Tivoli Access Manager for Enterprise Single Sign-On (TAMESSO) 疑難排解

等級：中級

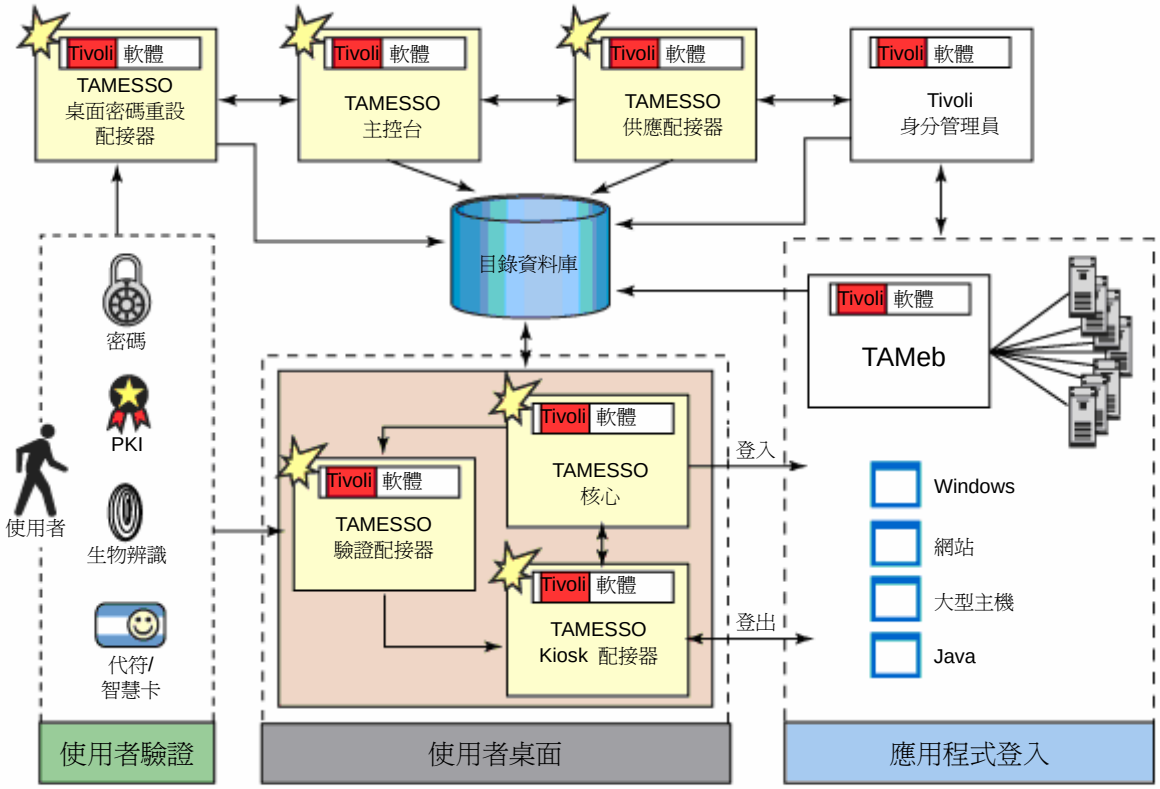
Giancarlo V. Marchesi (gmarches@us.ibm.com)，IBM 解決方案架構設計師
Rajalakshmi Iyer (iyer_rajalakshmi@in.ibm.com)，IBM 軟體工程師

2007 年 10 月 1 日

本文可協助部署與運作 IBM® Tivoli® Access Manager for Enterprise Single Sign-On (TAMESSO) 產品的客戶、事業夥伴，以及 IBM 顧問，擴展其部署技巧。本文將說明各種常見問題的疑難排解技巧，並且有助於解決 TAMESSO 與其他產品整合時所遭遇的問題。

TAMESSO 推出一次驗證使用者的安全中間層，提供單一登入功能，接著並可自動偵測與處理使用者認證的後續要求。這是智慧型用戶端軟體，可代表使用者直接從其桌面回應登入要求。適當的應用程式輔助物件接著會自動提供正確認證，回應各應用程式的登入要求。此軟體可支援從任何認證介面（例如密碼、生物辨識、代符和智慧卡）和認證服務（例如 Microsoft® Windows®、Entrust PKI 或 LDAP）所進行的認證。軟體可搭配幾乎所有的 Windows、Web、專有與主機式應用程式立即使用，從而降低 IT、服務台與整合成本。下圖說明了 TAMESSO 的架構。

圖 1. TAMESSO 架構示意圖



TAMESSO 日誌

構成 TAMESSO 的元件爲分散式。管理員需要知道各元件間的互動情形，以及進行任何問題除錯時所需參考的日誌記錄。下表詳細說明了與 TAMESSO 相關的日誌記錄，以及啓用這些記錄的時機和方式。請注意，對所說明登錄檔設定的變更，必須在重新啓動 TAMESSO 後（會在電腦重新開機和用戶端啓動時自動發生）才會生效。

表 1. TAMESSO 疑難排解時可參考的重要記錄

日誌類型	啓用時機	如何啓用
事件日誌	啓用事件日誌，監控各種使用者事件，包括用戶端開機與關機、登入、密碼變更、認證資料更新、認證介面變更、備份與還原等。事件可記錄到任何想要的位置，包括本機 XML 儲存、SNMP 服	事件日誌爲 TAMESSO 的選擇性功能，可在自訂安裝時啓用事件管理員 (Event Manager) 和所需的延伸程式進行安裝。事件會快取暫存一段特定時間，並透過選定的延伸程式定期清除。若要設定記錄的事件與延伸程式，請移至 TAMESSO 管理主控台	全域代理程式設定 |<選定一組>| 事件記錄：

	務、Windows 事件日誌或是目錄伺服器。	• 勾選**選擇要記錄的事件**勾選框，並從可用清單中選擇事件。 • 移至**進階**標籤，並提供其他設定，像是快取上限和快取重存間隔。 • 取決於是否使用 XML 延伸程式或 Windows 事件檢視器延伸程式，可在個別標籤中設定對應選項。
閒置日誌	當 TAMESSO 未回應設定爲單一登入的應用程式時，請啓用此日誌。因爲此一追蹤記錄會產生許多資料，啓用時間請勿過長。	使用 **regedit**： • 將 DWORD 登錄機碼 HKLM\Software\Passlogix\Shell\LogInactive 設定爲 1。 • 將登錄機碼 HKLM\Software\Passlogix\Shell\LogInactivePath 填入應包含記錄之目錄的完整路徑（例如 C:\ESSODUMP） 請注意，必須先建立包含追蹤記錄的目錄後才能開始記錄。設定時，請啓動應用程式（Windows 或 Web），每個視窗 ID 會建立一個追蹤記錄檔。
Java™ 輔助物件日誌	在定義範本後，TAMESSO 若未回應 Java 應用程式時，請啓用此日誌。	使用 **regedit**，將 DWORD 登錄機碼 'HKLM\Software\Passlogix\Extensions\AccessManager\Enable JHOLog' 設定爲 1。啓用時，會在使用者的 %appdata%\Passlogix 目錄中建立 JHO.log 檔。
大型主機輔助物件狀態視窗	在定義主機應用程式範本後，TAMESSO 若未回應大型主機應用程式時，請啓用 SSO MHO 狀態視窗	• 建立至 ssomho.exe（預設路徑爲 <TAMESSO 用戶端安裝路徑 >\v-GO SSO\Helper\Emulator）的捷徑，並將捷徑拖曳到桌面上。 • 修改此捷徑的內容，在「Target」欄位中新增 /ssomho 選項。 • 在執行 TAMESSO 時按兩下 ssomho.exe 捷徑啓動 SSO MHO。

		• SSO MHO 視窗現在會顯示用戶端機器上所執行的主機應用程式。如果執行中的應用程式未顯示爲運作，在狀態視窗中的訊息常會提供資訊，說明爲何沒有偵測到該應用程式。 在 TAMESSO 用戶端關閉，或同樣的捷徑再按兩下以啓動 SSO MHO 視窗時，SSO MHO 視窗會關閉。
同步日誌	TAMESSO 用戶端無法與儲存庫同步時，登入管理員中因此無法提供範本，或是使用者認證資料因而未儲存到儲存庫中，請參考此日誌。	使用 **regedit**，將 HKLM\Software\Passlogix\Extensions\SyncManager\Syncs 中的 **DWORD 登錄機碼** TraceSync 設定爲 *1*。設定此一旗標時，如果有任何同步化錯誤，會在使用者的 **%appdata%\Passlogix** 目錄中建立記錄檔 SYNCLOG.txt。
當機日誌	當 TAMESSO 無法啓動時請參考此日誌。此日誌是要送到 IBM 支援服務以供分析。	當 TAMESSO 無法啓動時將會產生此日誌，其位置爲 Documents and Settings\<使用者設定檔>\Application Data\Passlogix，名稱是「vgo.log」
DPRA 日誌	在進行與桌面密碼重設配接器 (Desktop Password Reset Adapter) 相關問題除錯時，請參考此日誌。	若要啓用 DPRA 日誌檔，請使用 **regedit**，設定 **HKLM\SOFTWARE\Passlogix\SSPR\SSPRService** 中的**字串記錄檔**，將其值設定爲記錄檔的路徑（例如 C:\DPRA_LOG.txt）。

本文中後續的主題整理爲幾個段落，各提供 TAMESSO 個別元件的簡介，以及該元件的除錯技巧。

單一登入配接器 (SSO aDAPTER)

單一登入配接器（在上圖中定義爲 TAMESSO 核心）偵測到應用程式的認證要求，決定適當的動作，並以正確的認證資料回應。透過提供下列選項，它可設定許多受歡迎的應用程式：

- 作爲外掛程式的登入方式，以提供登入 TAMESSO 的不同方法。

- 強化與擴充 TAMESSO 功能的延伸程式。
- 由數個輔助外掛程式所組成的登入管理員，以協助 SSO。
- 同步化管理員 - 可同步化來自支援資料儲存庫的認證與設定資訊。
- 事件管理員 - 控制要記錄的事件、記錄的位置與時機，以及是否維持記錄的本機副本。

下列是除錯技巧與 SSO 配接器的常見問題，以及問題的疑難排解程序。

TAMESSO 未回應任何應用程式

出現下列一或多種情況時，會發生此一問題：

- TAMESSO 用戶端未執行。

  TAMESSO 執行時，在系統匣上會出現 TAMESSO 圖示，而在**工作管理員 | 程序**標籤中，至少會有一個 SSOShell.exe 實例。如果 TAMESSO 未執行，請試著從**開始**功能表啓動。如果仍無法啓動 TAMESSO，請將當機日誌（參考「TAMESSO 日誌」一段）傳送給 IBM 支援服務。如果無法使用儲存庫，TAMESSO 也有可能設定爲關閉。

- 有超過預期數目的 **SSOShell.exe** 程序正在執行。

  如果 TAMESSO 正在執行，請確認啓動的 SSOShell.exe 程序數目（如**工作管理員 | 程序**中所示）在預期之中。預期中的 SSOShell.exe 程序數目爲：

  - 一個是基本程序，對應系統匣上的圖示。
  - 開啓的登入管理員階段作業會各有一個程序
  - 在同步化事件、登入事件或密碼變更事件中，會暫時開啓一個程序（1 到 2 秒）。

  如果有超過預期數目的實例正在執行，請試著重新啓動 TAMESSO 用戶端。不當的檔案系統與登錄檔封鎖，會讓 Microsoft 與 RSA 加密無法正常運作。因此，請試著以具備管理員權限的使用者登入，或是以擁有少數或無原則限制的使用者身份登入。
  如果您在 TAMESSO 儲存庫中不具有適當權限，請試著以在它部電腦上成功操作的使用者身份登入。

- TAMESSO 無法與儲存庫同步 (Active Directory)，且未使用應用程式範本。

  TAMESSO 配置檔包括：

  - **entlist.ini**，是建立用來提供組織自訂的登入功能 （適用 Windows、Web 和大型主機應用程式）。此檔位於 Documents and Settings\<使用者資料>\Application Data\Passlogix 目錄中。
  - **applist.ini**，包含預先定義的登入功能（提供許多線上服務提供者的網路與 Web 跳出式登入對話方塊）。此檔位於 TAMESSO 的安裝目錄中（例如 C:\Program Files\Passlogix\v-GO SSO\plugin\LogonMgr）。
  - **aetlist.ini** 是 TAMESSO 應用程式登入說明檔，由 entlist.ini 和 aetlist.ini 合併所得。此檔位於 Documents and Settings\<使用者資料>\Application data\Passlogix 目錄中。

  查看 **entlist.ini** 是否存在。如果不存在，則 TAMESSO 無法連線到 Active Directory。即使 **entlist.ini** 存在，爲了確保能夠連線到 Active Directory，請將其刪除，開啓 TAMESSO 登入管理員並選擇**重新整理**。如果 TAMESSO 能夠連線到 Active Directory，會重新建立此檔。
  查看 **entlist.ini** 是否存在。如果不存在，則 TAMESSO 安裝已損毀且需要修復。從**控制台 | 新增/移除程式**重新安裝 TAMESSO，應可解決此問題。
  查看 **aetlist.ini** 是否存在。如果不存在，則 **entlist.ini** 與 **applist.ini** 的合併程序並未成功。如果 applist.ini 和 **entlist.ini** 都存在，請聯絡 IBM 支援服務取得協助。

- 缺少待測試應用程式的範本。

  如果受影響應用程式的登入管理員中出現認證資料，但列出的認證資料呈灰色，則目前未提供範本。請確定 Active Directory 中的範本未重新命名，且受影響的使用者具有存取範本的權限。
  從 TAMESSO 系統匣圖示移至**配置 | 設定**。在**密碼**標籤中，確認已勾選**自動提示**。在**登入**標籤中，確認已勾選**自動辨識**。在**排除的網站**標籤中，確認未列出該 Web 應用程式的基底域（例如 company.com）。

Web 應用程式的常見問題

- TAMESSO 用戶端未以框格內的認證要求回應 Web 應用程式。

  SSOBHO.exe 程序所代表的元件，是負責框格內 Web 應用程式登入與密碼變更的偵測及回應。檢查**工作管理員 | 程序**中，確實有正在執行程序的一個實例。如果 SSOBHO.exe 未執行，請看著**工作管理員 | 程序**，重新啓動 TAMESSO。如果發現此程序啓動後立即停止，表示此元件故障，請將當機日誌（參考 **TAMESSO 日誌**）傳給 IBM 支援服務以供分析。
  另一個可能性是 Internet Explorer 啓用了某些不必要的外掛程式（像是廣告軟體、間諜軟體等），這些程式的撰寫不當，大幅拖慢 Web 瀏覽，也對 TAMESSO 造成負面和非預期的影響。請注意，TAMESSO 和主流商業外掛程式並未有任何已知衝突。

- 自動識別對某些網站無用。

  自動識別選項是用來讓配接器自動識別應用程式和網站，並登入使用者。有可能在 TAMESSO 設定提供網站 SSO 後，網站的 URL 已變更。如果 URL 已變更，則網站的登入資訊也必須使用新 URL 更新。若要更新 URL，請按兩下 TAMESSO 的系統匣圖示，開啓**登入管理員**視窗，並選定所要的應用程式並按滑鼠右鍵，以編輯**內容**，提供新的 URL。

Windows（表單式）應用程式的常見問題

- 新增登入精靈中未列出應用程式

  即使新增登入精靈中未列出應用程式，TAMESSO 也可提供經過設定應用程式的單一登入功能。要這麼做，則需使用者名稱、ID 和密碼登入方塊在應用程式登入畫面中的位置資訊。若要完成設定：

  - 按兩下 TAMESSO 系統匣圖示（紅色），啓動**登入管理員**視窗。在**登入管理員**中按一下**新增**按鈕，選擇**新增登入**。在出現的**新增登入**精靈中，確定在下拉式選單中選擇了**不在清單中的應用程式**。在**應用程式名稱**和**說明**欄位中，提供應用程式名稱與選擇性的說明，然後按一下**下一步**。
  - 按一下**使用者名稱/ID** 欄位旁的 TAMESSO 標誌，並利用滑鼠將標誌拖曳到您應用程式的**使用者名稱**文字方塊。在 TAMESSO 標

誌旁接著會出現綠色打勾符號。

- 按一下**密碼**欄位旁的 TAMESSO 標誌，並利用滑鼠將標誌拖曳到您應用程式的**密碼**文字方塊。在 TAMESSO 標誌旁接著會出現綠色打勾符號。
- 按一下**下一步**，輸入登入應用程式所需的認證資料，並繼續進行**新增登入**精靈的最後步驟。

Java 應用程式的常見問題

- TAMESSO 用戶端未回應 Java 應用程式或 applet。

  TAMESSO 需要 Sun™ Java 1.3.1 或以上版本，以提供 Java 應用程式和 applet 原生支援。使用 java 版指令，判定 TAMESSO 所使用的 java.exe 版本。請注意，在多重 JRE (Java Runtime Environment) 安裝的情況中，java.exe 是從 JRE 路徑（system PATH 環境變數中第一個列出的變數）中挑出。
  JRE 安裝目錄應具有 \bin、\lib 和 \lib\ext 子資料夾。TAMESSO 需要下列支援檔位於作用中 JRE 路徑（針對所有需要原生 Java 登入與密碼變更支援的應用程式）的架構內：
  - \bin\ssojho.dll
  - \bin\accessibility.properties
  - \lib\logging.properties
  - \lib\ext\jaccess.jar
  - \lib\ext\jaccess.jar
  - \lib\ext\log4j_1.2.8.jar

  applet 是從 Web 瀏覽器中執行的 Java 應用程式。如果您使用 Internet Explorer，爲了確認 Sun Java 1.3.1 或以上版本設定爲預設的 Java 引擎，請移到**工具 | 網際網路選項 | 進階**，向下捲動至 **Java**（具有咖啡杯圖示的），並確認該選項存在且已勾選。如果選項不存在，請參考 Sun 的說明，以安裝和設定 Internet Explorer 的 Java 外掛程式，讓 applet 使用 Sun JRE 代替瀏覽器預設的 Java 執行時期。

- TAMESSO 用戶端無法識別由 Java 應用程式所呈現的**登入視窗**

  這需要啓用 Java 應用程式的服務登入。若要這麼做：
  - 在 TAMESSO 管理主控台中選擇**應用程式**節點。按一下主控台右方所要的應用程式，然後移到**其他**標籤。檢查**服務登入**選項。

- 移至主控台左側的**全域代理程式設定 | Live | 使用者經驗 | 回應 | Windows 應用程式**。勾選**服務支援的 Windows 類別**勾選框，並在以分號分隔的類別名稱清單尾端，新增所要應用程式的 window 類別。window 類別名稱可透過執行新的應用程式精靈來取得。

儲存庫與認證

儲存庫可用來統一加密儲存使用者認證與配接器設定資訊。用戶端可使用同步化外掛程式，來回備份和還原統一儲存庫中的認證資料。支援的儲存庫包括任何 LDAP v2 或 v3 相容目錄，支援的資料庫包括 Microsoft SQL 伺服器、Oracle、IBM DB2 和網路磁碟共用。在上面的架構圖中，此元件被稱爲「目錄/DB」。下列是與儲存庫相關的常見呈報問題，以及這些問題的疑難排解技巧。

手動綱目延伸

對於不能讓 TAMESSO 立即使用的儲存庫（例如 OpenLDAP），則需要手動綱目延伸。在試著進行自動綱目延伸時，TAMESSO 會呈報錯誤「本伺服器不支援自動綱目延伸」。使用位於 `Automated schema extension is not supported by this server. Use the file located at 'C:\Program Files\Passlogix\v-GO SSO Administrative Console\DirectorySchema\vGO\OLDAP\sso.schema` 的檔案，手動延伸綱目。「終止延伸綱目！」OpenLDAP 手動延伸綱目的步驟如下：

- 將 C:\Program Files\Passlogix\v-GO SSO Administrative Console\DirectorySchema\vGO\OLDAP 中的 sso.schema 檔複製到 OpenLDAP 伺服器機器上。
- 將 sso.schema 檔置於 OpenLDAP schema 資料夾中 (/usr/local/etc/openldap/schema)。
- 修改 OpenLDAP 配置檔 (slapd.conf)，新增一行 `include /usr/local/etc/openldap/schema/sso.schema`，以納入 TAMESSO 特定的綱目實體。

請注意，TAMESSO 可直接支援 SunONE 目錄伺服器、Novell eDirectory、Microsoft Active Directory 和 Microsoft ADAM。

Active Directory 儲存庫的常見問題

既然 TAMESSO 實質上是 Windows 應用程式，Active Directory 是最常使用的

儲存庫。下列是某些 Active Directory 重覆發生的問題，以及這些問題的疑難排解。

- **不允許綱目延伸**錯誤 - 在嘗試延伸綱目時，由 Active Directory 所呈報的錯誤。

  更新綱目需要寫入存取 Active Directory 中的綱目。這是透過**允許綱目更新**登錄機碼來啓用。綱目更新可透過綱目管理主控台來啓用。綱目更新只能在擔任主要綱目的網域控制器上啓用。若要啓用綱目更新：

  - 在命令提示列輸入 `regsvr32 schmmgmt.dll.`。請注意，只有顯示 **schmmgmt.dll** 中的 **DllRegisterServer 成功**對話方塊時，才算登錄成功。
  - 按一下**開始 | 執行**，然後輸入 **mmc**，開啓新的管理主控台。
  - 在**主控台**功能表上，按一下**新增/移除嵌入式管理單元**。
  - 按一下**新增**，開啓**新增獨立嵌入式管理單元**對話方塊。
  - 右鍵點選 **Active Directory 綱目**，然後按一下**操作主機**。
  - 按一下選擇**可在此網域控制器上修改綱目**勾選框，然後按一下**確定**並離開主控台。

- TAMESSO 顯示錯誤訊息「**同步程式延伸中的機碼與此電腦上的不符。將不會進行同步。請聯絡您的系統管理員。**」

  當使用者在一部工作站上設定 TAMESSO、與 Active Directory 進行同步、移至另一部工作站，並由 TAMESSO 首次使用 (FTU) 設定程序提示動作時，會通知此一錯誤。只有第二部系統無法連絡 Active Directory，或是使用者取消 Active Directory 提供的認證對話方塊時，才會進行首次設定。
  如果使用者先前未登入第二部系統並特地使用 TAMESSO，也會進行首次設定，TAMESSO 在第一部工作站上建立獨特的一對機碼，然後到第二部工作站上建立第二對機碼。
  若要處理此種情況，請使用下列步驟，移除第二部工作站上所有的本機資料（包括認證）：
  - 關閉 TAMESSO 用戶端。
  - 使用 **regedit** 刪除 **HKCU\Software\Passlogix**。請注意，這是 HKCU（目前的使用者）而非 HKLM（本機）。
  - 刪除 **C:\Documents and Settings\<user profile>\Application Data\Passlogix**。

- 啓動 TAMESSO。

管理主控台

管理主控台透過啓用大部分選項的配接器與伺服器配置，提供 TAMESSO 的統一化管理。所有變更都被送到統一儲存庫，然後再與配接器同步。
下列是使用管理主控台設定 TAMESSO 時要記住的一些重點。

多值勾選框設定

許多 TAMESSO 管理主控台中的配置選項，是透過多值勾選框控制項來設定。多值勾選框可爲下列狀態之一：

- **未勾選**，表示設定關閉，用戶端無法超控此設定。
- **勾選**，表示設定開啓，用戶端無法超控此設定。
- **勾選並呈灰色**，表示設定開啓，用戶端可超控此設定並將其關閉。

啓用「使用 WM_CHAR 訊息填入控制」設定的時機

如果通知有認證資料正呈送到應用程式，但在填入應用程式本身的欄位中並未識別出來，請在範本上啓用此設定。
某些應用程式要求密碼需以鍵盤輸入，而非「既定文字」的指令。啓用此控制可設定控制中的文字，以另一種方式模擬鍵盤輸入。例如，在 Citrix 9.15 ICA Client 的情況中，雖然提供認證，但卻像是損毀或錯誤的值。**WM_CHAR** 選項向來用於解決 Citrix、Novell 與 Lotus Notes 的範本問題。

鑑別配接器

鑑別配接器可讓組織平順地進行所有應用的強型態鑑別功能，包括智慧卡、生物識別裝置，以及受信任的認證者。使用者可在不同時候部署不同的認證介面，應用程式存取也可根據所使用的認證介面來控制。

IBM ThinkPad 的 TAMESSO 配置嵌入一個觸摸指紋生物辨識感應器

TAMESSO 可經過設定，使用指紋作爲登入方式而提供單一登入，例如 IBM ThinkPad 指紋式生物辨識感應器。此項設定包括下列步驟：

- **安裝 ThinkVantage 指紋軟體**

ThinkVantage 指紋軟體可安裝在任何備有 Windows 2000、Windows XP Home 或 Professional edition、Windows Vista 和未佔用 USB 連接埠的電腦上。請注意，具有內建生物辨識感應器的 ThinkPad 並不需要未佔用的 USB 連接埠，只有使用外接生物辨識感應器時才需要。安裝或解除安裝 ThinkVantage 指紋軟體需要管理員權限。安裝步驟如下：

- 如果有光碟，請插入 CD 光碟機，否則請執行 Setup.exe 並跳過下一步驟。
- 會出現 **ThinkVantage 指紋軟體**畫面。按一下**安裝**圖示。如果未出現此畫面，請手動執行 Setup.exe。
- 會顯示**歡迎**畫面。
- 按一下**下一步**繼續。
- 會出現**使用者資訊**畫面。
- 輸入您的使用者資訊，然後按一下**下一步**繼續。
- 確認或選擇安裝目錄。
- 按一下**下一步**開始安裝。
- 安裝完成後，請在出現提示時重新啓動電腦。

安裝現在已完成。在重新啓動電腦後，會顯示登入畫面。請注意，安裝時會安裝所有必需的裝置驅動程式。如果您想使用外接指紋感應器，我們建議您在安裝完成後連接指紋感應器硬體，並重新啓動電腦。

- **指紋登錄**

ThinkVantage 指紋軟體中的各使用者身份，是以**護照**來代表，其中包含用來驗證使用者身份的生物指紋資料。指紋登錄是建立使用者名稱、密碼與指紋間對應的程序。若要建立新的護照（也就是登錄指紋）：

- 如果您想使用外接指紋辨識感應器，請接上裝置。所有必需的驅動程式已隨 ThinkVantage 指紋軟體安裝。在畫面的右下角會顯示訊息，告知感應器已連接且可以使用。
- 會顯示授權合約。仔細閱讀授權合約。
- 選擇正確的圓鈕接受授權合約。您必須同意授權合約才能安裝此產品。如果您不同意授權合約，按一下取消，關閉應用程式。
- 若要啓動登錄精靈，請選擇**開始**功能表 | **程式集 | ThinkVantage | ThinkVantage 指紋軟體 | 使用者登錄**。
- 輸入您的使用者名稱、密碼和網域（如果適用的話），然後按一下

下一步。

- 按一下**下一步**繼續指紋教學。或是取消勾選**進行互動教學**勾選框，然後按一下**下一步**跳過教學。
- 按一下您想登錄指紋上方的方塊。根據教學中的指示製作選定手指的三個指紋樣本。這些樣本會合成一個單一的指紋護照。如果三個樣本不符，會出現警告。
- 選擇另一個要登錄的指紋。您最多可登錄 10 個指紋。我們強烈建議您登錄一個以上的指紋，以備受傷時使用。完成時請按**下一步**。

- **透過管理主控台設定 TAMESSO**

  - 在 TAMESSO 管理主控台中，反白選取並右鍵點選**全域代理程式設定**。
  - 選擇**匯入 | 從 Live HKLM**，從本機登錄檔中，以一組名爲 **Live** 的設定，匯入目前的配接器配置。
  - 現在可看到 **Live** 出現在**全域代理程式設定**標籤中。按一下 + 號展開，檢視 SSO 配接器目前的登錄檔設定。
  - 展開**主要登入方式**節點並選擇 **Windows V2**，這提供了 Windows authenticator 第 2 版的主要控制項。
  - 在主控台右側，啓用**重新鑑別對話方塊**，並選擇**使用 GINA**。這會將 Windows GINA（圖形化識別與驗證）設定爲 TAMESSO 用來重新認證使用者的方法。
  - 在主控台左側，選擇 Windows V2 下方的**進階**節點，並在主控台對應的右側，啓動**密碼**，然後選擇**停用**選項。這會停用額外安全性所要求的密碼。
  - 回到主控台左側，選擇 TAM E-SSO 中的**應用程式**標籤，然後在主控台對應的右側，按兩下您想使用生物辨識保護的應用程式。在**其他**標籤中，啓用**強迫重新認證**。這將會要求使用者在提供認證資料給此應用程式前，重新進行認證。

- **部署 ThinkPad 用戶端機器上的 TAMESSO 配置**

  - 從 TAMESSO 管理主控台中選擇**全域代理程式設定 | Live**，然後右鍵點選並選擇**匯出**。從匯出格式清單中選擇 **HKLM 登錄檔格式 (.REG)**，並將檔案儲存在方便的位置，可以從其他用戶端機器輕鬆存取。
  - 將匯出的 .REG 檔複製到 ThinkPad 用戶端機器上，並將此檔併入 ThinkPad 登錄檔。

- **ThinkPad 用戶端設定**

    - 移至**控制台 | 新增/移除程式**。選擇 **IBM Tivoli Access Manager for Enterprise Single Sign On**，然後按一下**變更**。
    - 展開**登入方式**，按一下 **Windows V2**，然後選擇 **GINA 安裝**。讓其他登入方式保持原狀，並繼續完成安裝。
    - 右鍵點選系統匣上的**登入管理員**圖示。移至**配置**，然後按兩下**變更登入方式**選項。選擇 **Windows v2**，然後按一下**完成**。

從此時開始，如果使用者已定義應用程式的強迫重新認證，將會出現生物辨識提示。如果使用者試著在登入管理員中顯示密碼，將會看到生物辨識提示。
請注意，ThinkVantage 配置可以任何生物辨識感應器軟體及驅動程式配置取代，但生物辨識認證式應用程式的 TAMESSO 配置仍維持不變。

桌面密碼重設配接器 (DPRA)

桌面密碼重設配接器可在您遺失或忘記網域密碼時，允許存取 Windows 使用者帳戶。用不著致電服務台，只要回答用來驗證人員的跳出式小測驗，即可讓該名人員重設自己的密碼。小測驗是在完成 DPRA 登錄訪問時由該名人員所設定的。
下列是 DPRA 的常見問題，以及這些問題的疑難排解技巧。

動態伺服器網頁 (Active Server Page) 相關的常見問題

- **試著存取 DPRA 主控台時，**出現拒絕存取錯誤。

此問題只會發生在 Windows 2000 SP4 伺服器上。當 ASP .NET 1.1 安裝在執行 Windows 2000 網域控制器加 Service Pack 4 (SP4) 的電腦上，內建的 IWAM 使用者帳戶（由具 ASP 的 IIS Web 服務所用）未獲得 ASP .NET 1.1 的使用者權限。因此，對任何 ASP 資源（包括 TAMESSO DPRA 管理主控台）的要求都會產生**拒絕存取錯誤**。這是已知的問題（參考 Microsoft 知識庫文章 # 824308）。若要解決此問題：

    - 按一下**開始**，將游標指向**程式集**，指向**管理工具**，然後按一下**網域控制器安全政策**。
    - 按一下**安全設定**。
    - 按一下**本機政策**，然後按一下**使用者權限指派**。

- 在右側窗格中按兩下**在認證後模擬用戶端**。
- 在**安全政策設定**視窗中按一下**定義這些政策設定**。
- 按一下**新增**，然後按一下**瀏覽**。
- 在**選擇使用者或群組**視窗中選擇 IWAM 帳戶名稱，按一下**新增**，然後按一下**確定**。
- 按一下**確定**，然後在接下來的兩個視窗中再按**確定**。
- 若要進行電腦政策更新，請輸入下列命令 `secedit /refreshpolicy machine_policy /enforce`。
- 在命令提示列中輸入 iisreset，重新啓動 IIS。

- 無法存取 DPRA 管理主控台，出現錯誤 - **目前的身分 (NT_AUTHORITY\NETWORK SERVICE) 不具有 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\Temporary ASP .NET files 的寫入存取權限。**

  爲了解決此項錯誤，指定的使用者或群組（也就是 NT_AUTHORITY\NETWORK_SERVICE）必須被授與權限存取 IIS metabase 和其他 ASP.NET 所使用的目錄。若要這麼做，啓動命令提示，移至錯誤中所提及的目錄，也就是 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\Temporary ASP .NET files，並執行命令 `aspnet_regiis -ga "NT_AUTHORITY\NETWORK_SERVICE"`。請注意，ASP .NET 2.0 以前的 ASP .NET 版本無法使用此選項。在成功進行 ASP .NET IIS 登錄後，必須允許對 DPRA 管理主控台的存取。

成功完成 DPRA 服務重設小測驗，將會導致「您不能重設密碼」錯誤訊息

這是極常呈報的問題，是網域密碼政策非常嚴格所致。如果 Active Directory 被用作使用者儲存庫，會利用 **密碼最小存留期**密碼政策設定，決定新密碼至少必須使用幾天，使用者才能予以變更。如果設定爲 0，使用者可立即變更密碼。如果大於 0，使用者一天至多只能變更密碼一次。在透過 DPRA 管理主控台設定密碼重設服務時，也請確認所選的新密碼符合密碼複雜度規則。

在安裝 DPRA 後，Internet Explorer 出現奇怪的錯誤

有時因爲不明理由，DPRA 安裝似乎會損毀 Internet Explorer (IE) 瀏覽器的登錄機碼。因此在關閉瀏覽器視窗、存取書籤或開啓選項功能表時，IE 會報告錯誤。解決此問題不需要重新安裝 DPRA。使用 **regedit**，找出

HKLM\Software\Passlogix\Microsoft\Internet Explorer\Restrictions 目錄。在此處列出各種選項，像是 **NoBrowserClose**、**NoBrowserOptions**、**NoFavourites** 等，其數值皆設定爲大數字。將這些值重設爲 0，則 IE 應該不會再出現奇怪的錯誤。請注意，進行這些變更完全不會干擾 DPRA 安裝。

將本機使用者帳戶排除在強迫登錄之外

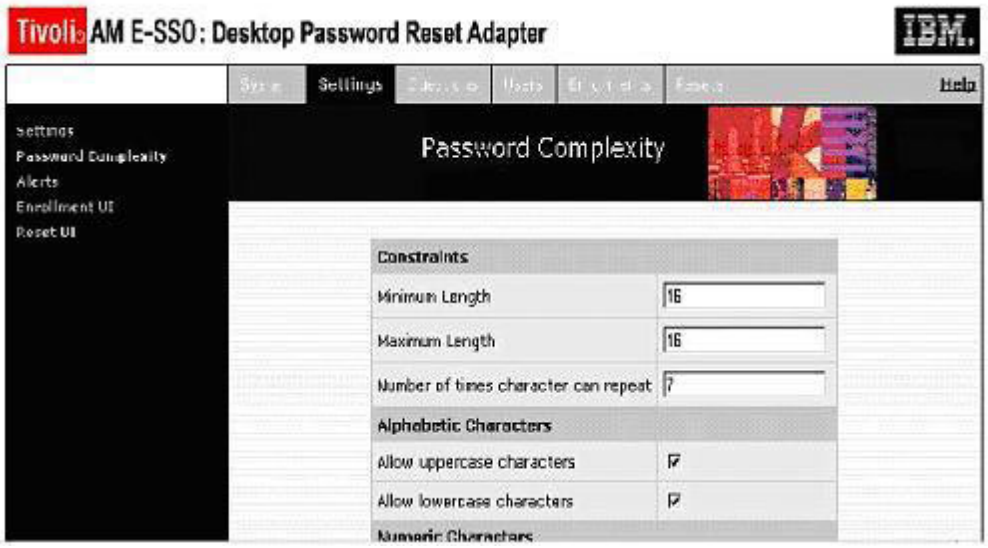
如果僅有用戶端機器的網域使用者（而非使用者）必須登錄 DPRA，請使用 **regedit**。

- 選擇登錄機碼 **HKLM\Software\Passlogix\SSPR\WindowsInterface**
- 按一下**編輯**，然後移到**授權**。
- 按一下**進階**按鈕，並取消勾選**從父代繼承套用到子物件的授權記錄**。在這些記錄中加入此處明確定義的資料。
- 在出現的跳出式對話方塊中，按一下**複製**，複製先前從父代套用到物件的授權資料。
- 從授權資料中移除所有本機使用者與群組，將**系統**保持原狀，並新增**網域使用者**的讀取權限，以及**網域管理員**的完全控制權限。

由於密碼重設失敗和舊密碼停止作用，使用者因此被封鎖

這是典型的情境，使用者嘗試重設密碼失敗，而且無法再使用舊密碼登入，因爲舊密碼已過期。爲了避免此種情形發生，使用者必須確定 DPRA **密碼複雜度設定**（如下列螢幕擷取畫面所示）符合 Active Directory（假設爲所選定的儲存庫）中的密碼複雜度設定。DPRA 密碼複雜度資訊，可在 DPRA 管理主控台中的密碼複雜度設定頁中取得。請注意，這些設定並未強迫用戶端的密碼重設值，但是被用來產生暫時的密碼值。

圖 2. 密碼複雜度設定



Kiosk 配接器

kiosk 配接器提供安全而使用簡易的管理解決方案，可滿足電子便利站環境中傳統單一登入的需求。用戶端配接器會暫停或關閉閒置的階段作業，並且不著痕跡地關閉所有應用程式。
使用電子便利站模式操作的一項典型要求，就是跳過電子便利站歡迎畫面。

跳過電子便利站歡迎畫面。

如果有時 kiosk 配接器沒有正確設定，使用者因此無法使用電子便利站歡迎畫面登入，您可能需要跳過此畫面並像平常一樣登入。爲了讓 kiosk 配接器不要啓動，在登入機器時請按住 **Shift** 鍵。輸入密碼後，在按一下登入按鈕前必須按住 Shift 鍵不放，而且直到機器完全登入前都必須按住此鍵。請注意，即使採用此種方法，電子便利站也可能啓動，但絕對會延遲啓動，因此會有足夠的時間在其完全啓動前，開啓工作管理員並停止代表 kiosk 配接器的 **smagent.exe** 程序。

供應配接器

供應配接器伺服器可接收和處理由 Tivoli 身分管理員發出的供應要求。供應配接器伺服器與 Tivoli Identity Manager (TIM) 間的整合，是透過使用工作流程延伸程式來完成，TIM 使用此延伸程式來和供應配接器伺服器 Web 服務進行通訊。
下列是供應配接器的常見問題與問題解決方法。

無法登入供應配接器主控台

有時儘管已提供管理員認證資料，在嘗試登入供應配接器主控台時會導致回應內容類型爲 **text/html** 而非 **text/html**，因此登入要求失敗並出現錯誤訊息**無法使用伺服器應用程式**。一旦出現此錯誤，請查看 ASP .Net 是否爲 Internet Information Services (IIS) 登錄的 Web 服務延伸程式。若要這麼做：

- 移至**控制台 | 管理工具 | Internet Information Services (IIS) Manager**。
- 在 **Web 服務延伸程式**中，如果已登錄 ASP .Net 延伸程式，且其設定爲**禁止**，請將其設定變更爲**允許**。

如果 Web 服務延伸程式中完全未列出 ASP .Net，請遵照下列步驟安裝 ASP .Net 延伸程式，然後確認 IIS 登錄此延伸程式：

- 移至**控制台 | 新增或移除程式 | 新增 / 移除 Windows 元件**。
- 出現精靈時，請選擇**應用程式伺服器**，然後點選**詳細資料**按鈕。
- 從元件清單中選擇 **ASP .NET**，然後繼續執行精靈。

如果這沒有解決登入問題，請試著使用命令列工具 `C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis.exe -I` and restart IIS，將 ASP .Net 延伸程式登錄到 IIS，然後重新啓動 IIS。

無法透過供應配接器主控台提供 SSO 使用者的新認證資料

儘管啓用了供應配接器中的**角色/群組支援**設定，有時候登入供應配接器主控台的使用者，不能夠新增應用程式範本，並出現錯誤訊息「使用者沒有進行此動作的權限」。爲了解決此問題，請移到 TAMESSO 主控台供應配接器連結中的預設權限標籤，定義使用者與群組，以及所將擁有的存取權限。這些預設權限將會由任何新應用程式範本所繼承。同樣的設定可複製到管理主控台的現有應用程式範本中。

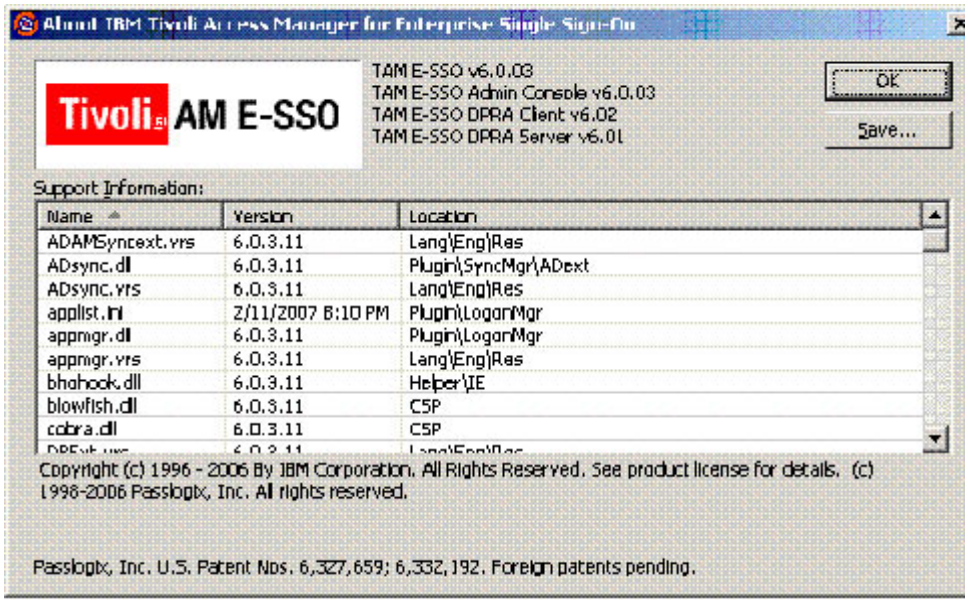
聯絡 IBM 支援服務

爲了連絡 IBM 支援服務解決 TAMESSO 問題，必須產生問題管理報表 (PMR)。報表必須包含下列資訊，以加速解決問題：

- 「關於 TAMESSO」資訊

右鍵點選 TAMESSO 用戶端（系統匣中的紅地毯圖示），然後選擇**關於 TAMESSO**。這將顯示 TAMESSO 安裝中所有程式庫和二進位檔的確切版本清單，如下圖所示。按一下**儲存**，以文字格式儲存此資訊。將此資訊傳送給 IBM 支援服務，協助他們快速辨識所使用的元件版本，以便快速重建問題。

圖 3. 關於 TAMESSO 視窗



- TAMESSO 管理主控台設定 XML 檔
  如果 XML 檔案中尚未提供 TAMESSO 配置，請到 TAMESSO 管理主控台，並選擇**檔案 | 另存新檔**，然後提供配置 XML 檔案的名稱與位置。在呈交 PMR 時請將此檔案傳送給 IBM 支援服務。

資源

- *Deployment Guide Series: IBM Tivoli Access Manager for Enterprise Single Sign On* describes how to install and configure major TAMESSO components, planning of an enterprise SSO deployment, best practices, and troubleshooting tips.

作者簡介

Giancarlo Marchesi 是 Tivoli 全球安全 SWAT 小組的解決方案架構設計師。他與客戶合作的豐富經驗，提供系統整合、應用程式與企業安全性的解決方案。他

擁有加州大學的電腦系統工程理學士學位。他被認定爲 IBM 的 TAMESSO 領域專家，目前在西班牙工作。

Rajalakshmi Iyer 是印度 Pune 軟體實驗室 IBM Tivoli Directory Server 小組的資深開發人員。身爲開發人員，她負責功能開發生命週期的所有階段。她在目錄網域方面具有超過 7 年的經驗。她擁有印度孟買大學的電腦科學工程學士學位。