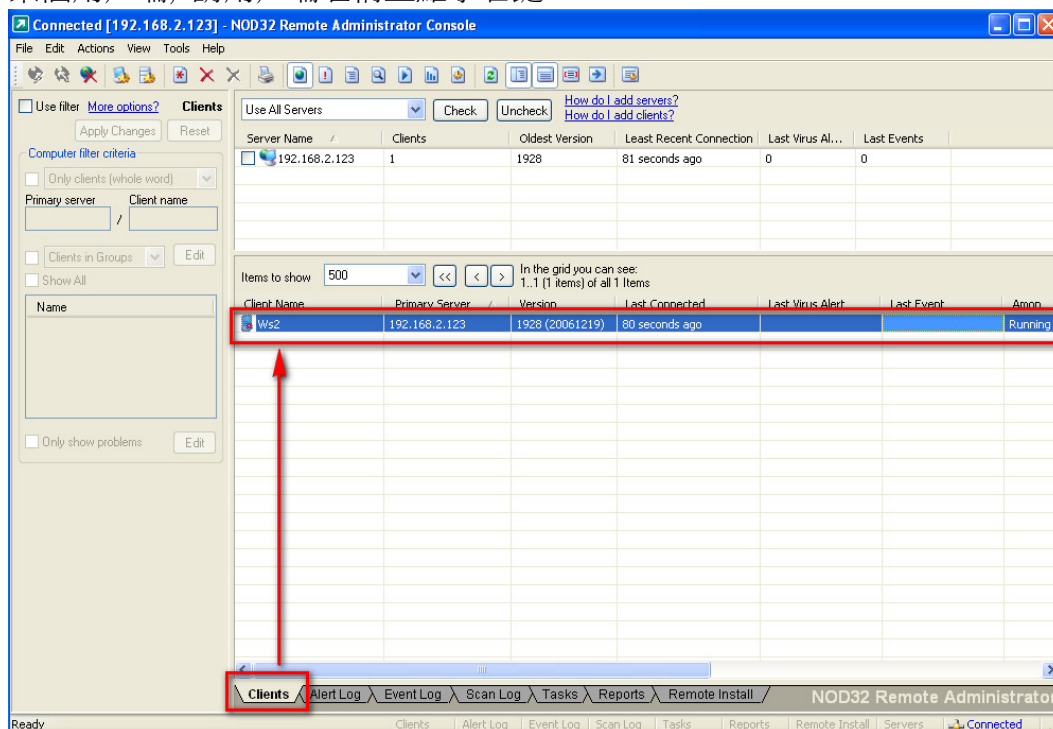




9. 請根據你的網路環境，輸入用戶端機器系統管理員的帳號和密碼。



10. 安裝成功後，你就可以看到用戶端連接到了遠端管理伺服器。如果你想控制某個用戶端，請用戶端名稱上點擊右鍵。



查找未受保護的電腦

在“Remote Install”部分選擇“Find Unprotected Computers”可以找到網路上沒有列入伺服器資料庫的所有電腦，並使得它們可以立即用 push 安裝法進行 NOD32 安裝。這有利於查找到網路上可能還沒有安裝 NOD32 的新電腦。按“Find”按鈕開始搜索。搜索過程可能需要幾分鐘。



安裝過程結果

在“**Remote Install**”部分選擇“**Successful Install List**”，列出遠端安裝成功的電腦。“**List of Pending and failed**”列出了所有遠端安裝失敗的電腦。右鍵點擊需要重新進行安裝的電腦，選擇“**Retry**”可以重新安裝。如果需要修改所選安裝的管理員用戶名與密碼，右鍵點擊所選機器，從功能表中選擇“**logon**”。



推送安裝問題解析

如果你發現推送安裝失敗，請按照以下步驟檢查 windows 設定：

1. 確保網路連接是正常的：伺服器端和用戶端能互相 ping 得通嗎？
2. 用戶端有沒有禁止“簡單檔共用”？
3. 工作站是否運行了防火牆阻礙了遠端安裝？
4. 能遠端存取用戶端 //192.168.*.*/admin\$嗎？
5. 你確認在遠端管理控制台上輸入了正確的用戶端管理員用戶名和密碼嗎？
6. 從其中的一台工作站，在命令提示符下運行：net use \\servername\ipc\$（建立與伺服器的 IPC 連接）命令,能否成功？
7. “網路的檔和列印共用”必須開啟（控制面板->網路連接->本地連接->屬性）
8. 管理員密碼（或者用於安裝的具有管理員許可權的用戶）不能為空。
9. 需要在目的機器上運行 RPC 服務（Remote Procedure Call）。
10. 需要在目的機器上運行遠端註冊服務（Remote Registry）。
11. 遠端程序呼叫服務(RPC)啟動類型應該設置為“手動”無需運行

請確保個人防火牆（比如 WinXP SP2）打開了你所用到的埠，（**大多數是在伺服器端**）。典型的終端工作站只需要允許 ICMP 在推送安裝過程中回應請求。

NOD32 和遠端管理服務所使用的埠如下：

- 2222- 用戶端與伺服器之間的通訊。
- 2223 - 遠端管理控制台與遠端管理伺服器之間的通訊。
- 2224- 安裝檔與遠端管理伺服器之間的通訊。
- 2846- 遠端管理伺服器之間的同步
- 8081 - 用戶端到本地升級伺服器的通訊（默認設置為 8081,但是可以更改）
- 445- 遠端管理伺服器到用戶端的請求資訊和建立 IPC 連接(埠 445 是標準的微軟“檔和列印共用”埠)



由於網路的限制，遠端安裝在正式安裝開始前就可能已經出錯了。如果那樣的話，錯誤原因會在表格中描述（SC 錯誤代碼，GLE 錯誤代碼）

SC 編碼主要是幫助管理員定位的內部錯誤代碼，GLE 錯誤代碼對用戶來說更有用，他們都是典型的“Win32 錯誤代碼” - 你可以登錄以下網站查看詳細錯誤代碼解釋：

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/debug/base/system_error_codes.asp

以下是一些常見的錯誤描述類型：

Could not set up IPC connection to target computer (SC error code 6 , GLE error code 53) - 不允許訪問網路共用（很可能因為防火牆遮罩了 445、135－139 埠），或者無法連接到目標電腦。

Could not install NOD32 Installer onto target computer (SC error code 6 , GLE error code 67) - 無法訪問目標工作站的 ADMIN\$ 共用檔夾（有可能此檔夾共用已經關閉，可用命令 net share admin\$ 開啟）

Could not retrieve required information from target computer (RES error code 13, GLE error code 97) - 有可能目標工作站沒有開啟“Remote registry”服務

Could not set up IPC connection to target computer (SC error code 6 , GLE error code 1327) - 目標工作站的管理員密碼為空。

Could not set up IPC connection to target computer (SC error code 6 , GLE error code 1326) - 目標工作站啟用了“使用簡單檔共用”

SC 代碼時常出現的是 6 或 11，它們表示“拒絕訪問”或“伺服器不能連接到遠端服務管理器”。以下列表詳細列出了每一個代碼的解釋。這些代碼也可能出現在日常使用時的警告視窗中。

SC 代碼	代碼解析
0	一切正常
1	拒絕訪問
2	連接註冊表錯誤



3	打開註冊表錯誤
4	刪除註冊表項錯誤
5	電腦名錯誤
6	建立連接時錯誤
7	取消連接時錯誤
8	參數錯誤
9	拷貝檔時錯誤
10	刪除檔錯誤
11	打開服務控制管理器錯誤
12	服務名稱錯誤
13	枚舉服務錯誤
14	詢問服務錯誤
15	創建服務錯誤
16	打開服務錯誤
17	開始服務錯誤
18	刪除服務錯誤
19	記憶體錯誤
3010	一切正常，需要重啟
101	需要管理員許可權
102	缺少配置檔
103	記憶體不足
104	作業系統版本過舊
105	無法在系統暫存檔案夾中解壓壓縮檔
106	解壓時發生錯誤
107	安裝檔丟失或損壞（帶元件配置的安裝檔）
108	安裝的元件比已安裝元件舊
109	無法建立 dll 連接
110	不支援此操作（在動態連結程式庫中）
111	無法在磁片中創建檔
112	元件數目不匹配
113	元件數目不明
114	setup.xml 檔丟失或損壞



115	新舊版本不相容，需要卸載舊版本。
116	寫入註冊表錯誤
117	升級錯誤
118	安裝版本同當前版本的語言版本不一致，需要卸載
119	卸載檔損壞或丟失
120	註冊服務錯誤
121	安裝元件錯誤（關於元件詳情見 nsetup.log）
122	無法安裝組件
123	你安裝的試用版本已過期
124	作業系統不匹配- Windows NT
125	作業系統不匹配- Windows 95



其他安裝方法示例

由於 Push installation 要受到 Windows 的許多限制，如必須有管理員許可權，遠端電腦必須設為允許遠端存取，埠不能被防火牆遮罩等，這些都可能導致 Push installation 失敗。本章中我們將介紹幾種額外的安裝方式。

1. 共用檔夾安裝

一，.在伺服器上準備一個 test 共用檔夾，裏面放 ndntcsst.exe 和 config.xml 文件。

config.xml 可以參考安裝手冊內的配置，並做出相應修改（遠端管理伺服器 IP，更新伺服器 IP，用戶端密碼保護設定）

二，. 準備一個批次檔案，也放在共用檔夾裏。

製作方法如下：

a.在 Test 檔夾中右鍵單擊>>新建>>文本文檔(命名為 test.txt)

b.打開 test.txt 並添加如下內容：

```
@echo off
```

```
\\192.168.1.80\test\ndntcsst.exe /SILENTMODE /REBOOT
```

```
/cfg=\\192.168.1.80\test\config.xml
```

```
:end
```

（注：\\192.168.1.80\test 為共用檔夾的地址）

c.保存此 txt 檔,並重命名為 test.bat

三， 在用戶端安裝

方法如下：開始>>運行\\192.168.1.80\test\test.bat 然後按確認

程式將自動以你預定義的配置開始安裝。

2. 導出到登錄腳本安裝法(Logon script)

此種方法需要網路存在域的環境

導出到登錄腳本安裝法會將 NOD32 安裝腳本添加到局域網內電腦中存在的登錄腳本檔中。導出到登錄腳本安裝法也包含卸載程式。

選擇所要應用的安裝包創建安裝腳本，在“安裝位置”選擇安裝檔夾，選擇 NOD32 installer 的檔夾，並確保要安裝 NOD32 系統的所有電腦可以訪問獲取安裝包所在的檔夾。

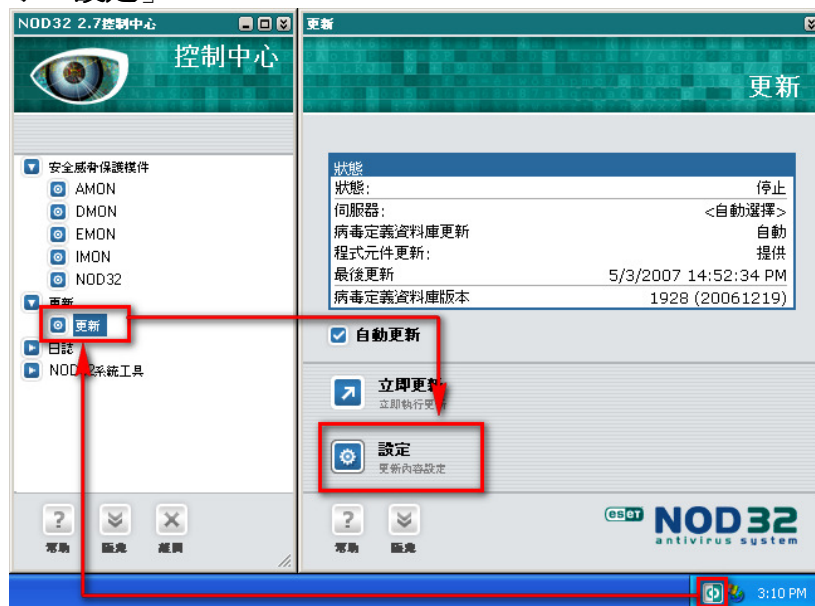


在“腳本位置”部分選定當前的登錄腳本檔夾，選擇將定制為 NOD32 登錄腳本安裝的登錄腳本。要編輯每個登錄腳本，使用“編輯”按鈕編輯，然後點擊編輯器上的“保存”按鈕保存結果。

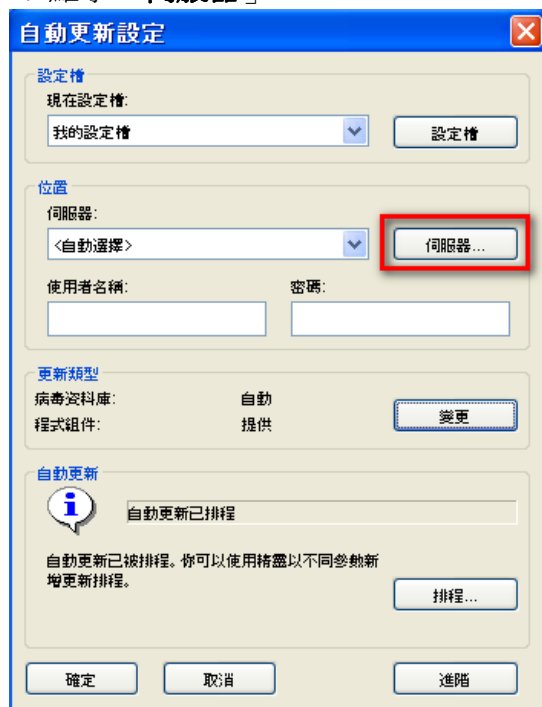
詳情請參閱：www.nod32.com.hk/faq

如何把單機加入管理

1. 在已安裝 NOD32 的用戶端，開啟「NOD32 控制中心」，點擊「更新」，再點擊「設定」

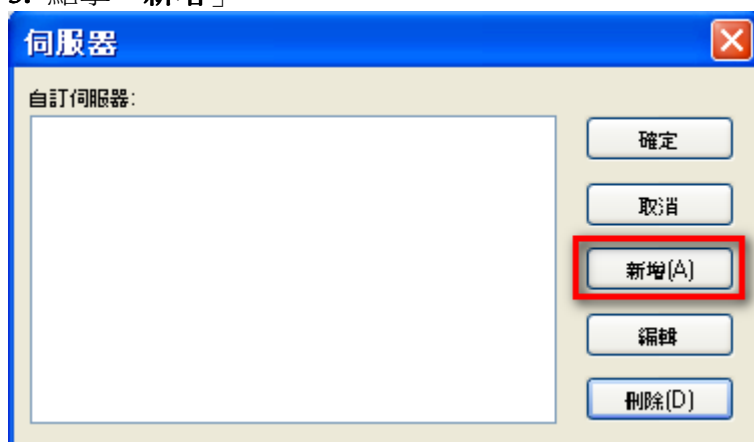


2. 點擊「伺服器」

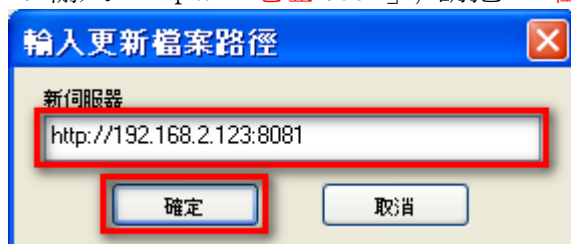




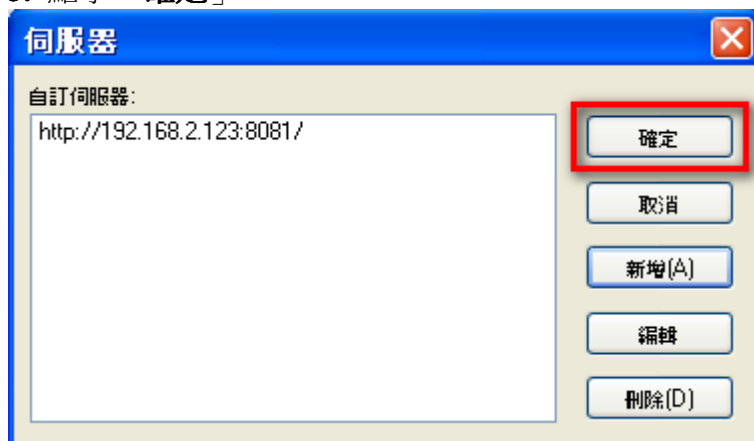
3. 點擊「新增」



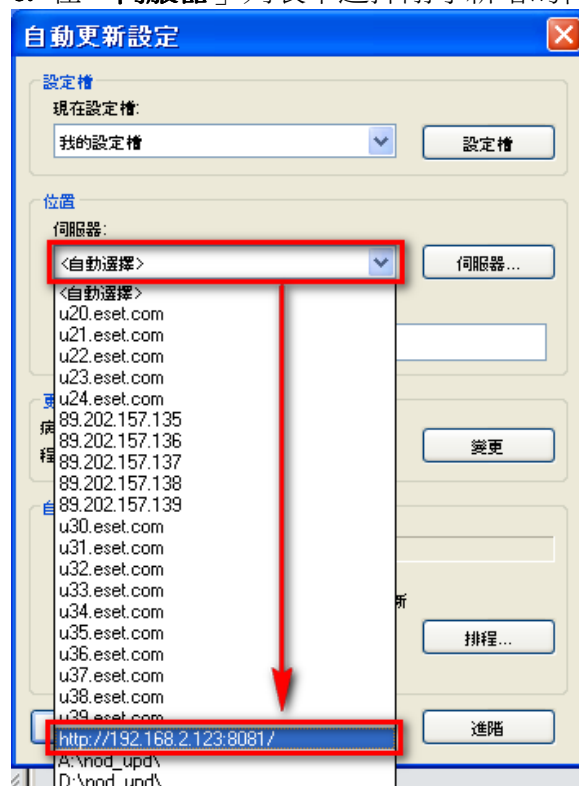
4. 輸入「http://IP 地址:8081」，請把 IP 位址 改為你更新伺服器的 IP 位址。



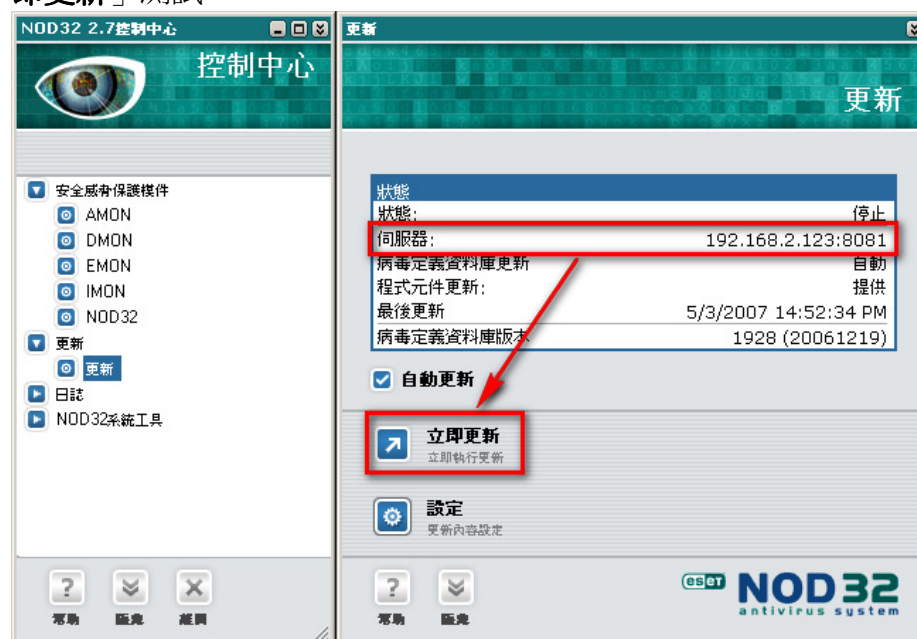
5. 點擊「確定」



6. 在「伺服器」列表中選擇剛才新增的伺服器，再點擊「確定」

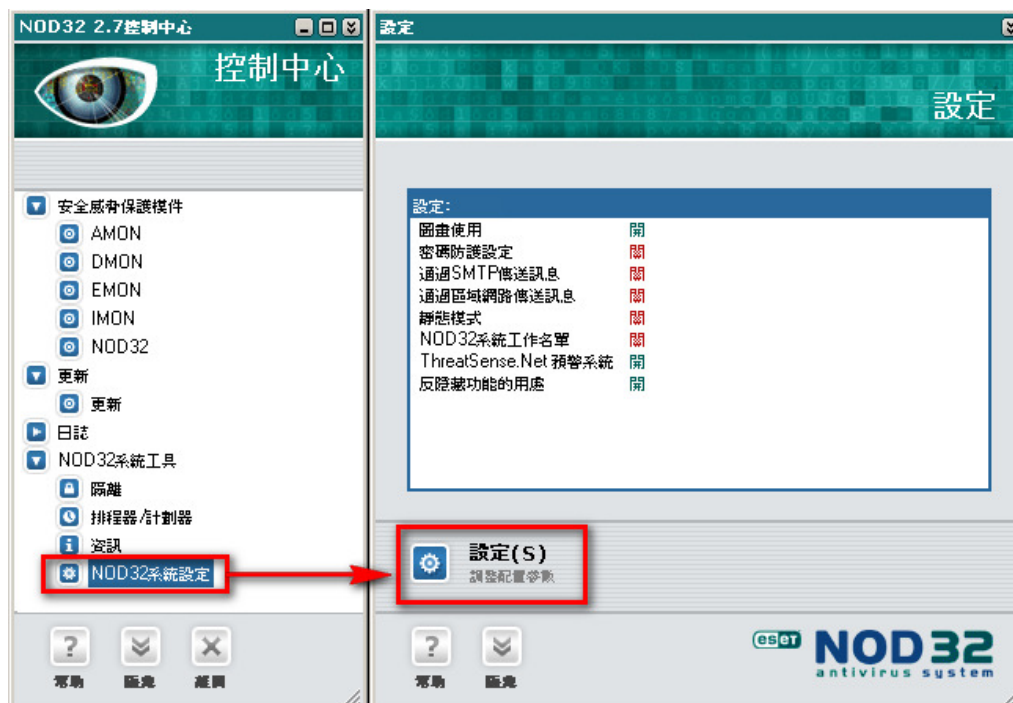


7. 最後你會看到「伺服器」變更成為你剛剛添加的更新伺服器，你可以點擊「立即更新」測試。

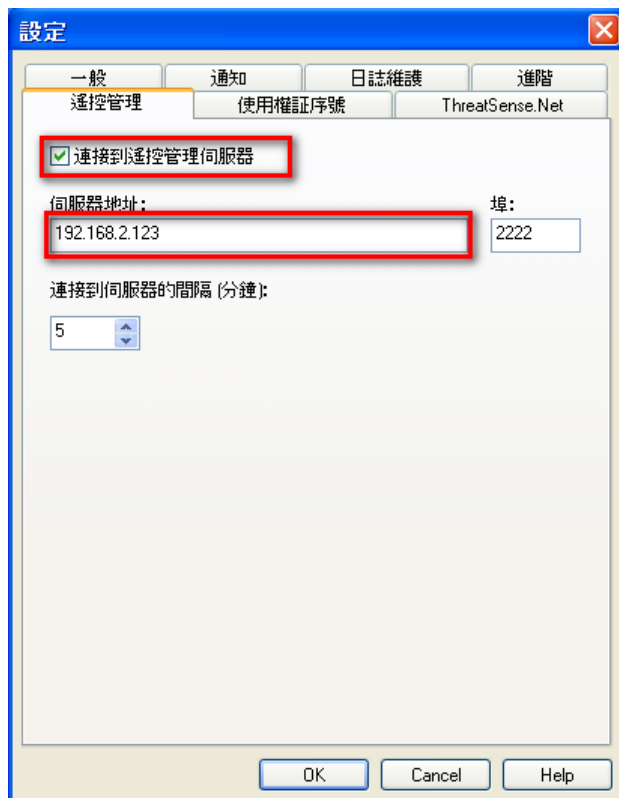




8. 添加遠端管理伺服器 IP



9. 在「遙控管理」選項表中加入遠端管理伺服器 IP 位址

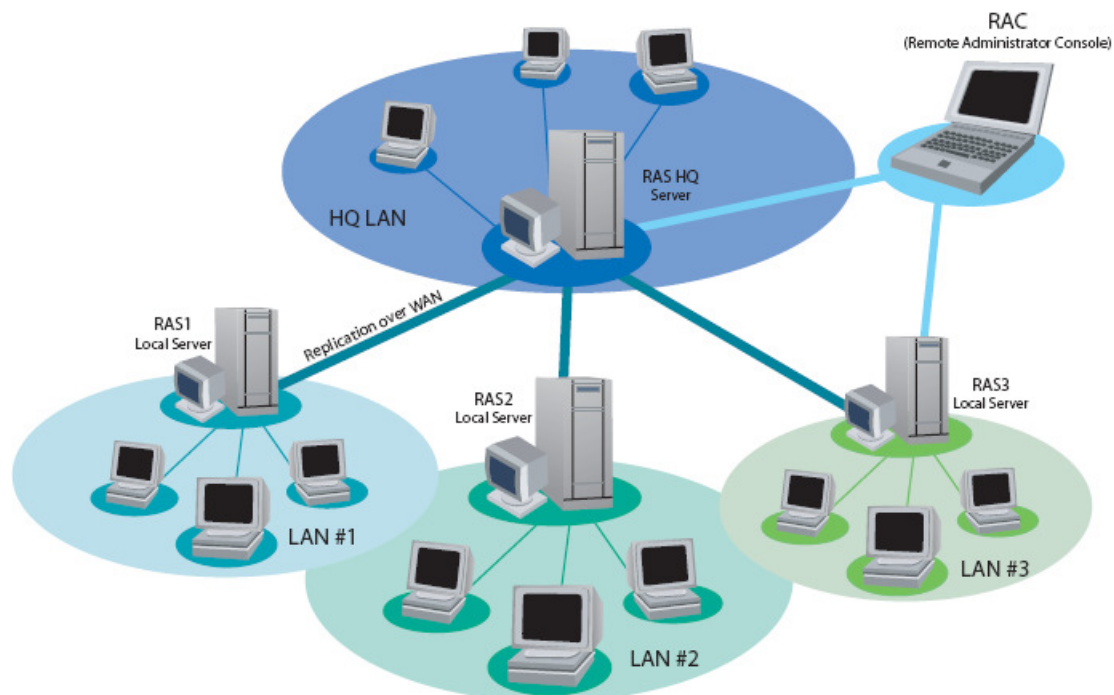




大型電腦網路與同步

大型電腦網路使用多個 RAS 伺服器，以樹狀結構構成。工作量將分發到網路中安裝的大量不同的 RAS 伺服器中，每個 RAS 伺服器都指定有本地管理員。網絡上 RAS 伺服器之間的所有聯繫都是經過加密的。

下圖展示了一個延伸至多個區域的大型電腦網路。



在這個例子中，RAS1、RAS2 和 RAS3 是分支辦事處的伺服器。它們都向總部伺服器 RASHQ 傳輸同步資料。總部伺服器是它們的“上級”伺服器。同時，RASHQ 必須配置為接受來自 RAS1、RAS2 和 RAS3 的連接。

RASHQ 可以監視和配置整個公司的用戶端。這可以通過兩種方式實現。一種是 RASHQ 收集資料生成整個公司範圍的報告，另一種是直接使用 RASHQ 管理整個公司（在分支區域網路沒有相應各自的管理員的情況下）。

連接樹狀結構的 RAS 伺服器，請使用“同步”設定，參看“RAS 伺服器設定”一章的描述。



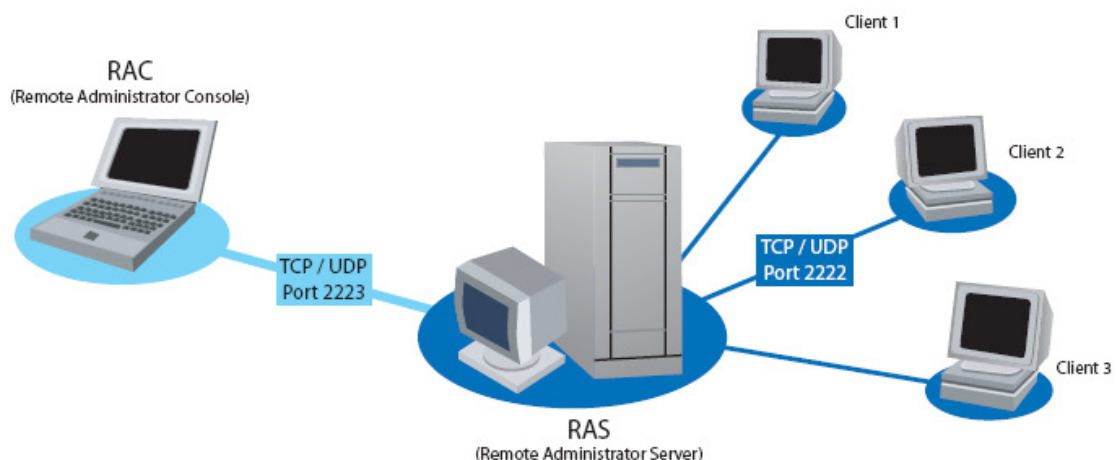
連接到 RAS 伺服器

使用 RAC 連接到 RAS 伺服器。在主功能表的“工具/控制台選項”選擇“連接”選項表設置 RAS 伺服器的連接指向。然後填入 RAS 伺服器的 IP 位址並點擊“連接”。鉤選“在控制台啟動時自動連接到選擇的伺服器上”來設定你的 RAC 控制台的一個默認 RAS 伺服器。

當連接向 RAS 伺服器時，會提示你輸入一個 RAS 伺服器密碼。默認密碼為空。如果想要修改 RAS 伺服器密碼，在 RAC 控制台主功能表中選擇“檔/修改密碼…”。

如果要保存密碼，連接伺服器時在“記住密碼”可選框處勾選。為安全起見，並不建議你保存 RAS 伺服器密碼。如果想清除所有以前保存的密碼，在 RAC 控制台主功能表中選擇“檔/清除保存的密碼”。

RAS 伺服器與 RAC 控制台通過 TCP/UDP 2223 埠通信。當通過網際網路接入 RAS 伺服器時，一定要保證防火牆或路由器的 TCP/UDP 2223 埠已打開，並且通訊通過 RAS 伺服器的內部 IP 地址重新定向。





RAS 伺服器設置

使用 RAC 控制台修改 RAS 伺服器的設置。伺服器的相關設置都列在“工具/伺服器選項”功能表中。

配置選項表

SMTP 設置

- 伺服器——e-mail 通訊使用的 SMTP 伺服器位址
- 發送人地址——RAS 伺服器管理員的 e-mail 地址

日誌設置

- 啟用日誌——使用 RAS 伺服器活動日誌
- 日誌檔案名——RAS 伺服器日誌檔案名
- 日誌容量——保存在日誌檔中的信息量。日誌容量有下列選項可選：
 - 1——只記錄嚴重錯誤日誌
 - 2——除 1 外，加上用戶會話錯誤日誌
 - 3——除 2 外，加上詳細的會話日誌與控制台連接日誌
 - 4——除 3 外，加上 NOD32 installer 連接日誌
 - 5——調試模式。所有的活動都會記入日誌，包括 NOD32 控制中心的通信日誌。

其他設置

- 總是允許新用戶端——選中時，當有新用戶端第一次連接 RAS 伺服器時，自動添加新客戶到客戶列表。在同步過程中，用戶通過其他 RAS 伺服器同步進入，也會被自動添加到客戶列表。
- 新用戶端自動標記為“新”——選中時，新用戶端將不會被標記為“新”，否則用戶端將會被標記為“新”。更多詳情參看“客戶”選項表描述。
- 只保留最近 xx 個用戶端事件——允許定期刪除舊的事件消息，僅保留最後的 xx 個事件。
- 自動清除間隔——設定執行清除資料庫任務的時間間隔。
- 立即清除——立即執行清除資料庫任務。

同步設置選項表

同步到上級伺服器設置

- 向上級伺服器同步——如“大型網路”那章描述那樣在大型網路中進行同步



- 上級伺服器——上級 RAS 伺服器的名字或 IP 位址，該伺服器從本地 RAS 伺服器上收集資料
- 同步間隔——設定同步時間間隔
- 立即同步——開始同步到上級伺服器
- 日誌類型——定義同步到上級 RAS 伺服器的事件類型（警報、事件、掃描）
- 自動同步——啟用定期同步。如果不啟用此功能，可以手動觸發同步。

接收來自下級伺服器的同步

- 啟用接收來自下級伺服器的同步——啟用本端伺服器從許可伺服器列表區域中的其他伺服器上收集資料。多個 RAS 伺服器之間，使用 “，” 號分隔。

RAS 伺服器還可以通過 nod32ra.ini 檔進行配置。



RAC 控制台設置

使用“工具/控制台選項…”功能表修改 RAC 控制台設置。

設置需要顯示的列——顯示/隱藏選項表

設定控制台選項表中的可見列。

配色方案選項表

指定控制台視窗中事件與屬性的顯示顏色。

- 用戶端：歷史版本——設定以前版本病毒資料庫的顏色
- 用戶端：版本太舊或未知——設定舊病毒庫的顏色或者顯示不存在項。
- 用戶端：最後連接——設定用戶端最後連接時間的顯示顏色
- 用戶端：最後一次病毒警報——設定最後一次病毒警報的顏色
- 用戶端：最後一次事件——設定最後一次非病毒警報事件的顏色
- 用戶端：Amon 停止——設定停止運行 AMON 時警報的顏色
- 事件日誌：診斷——設定“診斷”事件的顏色
- 事件日誌：警告——設定“警告”事件的顏色

路徑選項表

設置保存來自 RAS 伺服器的報告的“報告”檔夾的儲存路徑。默認的“報告”文件夾保存在 NOD32 根文件夾下的“reports”文件中。

其他設置選項表

日期/時間欄的顯示

設定日期/時間欄的顯示

- 絕對——顯示絕對時間（如 14:30:00）
- 相對——顯示相對時間（如“兩周之前”）
- 時區——根據 Windows 中的時區設置顯示本地時間
- 依據 UTC 時間計算本地時間（使用本地時間）——重新計算本地時間。否則時間會依據格林威治世界標準時間計算。

其他設置

- 啟用自動刷新——自動刷新當前視窗
- 在應用程式退出時自動清空回收站——當退出 RAC 時清空回收站
- 顯示格線——顯示格線
- 在系統託盤中顯示圖示——將控制台視窗在 Windows 託盤作為一個圖示顯示
- 當發現有問題用戶端時系統託盤的圖示高亮顯示——當檢測到一個錯誤



或警告時，高亮顯示系統託盤圖示。使用“編輯…”按鈕定義將要跟蹤的錯誤和警告。



網路活動總覽

使用連接到 RAS 伺服器的 RAC 控制台可以監控網路上的活動。RAC 控制台包括以下幾個選項表：

- 用戶端
- 警報日誌
- 事件日誌
- 掃描日誌
- 任務
- 報告
- 遠程安裝

使用“F5”鍵可以更新每個控制台選項表。

所有控制台選項表都可以定制排序。可以通過選擇項目欄，點擊標題，挑選選定的項目。如果要改變項目欄的顯示排序，直接拖放該欄目即可。

遠端控制台的用戶選項表

遠端控制台包含了一個你的網絡上連接到 RAS 伺服器的 NOD32 用戶列表。使用遠端控制台左邊的“過濾”(filter) 選項可以過濾後找制定合適用戶的顯示。依據所屬組別對客戶進行分組，使用“編輯/分組”功能表可以篩選出想要查看的群組與客戶。

網路中所有新用戶端都在用戶端選項表上標記為“新”顯示，這樣 NOD32 管理者可以很容易的找到它們並進行配置。



在對新用戶端進行配置後，點擊“重設‘新’標記”，將其標記為配置過的客戶。



所有用戶端帶有一個“注釋”區域，提供管理員一個地方儲存網絡上 NOD32 客戶的注釋資訊。

主伺服器屬性是 NOD32 客戶直接連接向的 RAS 伺服器名。

版本屬性顯示出當前客戶運行的 NOD32 病毒庫版本。

最後連接顯示出客戶最後一次連接到 RAS 伺服器的時間。最後連接時間按照 RAC 控制台設置中的設定格式顯示。所有正在運行的用戶端與過期的 NOD32



病毒庫版本都會以不同的顏色顯示。

最後一次病毒警報屬性顯示出客戶最後一次檢測出病毒的時間。

最後一次事件顯示出客戶報告的最後一次出現事件(如更新錯誤/系統模件錯誤)。

要清除某個客戶的最後病毒警報與事件錯誤消息，點擊客戶圖示，分別選擇“清除‘最後事件’文本”與“清除‘最後病毒警告’文本”。

要查看某個特定客戶的病毒警告消息或錯誤消息，分別點擊“最後一次病毒警告”“最後一次事件”可以查看屬於選定客戶的所有消息。

Amon 屬性顯示出選定客戶 AMON 模組的當前狀態。

配置屬性顯示出 NOD32 客戶的配置。更新配置查看點擊“請求”。查看當前配置點擊“查看”。保存配置點擊“保存為”。為 NOD32 客戶預置一個執行任務，點擊“新任務”。在更新配置過程中，配置輸出有兩種狀態：當配置刷新後為“完成”，正在刷新配置為“被請求”。

IP 屬性顯示出最後的 NOD32 客戶的 IP 位址。

作業系統屬性顯示出客戶運行的作業系統版本。

移動用戶屬性可以為網路上的移動用戶設定。通過接入網路，所有移動用戶可以將 NOD32 更新到當前版本。右鍵點擊客戶，使用“設定‘移動用戶’標記”可以將客戶設定為移動用戶。

警報日誌選項表

警報日誌選項表包括 AMON、EMON 與 IMON 防病毒模組監測到的所有病毒感染。要查看警報詳情，點擊選擇的警報。

顯示出的屬性如下：

- 事件 ID——事件日誌中的事件標識號碼
- 客戶名——發生事件的客戶名
- 主伺服器——客戶連接入的 RAS 伺服器名
- 日期——警報的日期與時間
- 接收——RAS 伺服器報告警報的日期與時間
- 模組——觸發警報的防病毒模組名稱
- 物件——被感染的物件類型
- 病毒——報告的病毒名稱
- 名稱——感染檔的名稱
- 操作——組織病毒擴散所採取的操作
- 訊息——警報的注釋與其他資訊



- 日誌詳情——日誌檔可用性

事件日誌選項表

事件日誌選項表包括從用戶端收集的所有警報與錯誤訊息，除了病毒警報訊息。使用“事件日誌類型”篩選選項，可以篩選出需要的事件日誌。要查看選擇的事件詳情，雙擊它。

顯示出的屬性如下：

- 警報 ID——事件日誌中的事件標識號碼
- 客戶名——發生事件的客戶名
- 主伺服器——客戶連接入的 RAS 伺服器名
- 日期——警報的日期與時間
- 接收——RAS 伺服器報告警報的日期與時間
- 模組——觸發警報的防病毒模組名稱
- 類型——警報類型
- 事件——事件描述

掃描日誌選項表

掃描日誌選項表包括 NOD32 手動病毒掃描器生成的報告。要查看選擇的事件詳情，雙擊它。

- 掃描 ID——掃描日誌中的事件標識號碼
- 客戶名——發生事件的客戶名
- 主伺服器——客戶連接入的 RAS 伺服器名
- 日期——警報的日期與時間
- 接收——RAS 伺服器報告警報的日期與時間
- 描述——事件的詳細描述
- 已掃描——已經掃描的檔數量
- 已感染——受感染的檔數量
- 已清除——清除病毒感染檔的數量
- 狀態——NOD32 手動掃描器的返回狀態
- 啟動者——啟動 NOD32 手動掃描器的用戶名
- 詳細日誌——可查看詳細日誌



使用 RAC 控制台的具體細節

本章將描述在大型電腦網路中使用 RAC 控制台的具體細節。

按住 CTRL 鍵點擊所要選擇的記錄可以在一個視圖下選擇多個記錄。如果要選擇一組記錄，按住 SHIFT 鍵，然後選擇組的第一個記錄與最後一個記錄。

分組

在控制台主功能表中點擊“編輯/分組”可以將 NOD32 用戶端按照用戶定義分組。可以針對某個 NOD32 客戶組設定具體的任務。

過濾

使用“過濾”選項可以篩選出想要在 RAC 控制台查看的記錄。在控制台主功能表中點擊“查看/顯示/隱藏過濾面板”，打開篩檢程式。

如果要在查看中應用過濾，在控制台中勾選“使用過濾”可選框，點擊“應用更改”應用過濾。

應用電腦過濾規則可以以多種方式篩選出控制台查看內容。

- 僅<客戶名>用戶端 只顯示指定客戶名的客戶
- 僅類似<字串>用戶端 顯示名字中含有給定字串的客戶
- 除去<客戶名>用戶端 從視圖中除去指定客戶名的客戶
- 除去類似<字串>用戶端 去除名字中含有給定字串的客戶
- <分組列表>組中的用戶端 只顯示指定分組中的客戶
- 其他分組中的用戶端或者 N/A 顯示屬於其他分組而不屬於指定分組的客戶以及不屬於任何分組的客戶。假如某個用戶端屬於多個分組，那麼只要其中一個分組為非指定分組，它仍將被顯示。

右鍵菜單

右鍵點擊視圖中的任何一個記錄可以進入右鍵功能表。右鍵功能表讓你可以用其他方式定制控制台視圖。下面是右鍵功能表選項的列表。

- 選擇‘aaa’——選擇視圖中包含撇號中字串的記錄。撇號中的字串取自你點擊的記錄。
- 反向選擇——反向選擇當前的選擇。
- 隱藏選定——隱藏選定的記錄。
- 隱藏未選定——隱藏沒有選定的記錄。

要清除過濾規則，到“查看/裁剪視圖”中清除或按“F5”。

**示例**

- 選擇被某個病毒感染的用戶端：到用戶端選項表，右擊任何一個沒有錯誤警告的客戶。從右鍵功能表中選擇“選擇由 “ a” (假設用戶為 a)，然後選擇“隱藏選定”。
- 查看名為 Joseph 和 Charles 的電腦上的病毒警報：在警報日誌選項表用戶端名項目欄中選擇一個名為 Joseph 的電腦的記錄，右鍵點擊，在右鍵功能表中選擇“選擇 ‘Joseph’ ”。現在按住 CTRL 鍵，然後對含有用戶端名 Charles 的一個記錄採取同樣操作。從右鍵功能表中選擇“隱藏未選定”，釋放 CTRL 鍵。

CTRL 與 SHIFT 鍵被用來選擇多個記錄。它們和在 Windows 作業系統環境下操作相同。

導出

使用 RAC 控制台“檔案”功能表中的“導出”功能可以將用戶端、警報日誌、事件日誌、掃描日誌和任務選項表的記錄輸出到本地電腦的一個檔中。使用“導出選定”選項可以僅導出某個選項表的選定文檔。

RAC 控制台支援多種輸出檔格式：HTML、逗號分隔 CSV 文件或分號分隔 CSV 文件。

列印

用戶端、警報日誌、事件日誌、掃描日誌和任務選項表的記錄可以通過標準印表機進行列印。

要配置列印輸出，到“檔案/頁面設置”，選擇“模式”，選擇 WISIWYG 模式或灰白比例模式列印。

在“表格”選項表下選擇是否列印圖表。在“頁首和頁尾”選項表上調整列印頁面的頁首和頁尾。

使用“預覽”按鈕預覽所要列印頁面。

記錄檔案

使用“編輯/刪除特定…”選項刪除警報日誌、事件日誌、掃描日誌和任務選項表的陳舊記錄。使用“指定日期”按鈕定義所要刪除的記錄。



任務

任務用來觸發遠端電腦上的病毒掃描，修改它們的配置，或者從 RAS 伺服器上更新 NOD32 防病毒系統。所有任務可以預先設定或者手工啟動。

任務選項表顯示了所有網路上目前預先設定的任務。從 RAC 控制台主功能表中選擇“檔案/新任務”創建一個新任務。你可以選擇下列類型的任務：

- 配置
- 手動掃描
- 立即更新

配置

使用這個任務可以修改網路上運行 NOD32 防病毒系統的任何電腦的配置。配置存儲在你電腦上的一個 XML 檔中。你可以利用 RAC 控制台提供的一個範本創建一個新的配置檔，或者從零開始創建。要從一個現有的範本中創建一個新的配置，可以在 NOD32 配置編輯器中選擇“從範本創建...”。使用一個現有配置選擇“選擇...”。從零開始創建一個新配置，使用“創建...”選項。

從用戶端列表中可以選擇應用新配置的用戶端。可以使用計畫器預設應用任務或者選擇立即運行。為了避免控制台視窗溢出，使用“自動刪除任務”，當成功完成時清空所有已經成功完成的任務。

如果要查看任何預設任務的詳細情況，雙擊它即可。

每個任務都有如下狀態參數顯示任務的當前狀態：

- 完成——客戶已經完成了這個任務
- 等待——客戶還沒有執行這個任務

手動掃描

手動掃描任務將觸發 NOD32 手動掃描引擎。手動掃描器配置存儲在一個 XML 配置檔中。如果要修改配置檔，使用 NOD32 配置編輯器或者手動掃描基本配置功能。

- 注意：遠端電腦上的手動掃描器以靜默模式運行，在這種模式下遠端用戶沒有任何視窗或警告字句會彈出。建議打開 NOD32 手動掃描器上的自動清除病毒選項或者掃描遠端電腦上的病毒，然後一對一處理。

立即更新

立即更新可以更新選定的遠端電腦上的 NOD32 防病毒系統。在默認配置下，遠端電腦會定期更新它們的 NOD32 病毒庫，所以沒有必要去預先設定立即更新這個任務。但是當大規模病毒感染在你的電腦網路中蔓延而並不是所有電腦



都已經更新了它們的病毒庫時，就可以使用立即更新任務。



報告

報告選項表上收集了你的電腦網路上病毒保護的相關統計資料。這種報告按
要求手動生成或者自動生成。

在“報告/類型”中可以選擇所要生成的報告。“報告/格式”選項可以在可
用的報告格式中轉換。

使用“過濾”工具可以篩選報告中所包含的記錄。有兩種可用過濾規則：
“目標用戶端”可以針對特定客戶生成一個報告，“病毒”可以針對病毒生成一
個報告。

使用“其他設置”部分可以設定報告中包含的其他詳細情況。

在間隔選項表上可以定義生成報告的時間跨度。

- 當前——選擇此項，報告將包括選定的當前時間週期的資料（例如本周）
- 完成——選擇此項，報告將包括先前時間週期的資料（例如上個月、上
周）。如果勾選上添加當前週期，可以包括當前時間週期的資料（例如
本周或本月）

示例

如果要在下個週三生成上周從週一到周日的報告，操作如下：

在報告/間隔選項表上選擇“完成”，並設定為一周。不要勾選上添加當前
週期可選框。在報告/計畫器選項表上設定頻率為每週，並選擇週三。

- 從/至——用它來定義生成報告的時間跨度

計畫器選項表可以使你定期的生成各種類型的報告。生成報告的頻率可以通
過頻率參數來設定。設定運行時間參數可以設置生成報告的時間，設定存儲結果
參數可以確定報告保存的檔夾位置。報告可以自動發送到一個預先設定的 e-mail
位址或者保存到本地硬碟上。

- 注意：如果要通過 RAC 控制台發送報告，需要在 RAS 伺服器設置中正
確設立 STMP 伺服器。

使用範圍選項可以選擇報告生成的時間範圍。可以通過使用“在…之後”參
數設定生成報告的數量，也可以通過設定“在…之前”參數設定報告生成時間週
期的終止時間。

使用“保存”或“保存為”按鈕可以保存你的配置。

所有的當前報告生成配置都可以在控制台視圖中顯示。如果要生成一個手動
報告，可以使用一個選定的報告生成配置的右鍵功能表中的“立即生成”選項完
成。



如果要查看最新的報告，到常規報告選項表上查找。

使用收藏視窗保存最頻繁使用的報告範本。如果要在收藏視窗中添加一個新的報告範本，使用報告範本視圖裏的右鍵功能表中的“添加到收藏”選項。

下列是預設報告的一個清單：

- Top 病毒——顯示在網路中發現的實體事例數量最多的病毒
- 最多警報的 Top 用戶端——顯示最多病毒警報的客戶
- 警報進度表——按照時間顯示警報數量進度
- 相對警報進度表——顯示指定病毒與所有病毒數量的比例
- 模組警報——顯示 NOD32 模組發出的病毒警報數目
- 物件警報——顯示感染物件發出的病毒警報數目
- Top 用戶端/Top 病毒組合——顯示被最多病毒類別中的病毒影響而發出最多警報的用戶端
- Top 病毒/警報進度表組合——按時間線顯示最多病毒類別中的病毒
- Top 病毒/相對警報進度表——顯示最多病毒類別中的病毒與選定病毒的比例
- 客戶報告、警報報告、事件報告、掃描報告、任務報告——顯示涉及所有上述資料類型的一個報告
- 全面報告——顯示下列報告的一個摘要：
 - Top 用戶端/Top 病毒組合
 - Top 病毒/相對警報進度表組合
 - 特定警報進度表

版權所有©1997-2003。保留所有權利。

本文檔使用的某些程式產品名和公司名可能是註冊商標或者其他公司所有商標。

Eset、NOD32 與 AMON 是 Eset 公司所有商標。

Windows 是微軟公司所有商標。