PA File Sight

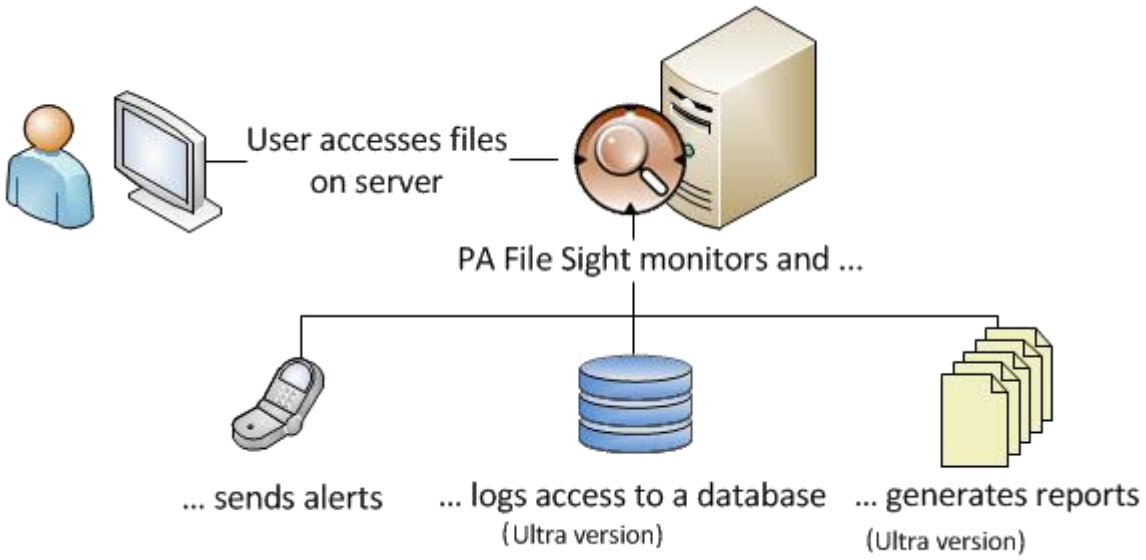
安裝操作說明

PA File Sight 的產品概述

產品架構與佈局

典型安裝（主要安裝）

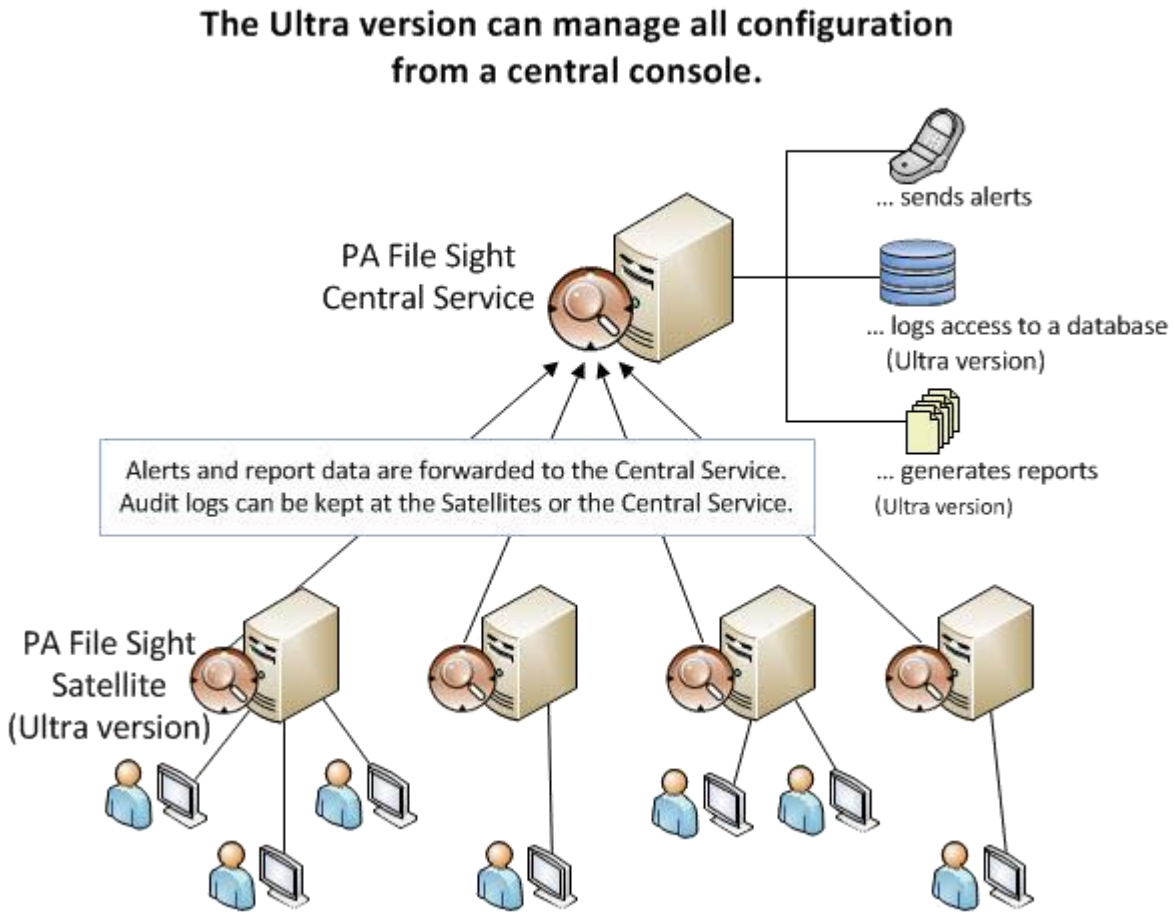
在每台 Windows Server 或 Workstation 上都安裝了監視服務。此監視服務將監視安裝在它上面的磁碟。



該安裝還會包括一個控制台 GUI 應用程序，用於處理和配置監視服務。

集中能力

除了監視本地伺服器上的硬碟之外，PA File Sight 的 Ultra 版本還可以管理對遠端伺服器的監視，包括透過 Internet 進行的監視，而無需 VPN。這是透過在其他伺服器或工作站上安裝 Satellite Monitoring Service 來完成的。衛星將監視自身（安裝它的伺服器）。警報和監視數據將透過 SSL 加密的 HTTP 發送回中央監視服務。



PA File Sight 的術語和概念

PA File Sight 在 Windows 電腦上運行，並監視該電腦上的文件活動。

PA File Sight 由兩部分組成：稱為控制台的圖形用戶介面和稱為監視服務（或中央監視服務）的後台進程。從桌面啟動 PA File Sight 時，您會看到控制台。中央監視服務是不可見的，並且沒有自己的用戶介面。

（中央）監測服務

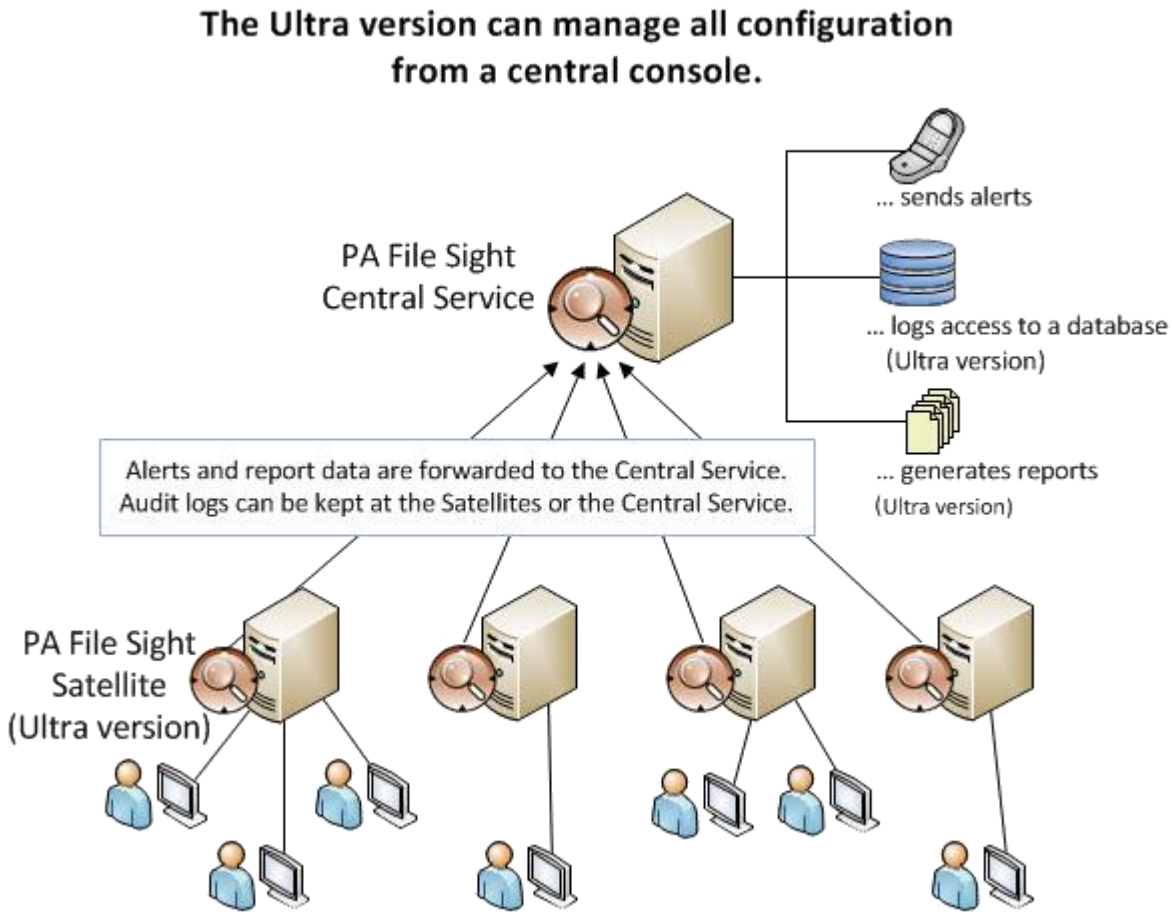
中央監視服務是產品的一部分，用於監視本地電腦上的文件活動。該服務設置為在 Windows 啟動時自動運行。控制台不需要運行即可進行監視。

如果僅監視單個伺服器，則它將是唯一的監視服務。如果正在監視其他伺服器，並且它們正在向該服務報告，則該服務稱為中央監視服務。請注意，Lite 版本不具有集中式功能，因此無法與其他 Monitoring Services 通信。

衛星監測服務（超版）

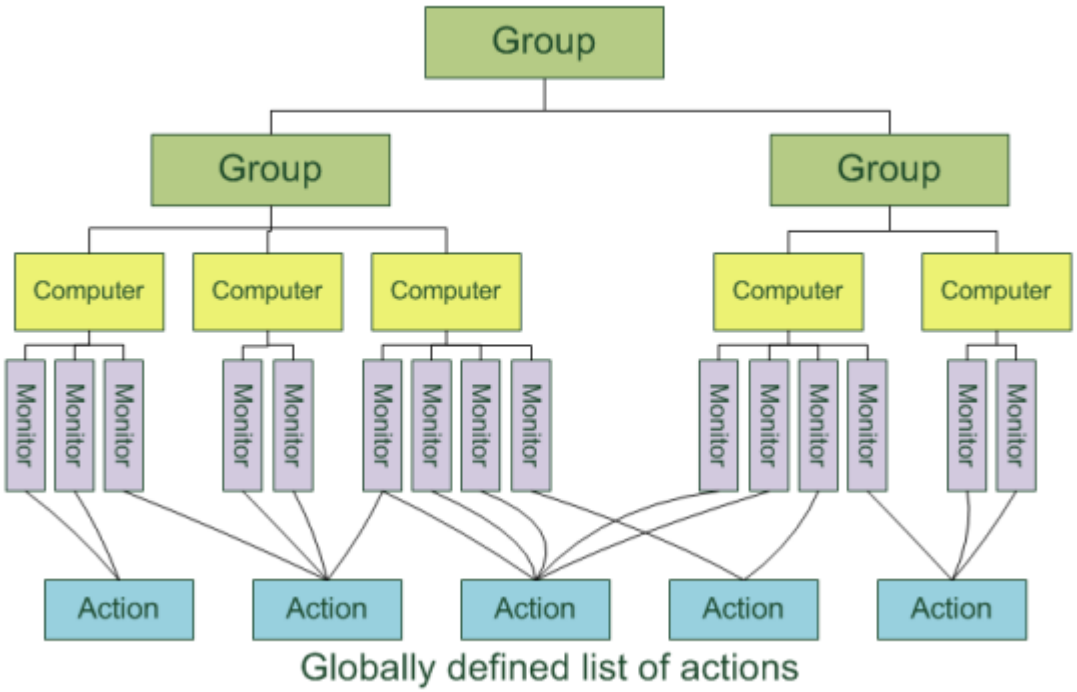
衛星監視服務（或簡稱為衛星）是可選的附加監視引擎。它可以像中央監視服務一樣在其他電腦上運行監視器。如果要對許多伺服器進行集中監視，配置和報告，通常會將衛星安裝在其他伺服器上，然後將它們指向中央監視服務。

注意：衛星監視服務僅在 Ultra 產品版本中可用。



產品術語

PA File Sight 基於群組、電腦、監視器、動作和報告的概念。它們在中央監視服務和/或衛星監視服務上運行。



群組（Ultra 版）

群組可容納電腦，也可以容納其他群組。它們供您用來組織您監視的電腦。您可以使用控制台將電腦和群組拖放到群組中。請注意，群組僅在 Ultra 版本中存在並且有意義，因為其他版本只能配置和監視單台電腦。

最好使用 Easy Deploy 添加新電腦。

組群狀態報告顯示群組中電腦的總體狀態。

電腦

電腦代表具有受監視硬碟的伺服器。監視器已建立並連接到電腦。

伺服器狀態報告是自動生成的，並顯示伺服器上監視器的狀態。

監控

監視器連續監視受監視硬碟上的文件和目錄活動，並將該活動與您指定的設置進行比較。檢測到的符合您條件的更改可以發出警報，並將 Ultra 版本寫入資料庫，以便可以運行歷史報告。

動作

運行一項動作以響應監視結果。動作示例包括發送電子郵件，執行腳本或將文本寫入日誌文件。動作僅定義一次，並且可以被系統中的許多監視器引用。也可以建立相同類型的多個動作（即，用於通知不同人員的不同電子郵件操作）。

報告書

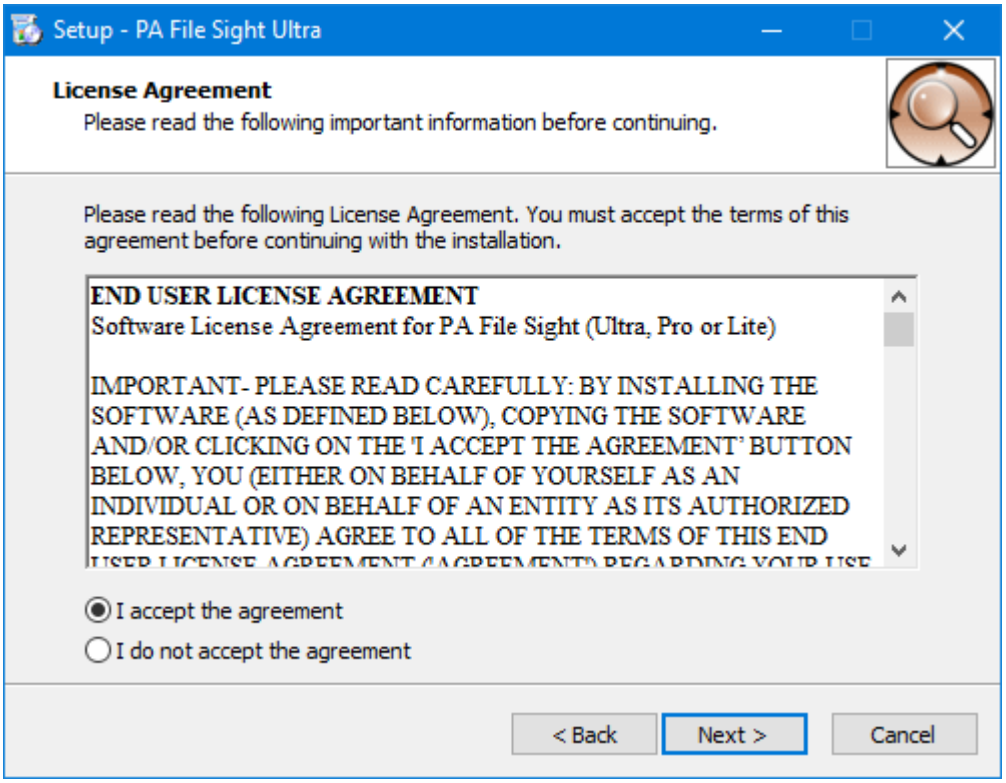
資料庫中的數據透過報告顯示（只有 Ultra 版本具有資料庫，而 Lite 版本則沒有）。您可以建立臨時報告以查看歷史數據。如果定期使用報告，則可以建立計劃報告。

安裝中央監控服務

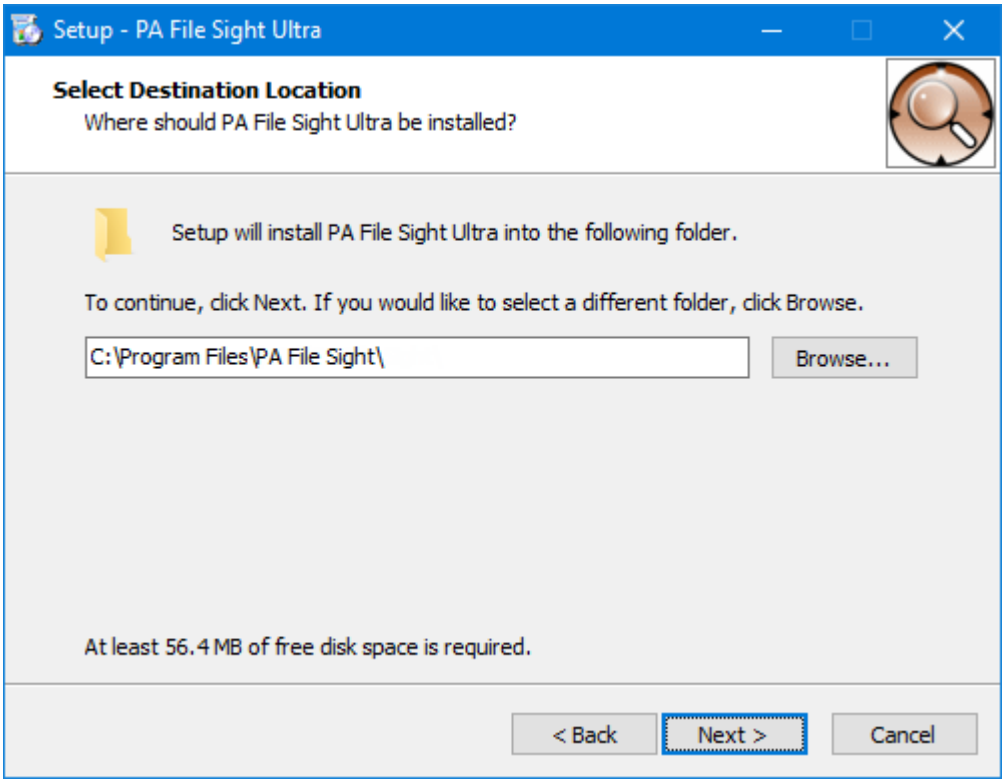
安裝中央監視服務

1. 運行 PA File Sight 安裝程序。出現“許可協議”頁面。

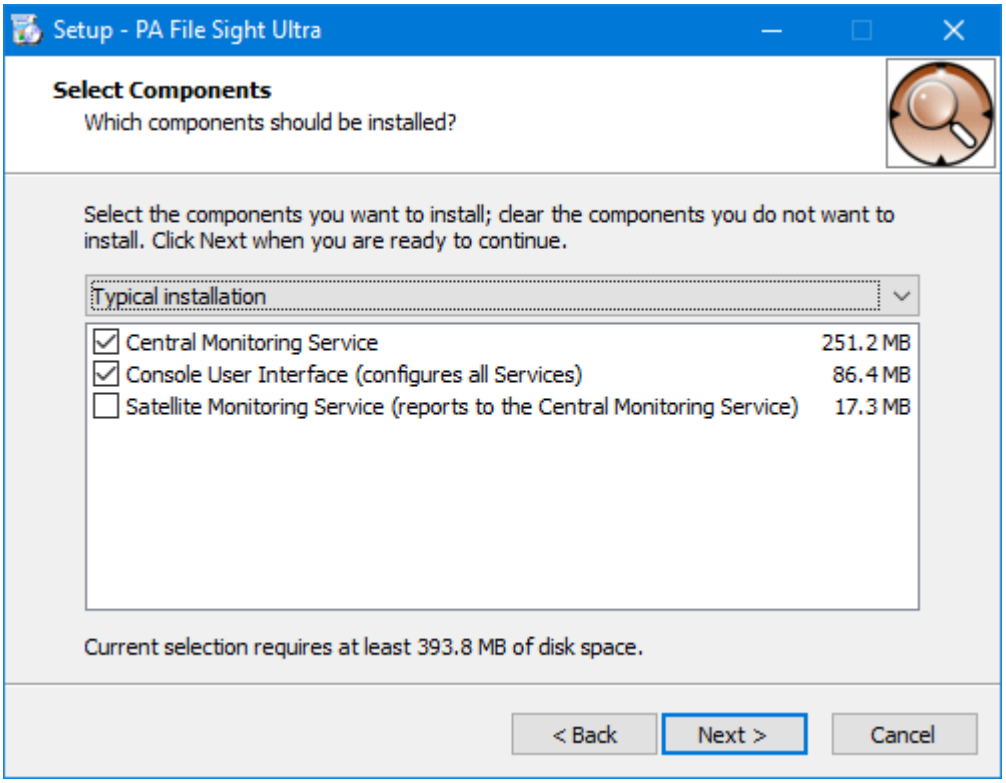
   注意：如果這是以前版本的更新，則安裝將停止現有服務。



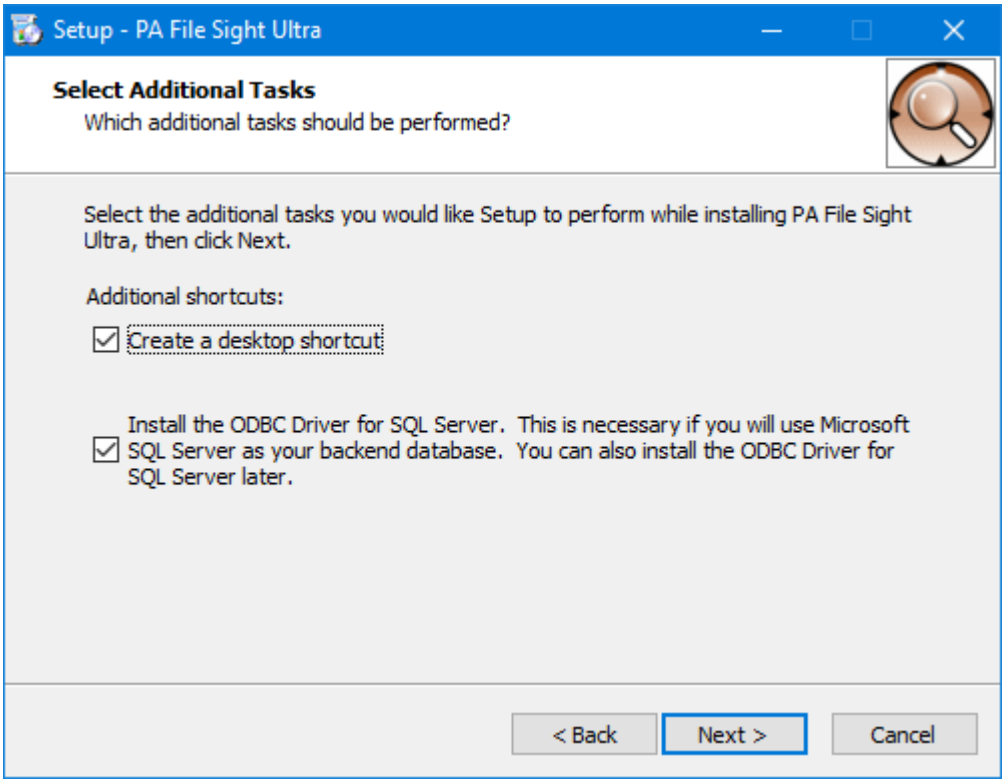
2. 選擇**我接受協議**選項，然後單擊**下一步**。出現“選擇目標位置”頁面。



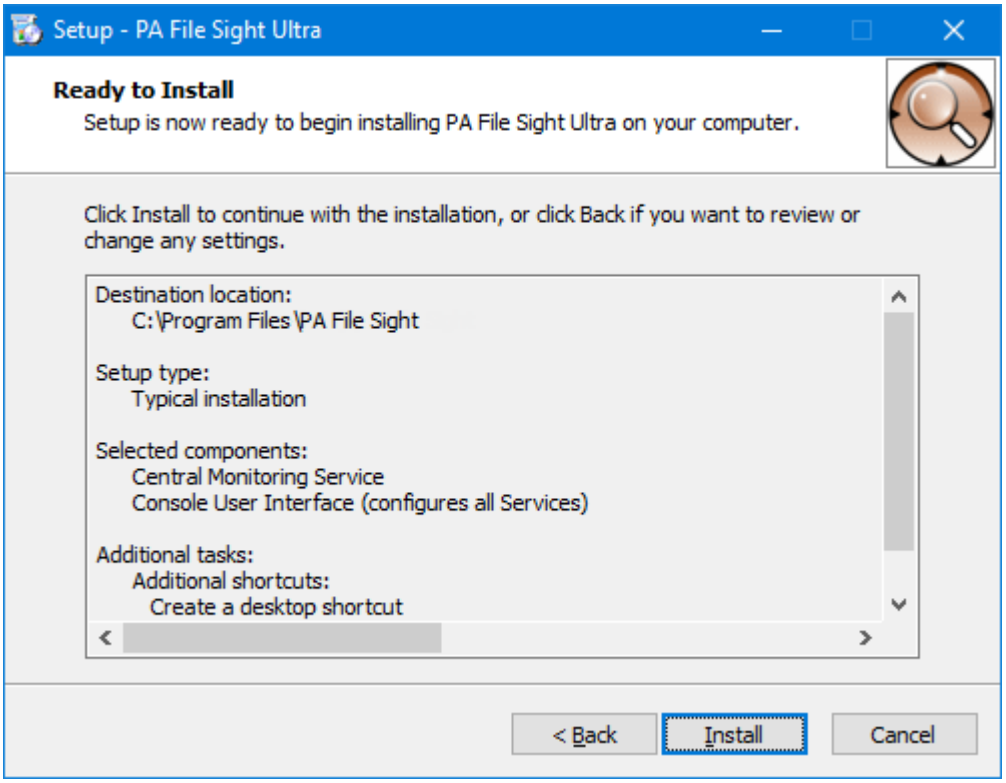
3. 請執行以下任一操作：
   - 接受默認文件夾路徑。
   - 在框中輸入一個新的文件夾路徑。您可以單擊**"瀏覽"**以顯示標準的 Windows 瀏覽窗口，然後導航到目標文件夾。
4. 單擊**下一步**。將顯示"選擇組件"頁面。



5. 接受默認安裝的默認值。您可以單獨選擇組件，也可以單擊**箭頭**，然後從列表中選擇安裝。對於首次安裝，請選擇帶有監視服務和控制台的默認“典型安裝”。
6. 單擊**下一步**。出現“選擇其他任務”頁面。

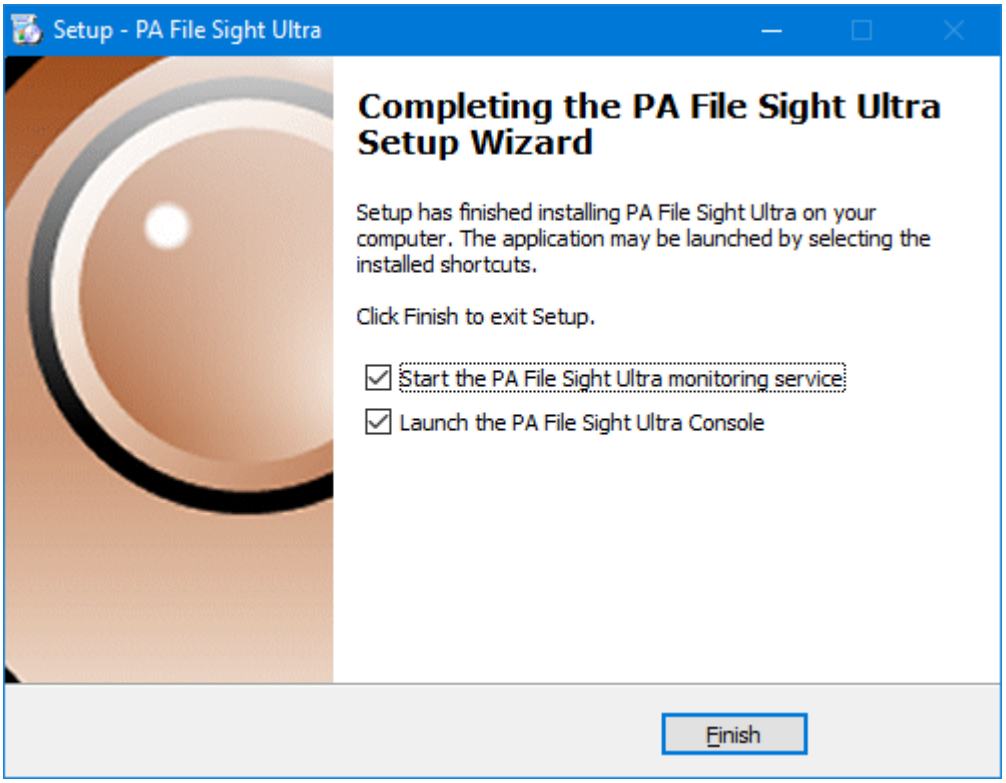


7. 如果要安裝將圖標放置在桌面上，請選擇“**建立桌面圖標**”選項。
8. 如果要將 Microsoft SQL Server 用作後端資料庫，請選擇“ **SQL Server 本機客戶端**庫”選項。如果您目前不確定，可以不選擇此選項-以後可以添加。
9. 單擊**下一步**。出現“準備安裝”頁面。

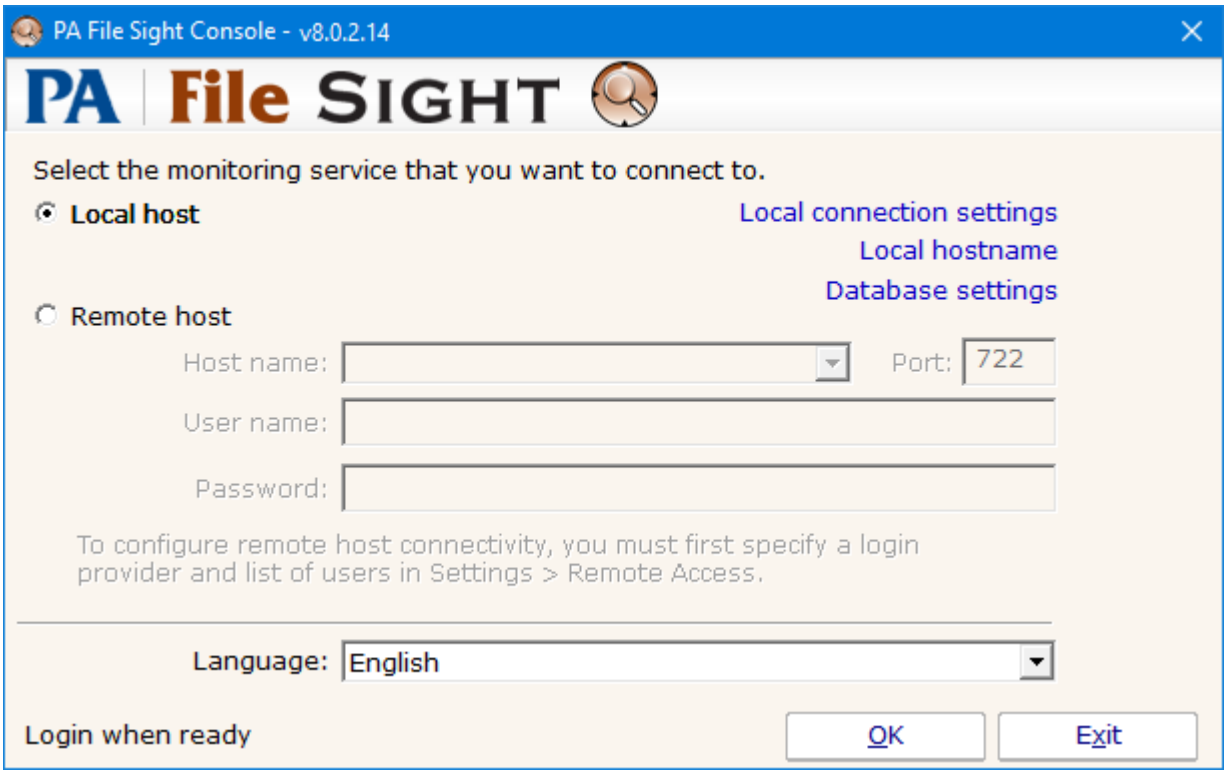


10. 選擇**試用許可證版本**。如果這是新安裝，則將要求您選擇要使用的跟踪許可證的類型。然後選擇安裝跟踪許可證。

11. 點擊**安裝**。出現安裝頁面。安裝完成後，將顯示“正在完成 PA File Sight 設置嚮導”頁面。



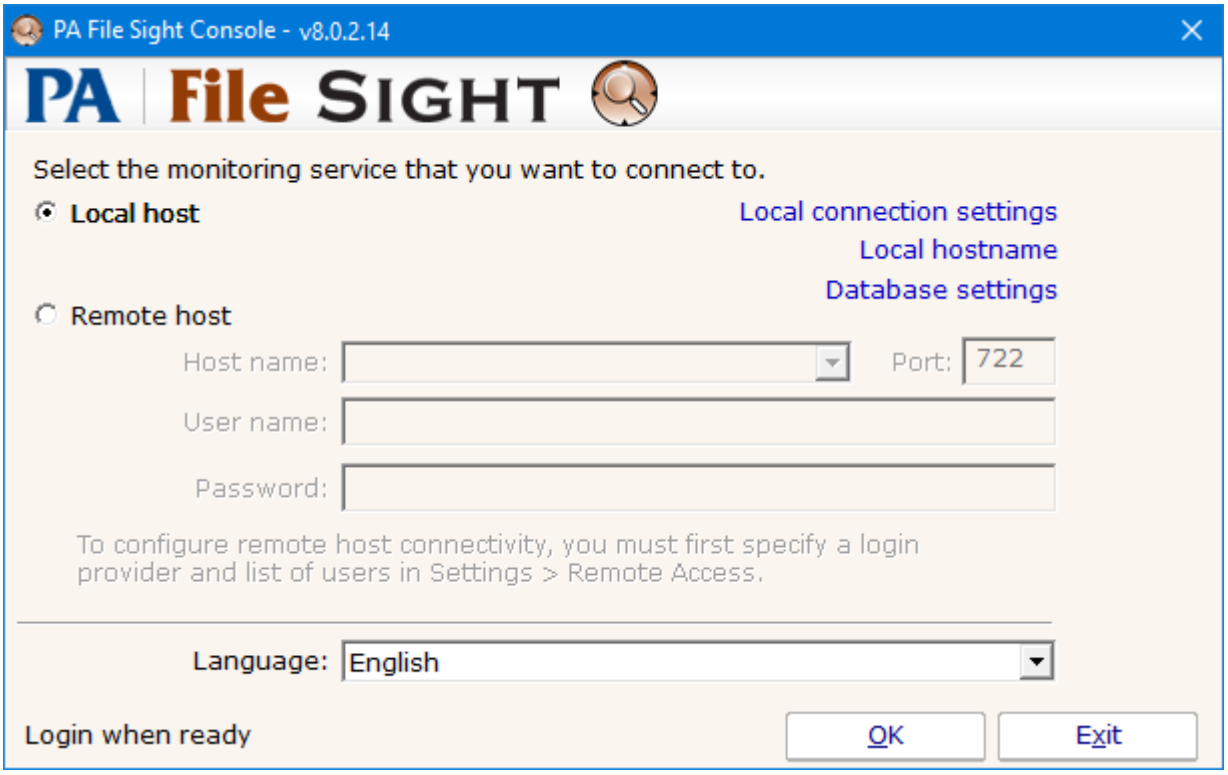
12. 透過選擇選項來指定是啟動 PA File Sight 服務還是啟動 PA File Sight 控制台，然後單擊**完成**。如果選擇了啟動控制台的選項，則會顯示“ PA File Sight 控制台”窗口。



啟動 PA File Sight 控制台

啟動 PA File Sight 控制台

1. 雙擊桌面上的 PA File Sight 控制台圖標。出現控制台連接窗口：

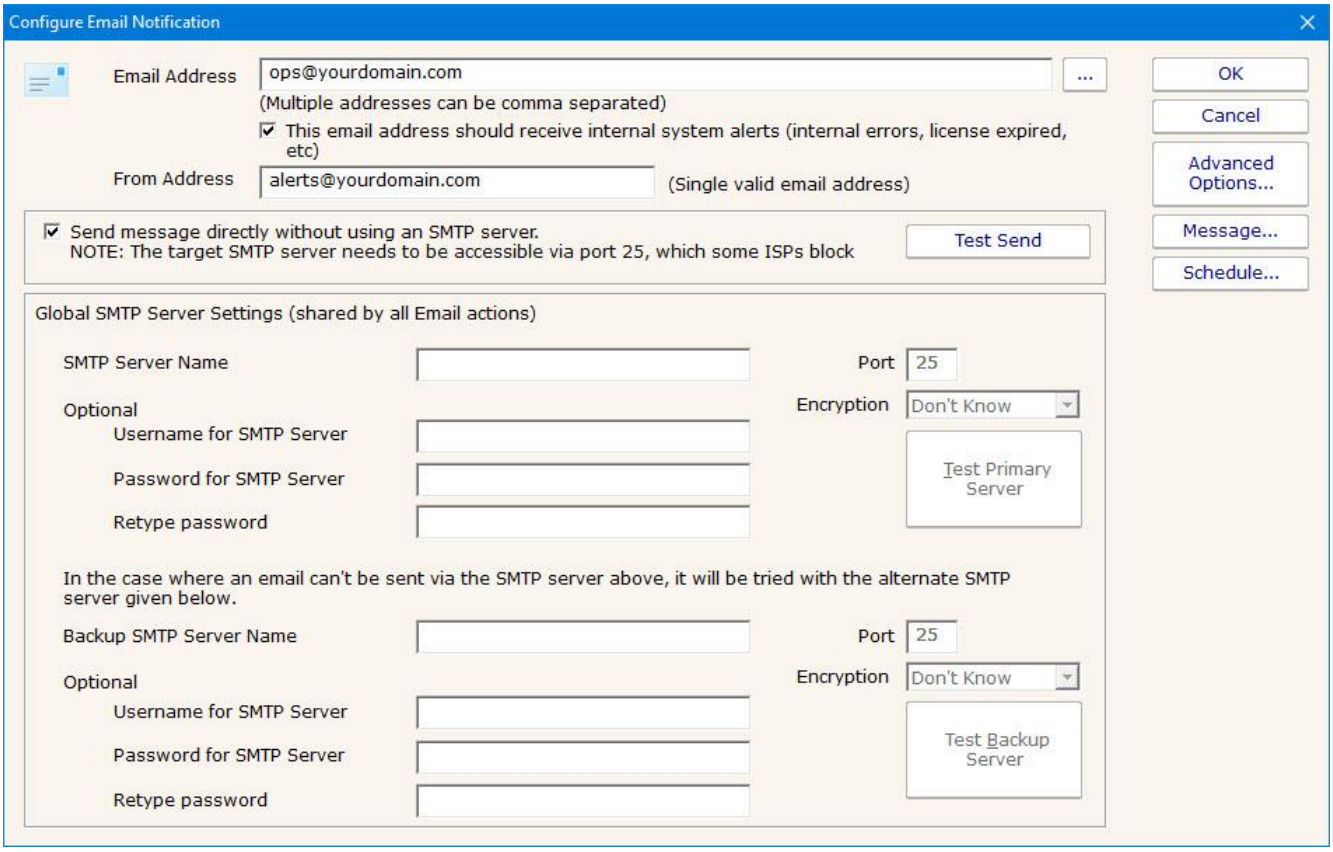


2. 請執行以下任一操作：
   - 選擇“**本地主機”**選項以連接到同一台電腦上的監視服務。
   - 選擇“**遠端主機”**選項以連接到遠端電腦上的主機。輸入遠程主機名、埠號、用戶名和密碼。注意：必須事先在“設置”->“遠程訪問”中配置了遠程訪問。
3. 單擊“**確定”**以連接並打開控制台 GUI。如果有任何錯誤，錯誤消息將提供有關如何解決它們的提示。
4. 該控制台介面將出現。

請注意，還有其他一些選擇。您可以選擇在對話框底部使用哪種嵌入式瀏覽器（Internet Explorer 或 Chromium）。您不需要安裝 Chrome 瀏覽器。
您還可以更改資料庫設置，伺服器 HTTP / S 設置以及連接到本地伺服器時使用的名稱（默認情況下為 localhost）。

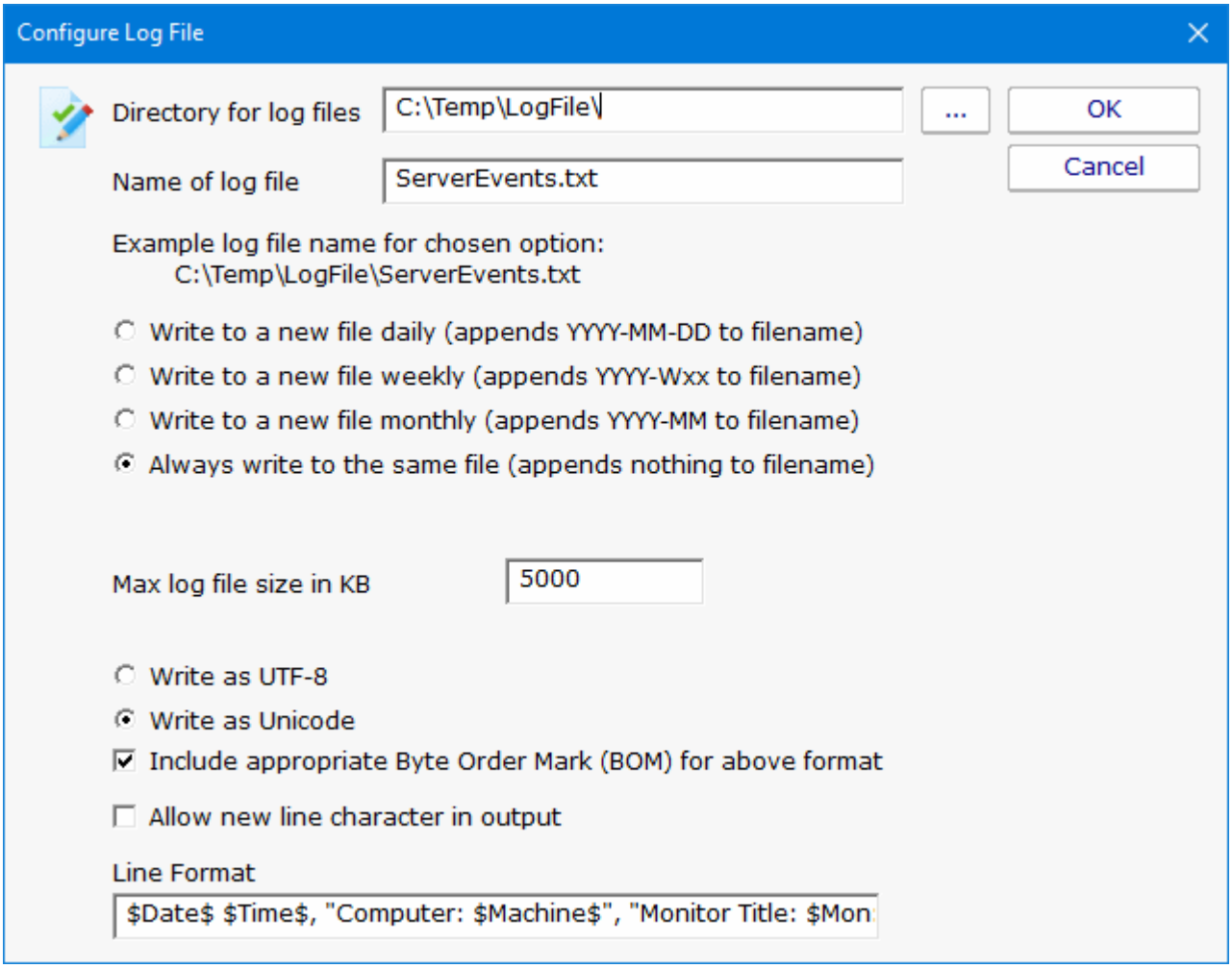
PA File Sight 啟動引導

此處提供的說明適用於首次運行 PA File Sight 時可以遵循的過程。
在“啟動引導”中將遇到的大多數畫面都是標準配置對話框，您可以從 PA File Sight 中使用這些對話框，之後您可以更改這些配置。
當您看到“歡迎”對話框時，請按“是”進入引導。按“否”返回到“ PA File Sight”（如果執行此操作，則將沒有任何配置，必須手動設置伺服器和其他受監視的設備。）如果按“是”，您將看到顯示的下一個畫面，“配置電子郵件通知”。



請參閱幫助頁面發送 SMTP 電子郵件以獲取指導。完成“配置電子郵件通知”畫面後，選擇“確定”。

下一個畫面可幫助您配置“寫入文本日誌文件”操作，監視器可以使用該操作來記錄發生的可讀事件。



完成此畫面後，選擇確定。

按確定繼續。此時，系統將提示您監視初始路徑。然後將建立 File Sight 監視器，並填寫此路徑。這將完成啟動引導。

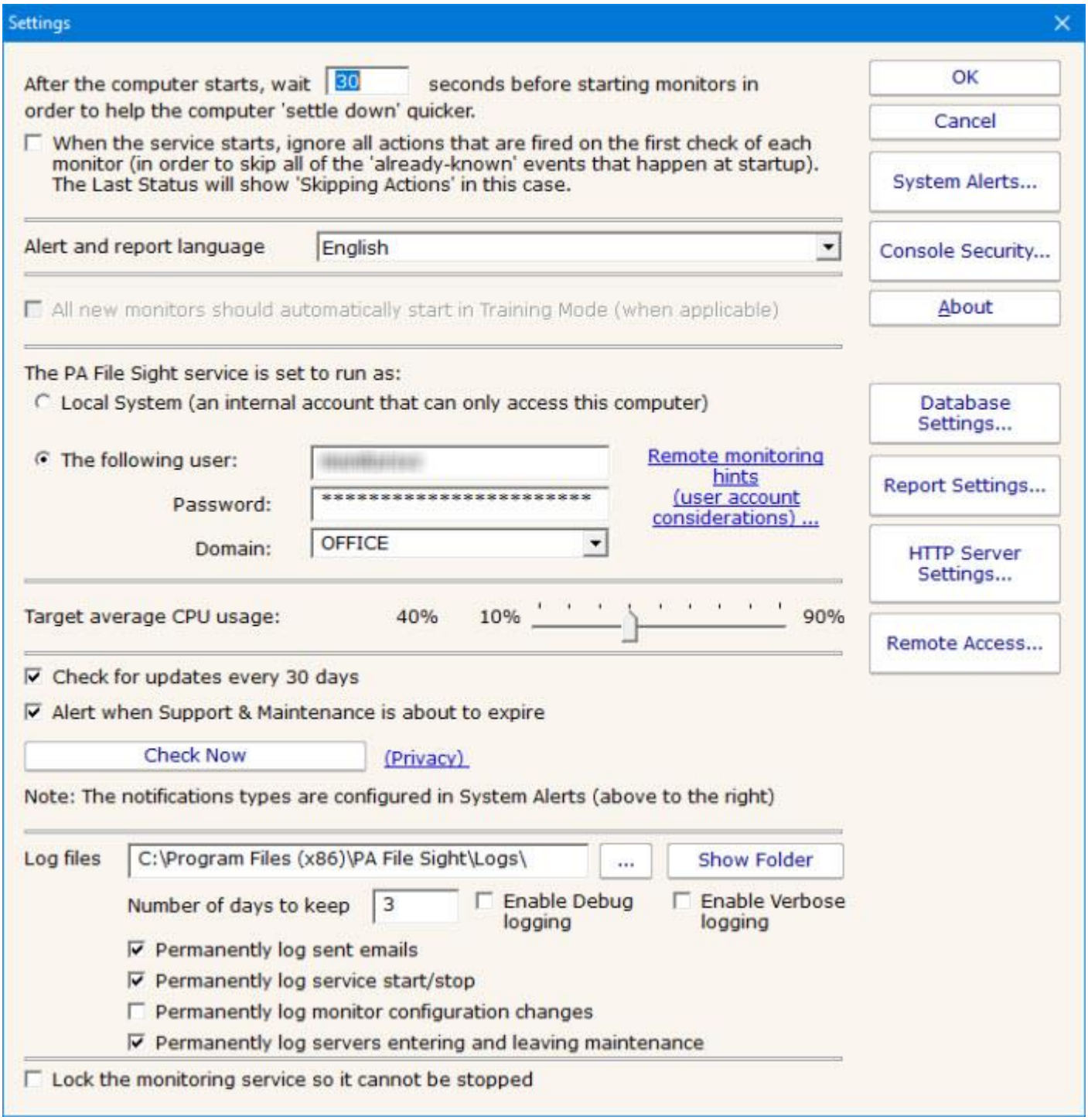
全局設置

使用“設置”對話框可以配置監視服務的全域設定。

該對話框右側的按鈕可以訪問多個對話框，也可以透過“設置”選單進行設定。

- **系統警報**－一些警報是從監視系統本身發送給您的，而不是來自特定的監視器。這些警報包括安全警告（配置更改等）、許可證問題、內部問題、無法訪問的電腦警告等。您可以控制啟用這些內部警報中的部份設定，以及每個警報應使用的通知方法。
- **控制台安全性**允許您設置控制台啟動時將要求的密碼。此設置允許您將對 PA File Sight 的訪問限制為授權用戶。
- **“資料庫設置”**對話框允許您設置 PA File Sight，以使用嵌入式 SQLite 資料庫或 Microsoft SQL Server 作為 PA File Sight 數據的儲存。
- **報告設置**會影響已存檔報告的儲存以及 PA File Sight 的報告功能的行為。

- **HTTP Server Settings（HTTP 伺服器設置）**允許您更改 PA File Sight 中內置 Web 伺服器操作方式的詳細訊息。
- **遠端訪問**允許您指定哪些用戶可以使用遠端控制台連接到中央監視服務和/或訪問 PA File Sight 中的報告。



啟動等待時間－監視服務啟動時，您可以指示它等待幾秒鐘，然後才開始主動監視。這樣可以在啟動時減輕系統負擔，還可以減少由於系統未完全啟動而引起的錯誤警報。

忽略第一個動作－為了進一步減少錯誤警報，監視器服務可以忽略每個監視器第一次運行時發現的問題。第一次運行後，所有監視器將正常運行。

警報和報告語言－更改所有報告和警報的顯示語言。
從培訓模式開始－大多數監視器支持自動培訓（請參閱 高級監視器選項）。首次創建監視器時，它們可以自動進入培訓模式。在大多數情況下這很方便，但是這意味著監視器可能最初會較難測試，因為在培訓期結束之前它不會觸發動作。
服務帳戶－這是*非常*重要的設置。透過此設置，您可以控制使用哪個用戶帳戶來運行監視服務（這與您可以在"管理工具"->"服務"程序中為每個服務設置的設置相同）。此帳戶是監視服務在監視所有資源時將使用的帳戶。
注意：

- 默認的 Local System 帳戶可以訪問所有本機資源，但不能訪問任何遠端 Windows 資源（但是可以訪問非 Windows 遠機資源，例如 ping，網頁等）。
- 如果要監視遠端系統，請選擇"The following user"單選按鈕，並將用戶名和密碼設置為網域帳戶或與遠端系統上的帳戶具有相同用戶名和密碼的本機帳戶（請參閱遠端監控提示）。另一種選擇是右鍵單擊監視控制台中的電腦，然後為伺服器選擇特定的憑證 "類型和憑證"→"設置登錄憑證"。

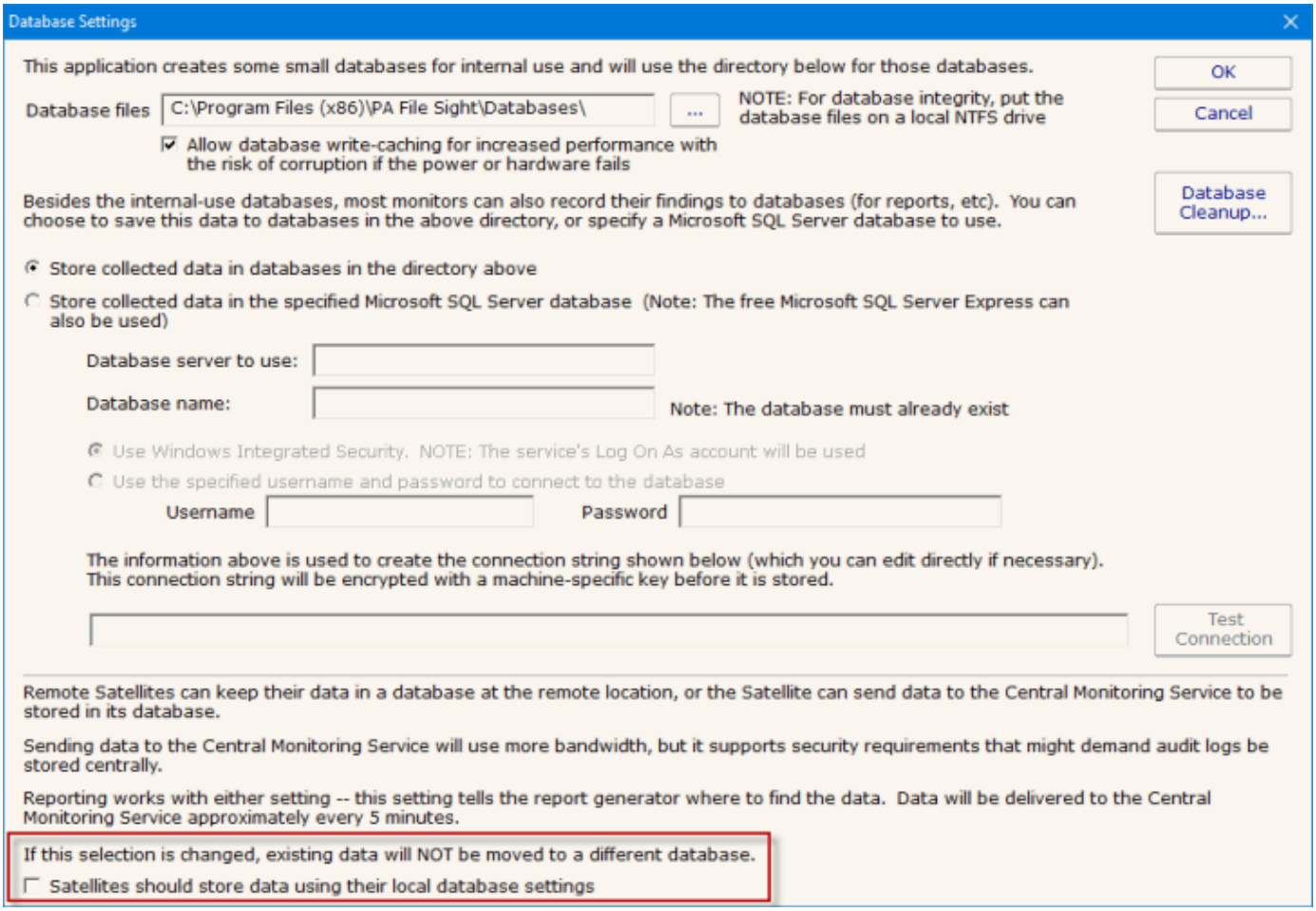
CPU 節流－監視服務具有內置的高級 CPU 節流功能，可將平均 CPU 使用率保持在您設置的值或附近。請注意，在建立報表的過程中，CPU 使用率有時會超過限制水平，但不會停留很長時間。
更新檢查－監視服務可以定期檢查是否有可用的較新版本的軟體，並透過警報電子郵件"動作"通知您。我們非常重視隱私：請查看更新檢查中內置的隱私注意事項。
日誌文件－監視服務在運行時寫入診斷日誌文件。您可以控制日誌文件的最大大小。達到最大值後，將刪除日誌文件開頭的一部分，然後新訊息繼續寫入文件末尾。調試日誌記錄會在很短的時間內將大量數據寫入日誌－除非 Power Admin 支援人員需要使用它來診斷問題，否則通常不應該啟用它。

- 服務日誌文件的儲存位置。可以透過輸入新位置來更改此位置。
- 您要保留日誌信息的天數。
- 有兩個"調試"選項可讓您收集更多信息，以調試監視問題。您通常不會打開此功能，因為日誌文件中記錄的數據量會快速增長並建立大型日誌文件。
- 有四個選項可將某些事件記錄到永久日誌文件中（這些日誌文件在一段時間後不會被移除）。這些日誌文件不受您為保留日誌訊息的天數設置影響。這些日誌文件中保留的事件包括發送電子郵件、服務啟動和停止、監視配置更改以及登入和退出維護。

鎖定監視服務－監視服務可以被鎖定，因此無法停止。這樣可以防止使用 services.msc 或 NET STOP 命令停止該服務。仍然可以卸載產品。還可以從控制台升級並重新啟動服務。要鎖定衛星監視服務，請使用 Bulk Config 中的"衛星：鎖定服務（這樣服務就不會停止）"選項 。

資料庫設置

PA File Sight 需要一個地方來儲存其在操作期間收集的數據。有兩種選擇可用於數據儲存。



SQLite（内建）

SQLite 是高度可靠的開源資料庫。默認情況下，PA File Sight 將其所有數據儲存在 SQLite 資料庫中。您可以透過選擇標題為“Store collected data in databases in the directory above”的單選按鈕進行選擇。這是最簡單的選擇，也是大多數用戶在使用 PA File Sight 時所做的選擇。

資料庫文件將被建立並儲存在指定目錄中。即使為資料庫選擇了 MS SQL Server，少量數據仍將儲存在指定的資料庫目錄中。

Microsoft SQL 伺服器

要使用 SQL Server 進行儲存，您需要安裝 SQL Server Native Client 庫，這是 Microsoft 最新的資料庫連接技術。SQL Server Express 資料庫適合大多數安裝，但請注意，它們會將資料庫的總大小限制為 10GB（對於 SQL Server 2008 R2 Express）。

如果您在安裝時未安裝本機客戶端庫，則現在可以通過啟動名為的安裝文件 sqlncli.msi，該文件位於 PA File Sight 的主目錄中（通常是）C:\Program Files\PA File Sight。

需要指定以下配置數據才能使用 SQL Server：

- 伺服器名稱-SQL Server 實例所在的伺服器的名稱。（請注意，對於 SQL Express，這通常是 {server_name} \ SQLEXPRESS）
- 資料庫名稱-將用於 PA File Sight 儲存的 SQL Server 資料庫的名稱。資料庫在使用前必須存在，並且可以為空（意即，請自行先建立一空的資料庫供儲存 PAFS 資料）。

- 用戶名和密碼－根據 SQL Server 實例的要求。
- 連接字符串-輸入上面的配置信息時，PA File Sight 將自動建立連接字符串。您可以根據需要手動編輯建立的連接字符串。
  注意：如果您正在使用資料庫鏡像，則可以手動添加 Failover_Partner 參數以指定要連接的備用資料庫。

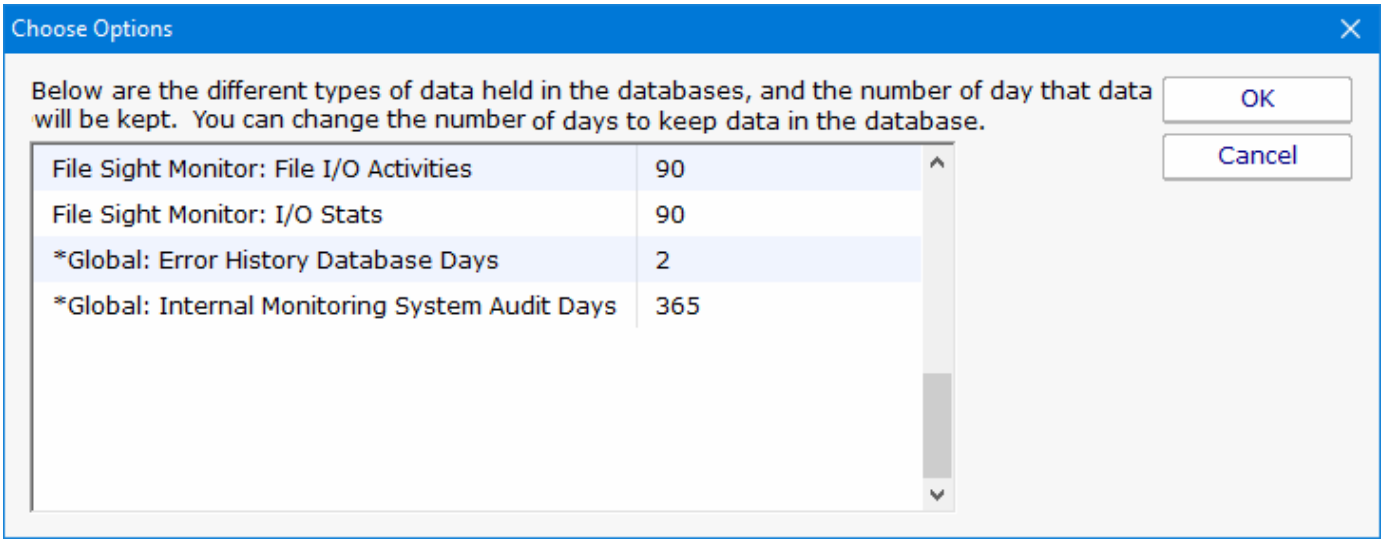
如果您不需要或希望將 SQL Server 用作 PA File Sight 的資料庫，則不需要安裝 SQL Server Native Client Library。

變更資料庫

如果更改資料庫設置，將提示您是否要將現有數據從當前資料庫複製到新資料庫。根據您當前資料庫的大小，這可能會花費一些時間（具有 6GB 資料庫的大型安裝可能需要一天的時間進行傳輸）。

資料庫清理

資料庫無需維護。所有監視器都會自動從資料庫中自動刪除舊數據，以幫助控制資料庫的增長。您可以通過“Database Cleanup”按鈕控制監視器保留多少天的數據。



資料位置

使用 Satellite 時，出現了將稽核數據保存在何處的問題。默認情況下，每個 Satellite 使用其自己的資料庫設置（這意味著每個 Satellite 默認將數據儲存在其自己的本機 SQLite 資料庫中）。您可以指定每個 Satellite 連接到 MS SQL Server 資料庫並在其中儲存其數據。底部的複選框提供了另一個選項：集中式資料庫儲存。

集中式資料庫儲存

透過取消選取“資料庫設置”對話框底部的複選框，您可以指示從屬設備將其所有文件 I / O 審核結果轉發給中央監視服務。然後，中央監視服務會將數據儲存在配置為使用的資料庫中（本機 SQLite 或 MS SQL Server，如上定義）。衛星將在內存中緩存文件 I / O 記錄，然後每隔幾分鐘

將記錄傳遞給中央監視服務。如果與中央監視服務的連接不可用，則記錄將被緩存在內存中，直到連接可用。

性能考量

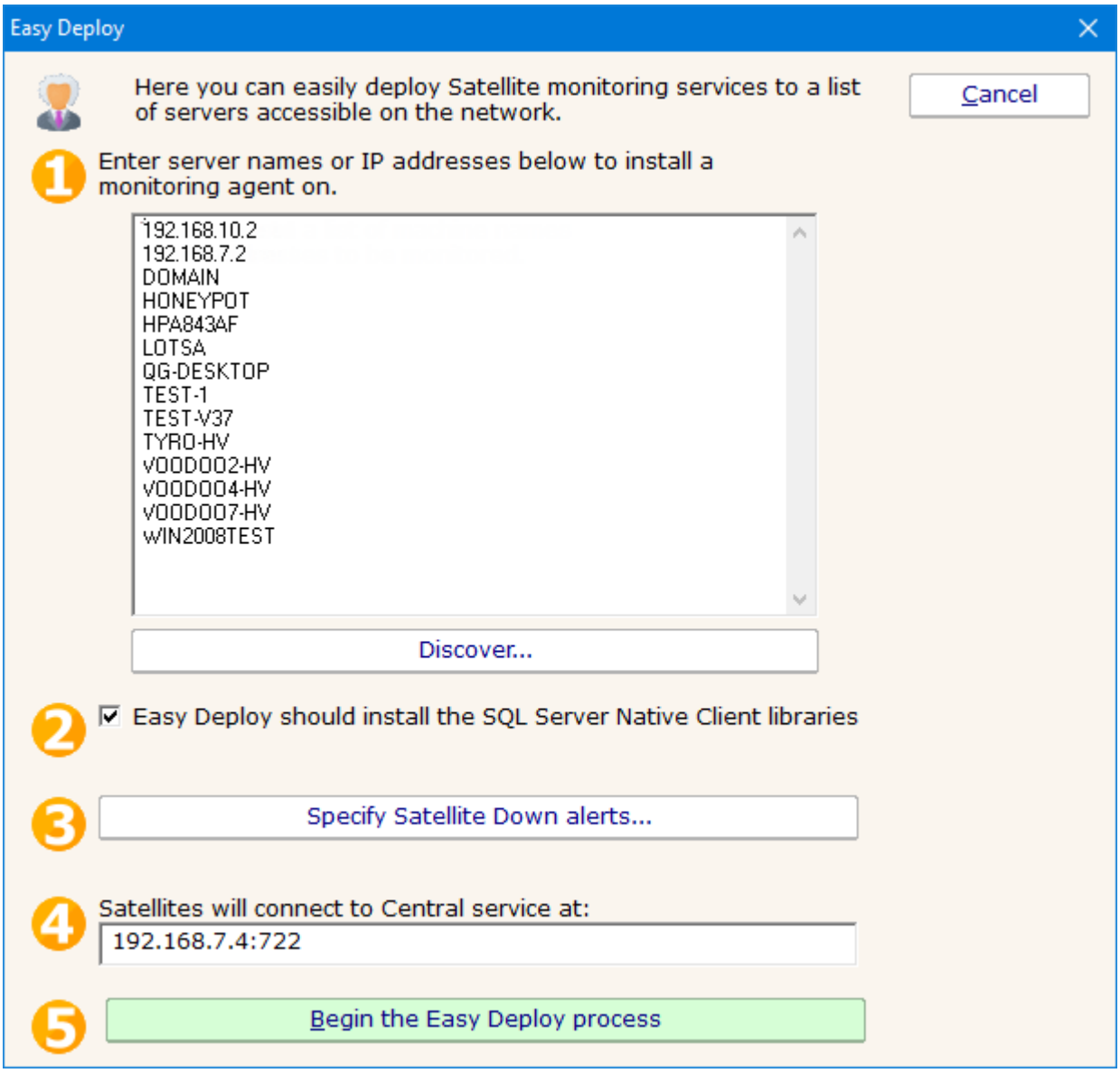
“集中儲存”設置將給中央監控服務，與之連接的網絡以及資料庫連接增加一些負載，這是一定的。在將 500 台衛星連接到中央監視服務的測試中，我們發現 MS SQL Server 可以輕鬆跟上。嵌入式 SQLite 可以滿足寫入請求，直到大約 100 至 200 台伺服器為止。使用的網路頻寬令人驚訝地輕。每分鐘，每台 Satellite 將建立約 4 個 HTTPS 連接。大約每分鐘將有 4KB 發送到中央監視服務，大約 2KB 將被發送回衛星。這些值可能會因監視器配置而有很大差異。在**[系統總結報告] →系統統計** 該報告顯示了每個 Satellite 的頻寬使用情況，這是一種針對您的特定配置進行檢查的好方法。

報告不受“集中式資料庫儲存”設置的影響。如果數據保存在中央資料庫中，則報表將查詢該資料庫。如果數據儲存在從屬位置，則在為報告的一部分生成報告時將查詢從屬。

請注意，更改集中式資料庫儲存設置後，資料庫中的現有數據不會移動到新位置，並且在某些情況下對於查詢是不可見的。

簡易部署

Easy Deploy 旨在幫助將 Satellite Monitoring Service 軟體推入應監視的伺服器。



只需按照橙色數字概述的步驟進行操作：

1. 輸入伺服器列表以接收 Satellite 軟體。“Discover”按鈕可用於執行 ping 掃描並為您查找本地網路上的伺服器。將使用它們的管理員共享與這些伺服器建立連接。這意味著您將希望 PA File Sight 服務作為將授予這些伺服器訪問權限的網域帳戶運行，或者在伺服器名稱旁邊的每一行中添加用戶名和密碼，例如：
   192.168.10.2，administrator，p @ assW0RD
2. 當 Satellite 未連接到中央監視服務時，您會收到一個可選警報。此按鈕控制。以後可以在各個 Satellite 上進行更改，也可以通過 Bulk Config 一次進行更改。
3. 附屬伺服器必須知道伺服器名稱和通訊埠才能連接到中央監視服務。默認值在大多數情況下都可以使用，但是如果需要使用其他電腦名稱（也許是 IP 位址），則可以在此處進行更改。一旦送出部署後，您可以根據需要在每個衛星上對其進行更改。
4. 開始！該過程開始時，您將進入一個報告，該報告每 30 秒更新一次，顯示進度。

部署過程

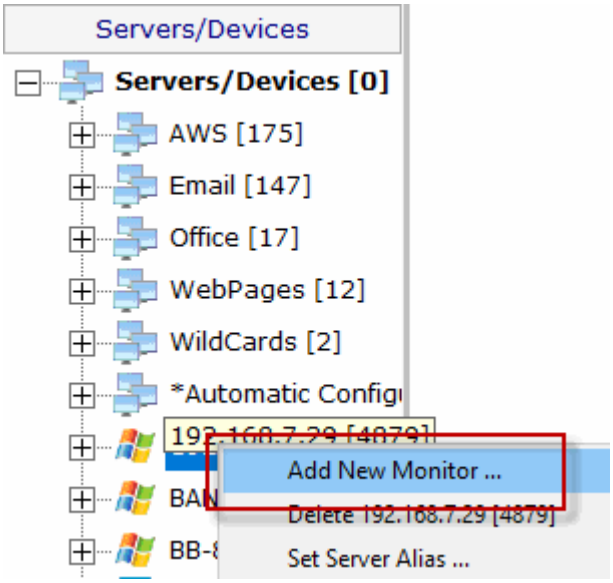
部署過程將自動執行以下步驟：

1. PA File Sight 的 Setup.exe（從產品的 Install 文件夾複製）通過管理員共享發送到遠端伺服器。
2. PA File Sight 的 Setup.exe 程序通過 RemCom 啟動，RemCom 是類似於 Microsoft PsExec 程序的開源軟體包。
3. Setup.exe 將以靜默方式在目標伺服器上安裝 Satellite 組件。安裝程序永遠不會指示要重新開機。
4. 衛星服務將被啟動，並被告知使用上面指定的伺服器名稱和通訊埠連接到中央監視服務。
5. Satellite 將連接，Easy Deploy 進程將自動接受它，然後添加一台電腦（Satellite 本身）以由 Satellite 監視。

此時，您可以將監視器添加到目標伺服器。

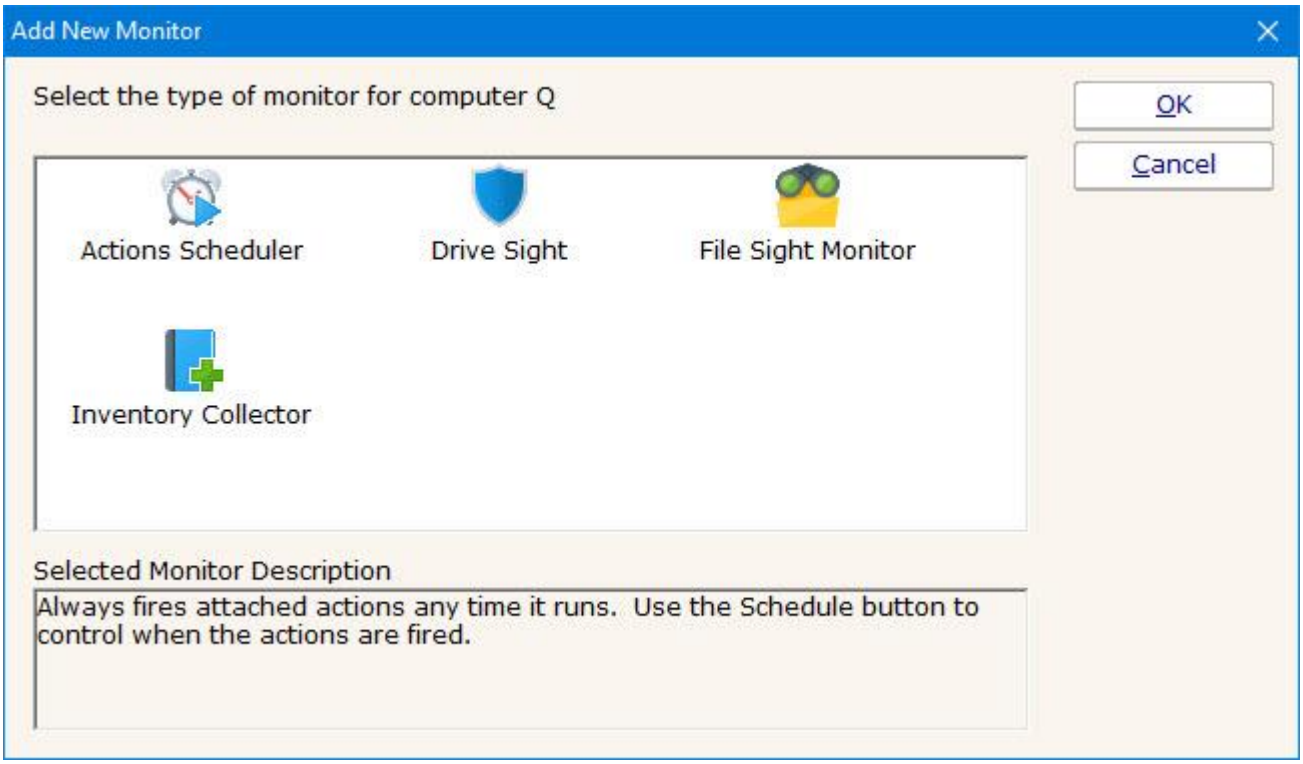
新增監視器

將監視器添加到現有電腦非常容易。在導航窗格中選擇電腦，然後右鍵單擊。選擇“新增新監視器...”菜單項。



將在下面的對話框中顯示您的產品和許可證的所有可用監視器（請注意，它們可能與圖中所示的監視器不同）。

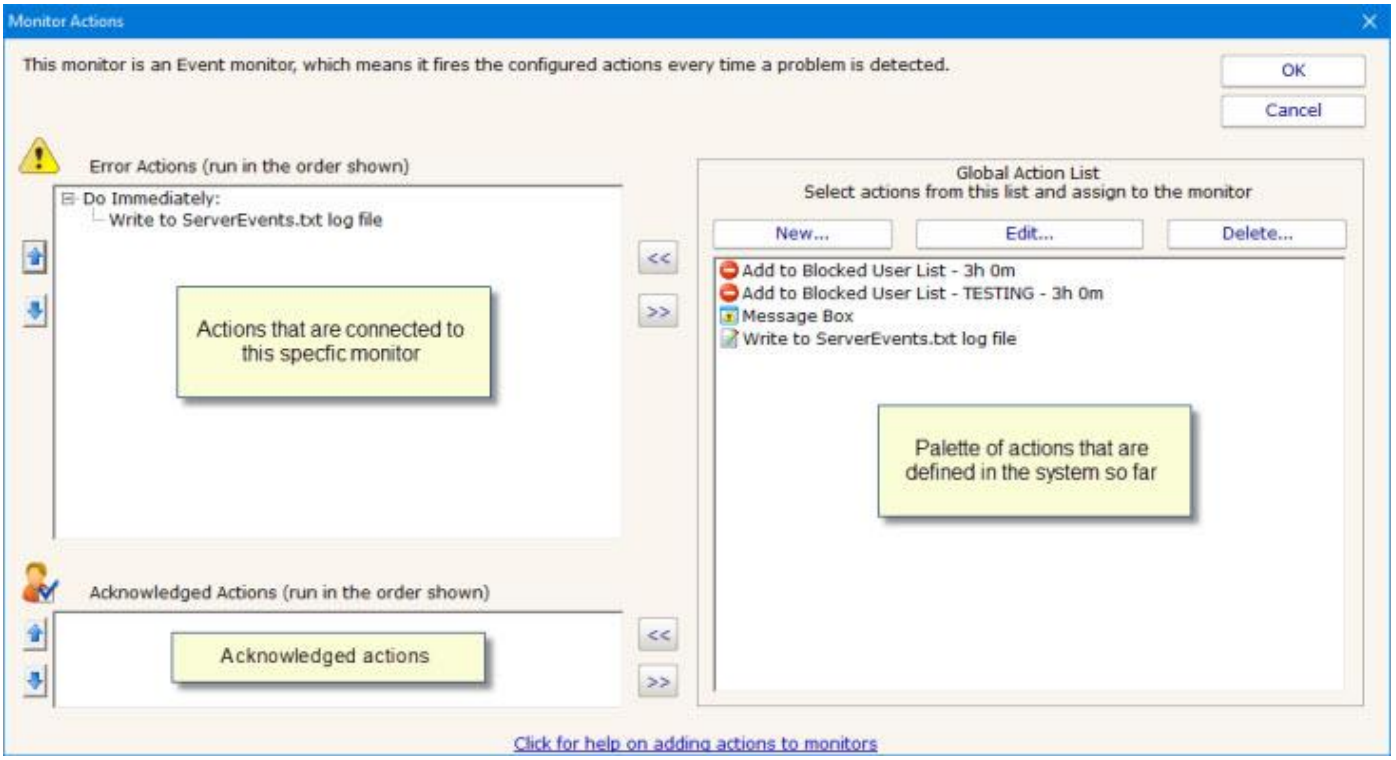
選擇監視器後，將顯示該監視器的配置對話框。



選擇所需的監視器類型，然後按 OK。然後將顯示監視器的配置對話框。

新增動作

動作對話框如下圖所示。（根據所配置顯示器的功能，該對話框看起來可能與下圖所示略有不同）。



左側顯示了此特定監視器附帶的所有動作。當監視器“觸發動作”時，它將按所示順序運行該動作列表。您可以使用藍色的向上和向下箭頭按鈕更改順序。	右邊是到目前為止定義的所有動作的列表。任何監視器都可以使用這些動作。 如果您需要未列出的動作（例如另一個電子郵件動作或“啟動應用程序”動作），請單擊全局操作列表上方的“新建...”按鈕。 您可以在此列表中編輯操作，所做的更改將反映在使用該操作的每個監視器中。

要將動作新增（或附加）到監視器，只需在右側的全局列表中選擇該動作，然後按綠色  按鈕將動作移至左側特定於監視器的列表，然後移至“立即執行”節點。（對於支援持事件升級的監視器，可能會顯示其他節點）