CA Performance Center

單一登入使用者指南

2.4

本文件包含內嵌說明系統與文件 (以下稱爲「文件」)僅供您參考之用，且 CA 得隨時予以變更或撤銷。

未經 CA 事先書面同意，任何人不得對本「文件」之任何部份或全部內容進行影印、傳閱、再製、公開、修改或複製。 此「文件」爲 CA 之機密與專屬資訊，您不得予以洩漏或 用於任何其他用途，除非 (i) 您與 CA 已另立協議管理與本「文件」相關之 CA 軟體之使用；或 (ii) 與 CA 另立保密協議同意使用之用途。

即便上述，若您爲「文件」中所列軟體產品之授權使用者，則可列印或提供合理份數之「文件」複本，供您以及您的員工內部用於與該軟體相關之用途，但每份再製複本均須附上所有 CA 的版權聲明與說明。

列印或提供「文件」複本之權利僅限於軟體的相關授權有效期間。 如果該授權因任何原因而終止，您有責任向 CA 以書面證明該「文件」的所有複本與部份複本均已經交還 CA 或銷毀。

在相關法律許可的情況下，CA 係依「現狀」提供本文件且不做任何形式之保證，其包括但不限於任何針對商品適銷性、適用於特定目的或不侵權的暗示保證。 在任何情況下，CA 對於您或任何第三方由於使用本文件而引起的直接、間接損失或傷害，其包括但不限於利潤損失、投資損失、業務中斷、商譽損失或資料遺失，即使 CA 已被明確告知此類損失或損害的可能性，CA 均毋須負責。

「文件」中提及之任何軟體產品的使用均須遵守相關授權協議之規定，本聲明中任何條款均不得將其修改之。

此「文件」的製造商爲 CA。

僅授與「有限權利」。美國政府對其之使用、複製或公開皆受 FAR 條款 12.212，52.227-14 與 52.227-19(c)(1) - (2) 與 DFARS 條款 252.227-7014(b)(3) 中所設之相關條款或其後續條約之限制。

 本文提及的所有商標、商品名稱、服務標章和公司標誌均爲相關公司所有。

CA Technologies 產品參考資料

本文件提及下列 CA Technologies 產品：

- CA Performance Center
- CA Infrastructure Management Data Aggregator
- CA Network Flow Analysis
- CA Application Delivery Analysis
- CA Unified Communications Monitor

連絡技術支援

如需線上技術協助及完整的地址清單、主要服務時間以及電話號碼，請洽「技術支援」，網址爲：http://www.ca.com/worldwide。

目錄

第 1 章： 在 CA Performance Center 中自訂驗證

本節包含以下主題：

CA Single Sign-On

*單一登入*是 CA Performance Center 及所有受支援資料來源適用的驗證計劃。一旦使用者通過 CA Performance Center 的驗證，便可在主控台和已登錄資料來源間進行導覽，而無須重新登入。

單一登入可提供連續在不同產品介面之間導覽的能力，可協助操作員順暢地分析效能和狀態資料。 例如，使用者如果登入 CA Performance Center，然後利用深入檢視路徑前往資料來源介面，則不需要再次登入。

CA Performance Center 採用分散式架構。 在每個已安裝支援資料來源或 CA Performance Center 的伺服器上，都會自動安裝一個單一登入網站執行個體。分散式架構可讓使用者登入執行這些產品的伺服器，以登入個別 CA 資料來源產品。

CA Performance Center 驗證與安全性

單一登入可提供 CA Performance Center 及受支援資料來源的驗證服務。 其也支援外部驗證計劃，例如 LDAP 及 SAML 2.0。 這項支援可讓您將 CA Performance Center 及其他 CA 資料來源產品整合於全企業的同一個驗證計劃中。

單一登入安全稽核功能可記錄哪些人於一天何時登入的資訊。 在 Linux 伺服器上，此記錄是儲存在下列位置：
`[安裝目錄]/PerformanceCenter/sso/logs`

在安裝資料來源的 Windows 伺服器上，此記錄是儲存在下列目錄：
`[安裝目錄]\Portal\SSO\logs`

驗證方法

「單一登入」元件可提供登入頁面，來支援 CA Performance Center 和資料來源產品中的使用者驗證。 單一登入可支援下列驗證方法：

- 以使用者帳戶爲依據的產品驗證
- LDAP
- 安全性聲明標記語言 (SAML) 2.0

CA Performance Center 管理員可以修改個別單一登入執行個體的設定。例如，您可以在單一登入中設定 LDAP 驗證。您也可以使用安全通訊端層 (SSL) 來配置選用加密，或變更預設虛擬目錄。

附註：由於採用分散式架構，因此單一登入網站的任何更新都只會影響同一部伺服器上執行的資料來源產品。

資料來源支援

CA 單一登入可支援下列所有資料來源：

- CA Infrastructure Management Data Aggregator
- CA Network Flow Analysis
- CA Application Delivery Analysis
- CA Unified Communications Monitor

「單一登入配置工具」的設計適合在 Linux 系統上執行。 不過，您也可以將它部署在已安裝資料來源的 Windows 伺服器上。 如果您從 Windows 伺服器啓動「配置工具」，請以系統管理員的身分登入該伺服器。

您也可以在 Linux 執行配置工具，並使用 [遠端值] 選項，將配置指示傳送到 Windows 上執行的資料來源。

配置工具安裝於 Linux 的下列目錄位置：
`[安裝目錄]/CA/PerformanceCenter`

在安裝資料來源的 Windows 伺服器上，配置工具是安裝在下列目錄：
`[安裝目錄]\Portal\SSO\bin\SsoConfig.exe`

單一登入配置工具

單一登入配置工具是一種命令列應用程式，可供管理員調整單一登入網站及相關 CA 資料來源產品的設定。

附註：「配置工具」中的「遠端值」選項會將設定散佈至每個登錄的資料來源。 使用 [本機覆寫] 選項可覆寫所選伺服器上散佈的設定。

「單一登入配置工具」的設計適合在 Linux 系統上執行。 不過，您也可以將它部署在已安裝資料來源的 Windows 伺服器上。 如果您從 Windows 伺服器啓動「配置工具」，請以系統管理員的身分登入該伺服器。

使用單一登入配置工具可執行下列工作：

- 配置資料來源產品使用 LDAP 驗證。

  使用此工具可更新每個產品所有的 LDAP 設定。 您也可以測試目前的 LDAP 配置，以驗證設定。

- 配置資料來源產品使用 SAML 2.0 驗證。

  除了使用配置工具之外，管理員也必須對於身分識別提供者進行一些步驟，設定 SAML 2.0 驗證。

- 使用各個產品參考的單一登入虛擬目錄。

  如果已經新增加密計劃或已經變更單一登入虛擬目錄，請使用此工具同步處理資料來源產品。 例如，修改的伺服器上的資料來源，需要關於將未成功驗證的使用者重新導向至何處的指示。

- 請讓執行 CA 軟體產品的伺服器能夠使用 HTTPS 相互通訊。

  此變更將影響單一登入 URL 計劃及連接埠。 單一登入配置工具可讓管理員輕鬆地更新所有必要資料來源產品中的這些值。

備份單一登入配置檔案

當您使用配置工具變更設定時，您的設定會儲存在配置檔案中。 請定期建立這些檔案的備份複本，以避免遺失單一登入設定。 使用 rsync 或其他您慣用的方法 (例如指令碼)，自動或在升級前備份這些檔案。

將下列檔案新增至您的備份程序：

InstallationDirectory/CA/PerformanceCenter/sso/start.ini
InstallationDirectory/CA/PerformanceCenter/PC/start.ini

另外也請備份下列目錄：

InstallationDirectory/CA/PerformanceCenter/sso/webapps/sso/configuration
InstallationDirectory/CA/PerformanceCenter/sso/etc
InstallationDirectory/CA/PerformanceCenter/sso/conf
InstallationDirectory/CA/PerformanceCenter/PC/etc
InstallationDirectory/CA/PerformanceCenter/PC/conf

附註：預設安裝目錄爲 /opt/CA。

更新單一登入網站設定

單一登入配置工具可讓您變更單一登入網站的預設設定。 例如，您可以變更單一登入網站的虛擬目錄。 需要有虛擬目錄，才能將加密計劃用於 CA 伺服器之間的通訊。

您可以變更當使用者嘗試登入時會影響單一登入行爲的其他設定。 某些參數也會影響使用者介面行爲，例如爲了回應閒置而自動將使用者登出的逾時期間。

重要！ 由於軟體採用分散式架構，因此單一登入網站的更新只會影響同一部伺服器上執行的 CA 資料來源產品。

請依循下列步驟:

1. 登入已安裝 CA Performance Center 或 CA 資料來源產品的伺服器。

   以 root 使用者身分或「sudo」命令登入。

2. 在下列目錄中執行「./SsoConfig」命令，啓動單一登入配置工具：

   ```
   [安裝目錄]/CA/PerformanceCenter
   ```

   系統會提示您選取選項。 可用的選項將對應於本機伺服器上執行的 CA 應用程式。

3. 選取設定時，視需要使用下列命令：

   - q (結束)
   - b (回到上一個功能表)
   - u (更新)
   - r (重設)

4. 輸入 1 來配置 CA Performance Center。

   系統會提示您選取選項。

   ```
   SSO Configuration/CA Performance Center:
   1. LDAP Authentication
   2. SAML2 Authentication
   3. Performance Center
   4. Single Sign-On
   5. Test LDAP
   6. Export SAML2 Service Provider Metadata
   Choose an option >
   ```

5. 輸入代表單一登入的 4。

   系統會提示您指定優先順序。

   優先順序參數僅會套用至 CA Performance Center。

6. 輸入下列其中一個選項：

   1. 遠端值

   指只有管理員才能變更的設定。 這類設定會傳播至已向此 CA Performance Center 執行個體登錄的其他所有 CA 產品。 只有在對應的「本機覆寫」值不存在時，才會使用「遠端值」設定。

   2. 本機覆寫

   指可對所有產品變更的設定。 如果「本機覆寫」值存在，其優先順序高於「遠端值」和預設設定。

   系統會提示您選取要配置的內容。

7. 輸入下列其中一個或多個內容。 出現提示時，輸入 u 來更新值，然後提供新的值：

   1. 啓用匿名使用者

   指定當使用者嘗試登入資料來源介面時，是否顯示登入頁面。 如果啓用此參數，則 [匿名使用者 ID 參數] 必須有值。使用者嘗試登入時，不會看見登入頁面。 他們會以與 [匿名使用者 ID] 參數相關聯的使用者身分登入。

   遇到下列狀況時，[啓用 Localhost 使用者] 參數會優先套用：

   - 使用者從單一登入伺服器登入。
   - [啓用 Localhost 使用者] 參數及 [啓用匿名使用者] 參數皆已啓用。

   預設：已停用。

   附註：匿名使用者登入機制優先於 Windows 驗證。

   2. 匿名使用者 ID

   指定略過登入頁面時，用來自動驗證使用者的使用者名稱。 只有在 [啓用匿名使用者] 參數啓用時，才能使用此參數。 選取下列其中一個值：

   - **1** - 預設管理員帳戶的使用者名稱 (admin)。
   - **2** - 預設使用者帳戶的使用者名稱 (user)。
   - CA Performance Center 資料庫中存在的另一個使用者名稱。

3. 啓用 Localhost 使用者登入頁面

指定當使用者從已安裝單一登入的伺服器登入時，是否顯示登入頁面。

如果啓用此參數，即使使用者從單一登入伺服器登入，仍會顯示登入頁面。

如果停用此參數，則會套用下列規則：

- 必須啓用 [啓用 Localhost 使用者] 參數。
- [Localhost 使用者 ID] 參數的值必須包含有效的產品使用者名稱。此值用於在略過登入頁面時，將使用者登入軟體介面。

預設：已停用。

4. 啓用 Localhost 使用者

指定當使用者從單一登入伺服器登入時，是否自動將使用者登入，而略過登入頁面。 如果啓用此參數，則 [Localhost 使用者 ID] 參數需要有值。

- 如果啓用 [啓用 Localhost 使用者登入頁面] 參數，此參數的使用時機是使用者按一下 [登入] 卻未輸入使用者名稱或密碼時。如此使用者就會以與 [Localhost 使用者 ID] 參數相關聯的使用者身分登入軟體。
- 如果使用者提供了使用者名稱及密碼，這些認證將用於驗證。
- 如果啓用此參數，但是停用 [啓用 Localhost 使用者登入頁面] 參數，使用者將略過登入頁面。 但使用者將改爲使用 [Localhost 使用者 ID] 參數的值登入介面。
- 如果使用者從單一登入伺服器登入，而且 [啓用 Localhost 使用者] 及 [啓用匿名使用者] 皆已啓用，則會優先套用 [啓用 Localhost 使用者] 參數。

預設：已停用。

5. Localhost 使用者 ID

指定使用者登入單一登入伺服器時，用來自動驗證使用者而略過登入頁面的使用者 ID。 只有在 [啓用 Localhost 使用者] 參數啓用時，才能使用此參數。 輸入下列其中一個值：

1 - 預設管理員帳戶的使用者名稱 (admin)。

2 - 預設使用者帳戶的使用者名稱 (user)。

6. Cookie 逾時分鐘

指定單一登入 Cookie 到期前所經過的分鐘數。 每次使用者在資料來源介面中執行動作時，Cookie 逾時就會重設。 如果逾時到期，使用者將登出而必須重新驗證。

預設：20 分鐘

7. 加密的解密金鑰

指定將單一登入 Cookie 加密和解密所使用的金鑰。

8. 加密演算法

指定將單一登入 Cookie 加密和解密所使用的加密演算法。 提供 DES 或 AES 做爲值。

9. 失敗睡眠秒數

指定單一登入應用程式在嘗試登入失敗後所等待的秒數。

10. 啓用記住我的帳戶

指定登入頁面上是否顯示 [記住我的帳戶] 核取方塊。[記住我的帳戶] 設定將決定 Cookie 逾時到期時是否自動登出使用者。

預設：已啓用。

11. 記住我的帳戶逾時天數

指定在登入頁面選取 [記住我的帳戶] 的使用者必須重新驗證前所經過的天數。 只有在 [啓用記住我的帳戶] 參數啓用時，才能使用此參數。 值 0 表至 [記住我的帳戶] 設定未到期；使用者必須按一下資料來源產品介面中的 [登出] 連結。

12. 計劃

指定資料來源產品可用來存取單一登入應用程式的 URL 計劃。 如果您是使用 SSL，請提供「https:」做爲值。

13. 連接埠

指定資料來源產品可用來存取單一登入應用程式的 URL 連接埠。

14. 虛擬目錄

指定單一登入的虛擬目錄名稱。

預設：SingleSignOn。

附註：如果您變更任何先前參數的值，預設值並不會被取代，但是現在將以新的值爲準。 新的值實際上是一項「本機覆寫」。

8. 完成變更預設設定時，輸入 b。
9. 您便會返回上一組選項。
10. 再次輸入 b 返回第一組選項。
11. 輸入 q 關閉單一登入配置工具。

    單一登入配置工具隨即關閉。

    CA Performance Center 會使用您提供的新值，將所有未驗證的使用者導向單一登入網站。

更新 CA Performance Center 網站設定

單一登入配置工具可讓您變更 CA Performance Center 網站與 Web 服務的預設設定。 例如，您可以爲 CA Performance Center Web 服務指定不同的主機或連接埠號碼。 這些設定將指示單一登入應用程式要如何連線至 CA Performance Center。

請依循下列步驟:

1. 登入已安裝 CA Performance Center 或 CA 資料來源產品的伺服器。

   以 root 使用者身分或「sudo」命令登入。

2. 在下列目錄中執行「./SsoConfig」命令，啓動單一登入配置工具：

   ```
   [安裝目錄]/CA/PerformanceCenter
   ```

   系統會提示您選取選項。 可用的選項將對應於本機伺服器上執行的 CA 應用程式。

3. 選取設定時，視需要使用下列命令：
   - q (結束)
   - b (回到上一個功能表)
   - u (更新)
   - r (重設)
4. 輸入 1 來配置 CA Performance Center。

   系統會提示您選取配置選項。

```
SSO Configuration/CA Performance Center:
1. LDAP Authentication
2. SAML2 Authentication
3. Performance Center
4. Single Sign-On
5. Test LDAP
6. Export SAML2 Service Provider Metadata
Choose an option >
```

5. 輸入代表 Performance Center 的 3。

   系統會提示您指定優先順序。

   優先順序參數僅會套用至 CA Performance Center。
6. 輸入下列其中一個選項：

   1. 遠端值

   指只有管理員才能變更的設定。 這類設定會傳播至已向此 CA Performance Center 執行個體登錄的其他所有 CA 產品。 只有在對應的「本機覆寫」值不存在時，才會使用「遠端值」設定。

   2. 本機覆寫

   指可對所有產品變更的設定。 如果「本機覆寫」值存在，其優先順序高於「遠端值」和預設設定。

   系統會提示您選取要配置的內容。
7. 輸入下列其中一個或多個內容。 出現提示時，輸入 u 來更新值，然後提供新的值：

   1. Web 服務計劃

   指定單一登入應用程式能夠用來存取 CA Performance Center Web 服務的 URL 計劃。 如果您要使用 SSL 進行加密，請將此值變更為「https」。

2. Web 服務主機

指定單一登入應用程式能夠存取 CA Performance Center Web 服務的主機 URL。

3. Web 服務連接埠

指定單一登入應用程式能夠用來存取 CA Performance Center Web 服務的 URL 連接埠。

4. Web 服務清查

指定單一登入應用程式能夠用來存取 CA Performance Center 清查 Web 服務的 URL 路徑。

5. Web 服務產品要求

指定單一登入應用程式能夠用來存取 CA Performance Center 產品要求 Web 服務的 URL 路徑。

6. 網站計劃

指定單一登入應用程式能夠用來存取 CA Performance Center 的 URL 計劃。 如果已經設定 SSL，請使用 https://。

7. 網站主機

指定單一登入應用程式能夠用來存取 CA Performance Center 的 URL 主機。

8. 網站連接埠

指定單一登入應用程式能夠用來存取 CA Performance Center 的 URL 連接埠。

9. 網站路徑

指定單一登入應用程式能夠用來存取 CA Performance Center 的 URL 路徑。

10. 啓用 SMTP

指定是否啓用 Simple Mail Transfer Protocol (SMTP) 以讓 CA Performance Center 操作員透過電子郵件傳送報告與事件通知。

預設：已停用。

11. SMTP 伺服器位址

是 SMTP 伺服器的 IP 位址。

預設：已停用。

12. SMTP 連接埠：

指定用於 SMTP 要求的連接埠。

預設：連接埠 25。

13. SMTP SSL

指定從 CA Performance Center 或其他 CA 資料來源產品傳送電子郵件時，是否使用 SSL 加密。 請先確認已經在系統上正確設定 SSL，再啓用此選項。

預設：已停用。

14. 電子郵件回覆地址

指定要讓 CA Performance Center 產生的電子郵件訊息使用的回覆地址。 輸入 u 來更新值，然後提供電子郵件地址。 使用 username@mydomain.com 格式。

15. 電子郵件格式

指定要讓 CA Performance Center 所傳送的電子郵件訊息使用的格式。 輸入 u 來更新值，然後輸入 HTML 或 text。

16. SMTP 使用者名稱

指定當電子郵件伺服器查問 SMTP 要求時使用的使用者名稱。 提供使用者名稱，或提供空字串停用用戶端驗證。

17. SMTP 密碼

指定當電子郵件伺服器查問 SMTP 要求時使用的使用者名稱。 提供任何有效的密碼。 需要 [SMTP 使用者名稱] 參數。

8. 完成變更預設設定時，輸入 b。

   您便會返回上一組選項。

9. 再次輸入 b 返回第一組選項。

10. 輸入 q 結束。

    單一登入配置工具隨即關閉。

    CA Performance Center 會使用您提供的新值，將所有使用者導向單一登入網站。

第 2 章： 設定 LDAP 驗證

本節包含以下主題：

LDAP 支援

單一登入可提供 LDAP 整合，讓操作員能夠向您環境中執行的輕量型目錄存取通訊協定 (LDAP) 伺服器進行驗證。 一旦經過驗證，操作員將對應到管理員可指定的使用者帳戶：預先定義的使用者帳戶或自訂帳戶。

單一登入配置工具可讓您精確指定單一登入伺服器連線至 LDAP 伺服器的方式。 您也可以將個別 CA Performance Center 使用者對應到可支援其支援工作流程、同時又能保護敏感資料的使用者帳戶。

附註：「單一登入配置工具」中所做的變更只會影響新建的 LDAP 使用者。不會套用至 CA Performance Center 內現有已登錄的 LDAP 使用者。

單一登入配置工具中的 LDAP 參數可讓您將 CA Infrastructure Management 及所有登錄的資料來源整合於某個現有的驗證計劃中。 例如，LDAP 伺服器可以授權對應到 CA Performance Center 中之單一自訂使用者帳戶的使用者群組。 實際帳戶名稱及 LDAP 群組均可予以廣泛自訂。 搜尋範圍參數可讓您決定進行目錄搜尋的方式。 而且，您可以選取驗證使用者時考量的使用者帳戶內容。

啓用不含驗證機制的 LDAP 驗證

使用單一登入配置工具可指示登錄的資料來源使用相同的 LDAP 計劃來驗證使用者。 單一登入配置工具可讓您提供使 CA 伺服器以安全的方式連線至 LDAP 伺服器的參數。您也可以使用配置工具，將 LDAP 目錄中的使用者與 CA Performance Center 中預先定義或自訂的使用者帳戶相關聯。

如果您使用 GSSAPI 等驗證機制 (位於 p. 24)，則啓用 LDAP 驗證時所需採取的步驟會略微不同。 如果沒有驗證機制，您必須擁有使用服務帳戶以繫結至 LDAP 伺服器。 此帳戶需要有 LDAP 伺服器的讀取和搜尋存取權。 您必須提供連線使用者的完整 DN (辨別名稱)，您也必須啓用 [使用者繫結] 參數。

單一登入會使用您在 [連線使用者] 及 [連線密碼] 參數提供的認證來繫結至 LDAP 伺服器。 接著，單一登入將按照您在 [搜尋字串] 參數提供的字串進行目錄搜尋。 搜尋結果包含使用者的 DN。 單一登入將使用此 DN 及密碼第二次繫結至 LDAP 伺服器。

重要！ 如果未使用任何驗證機制，強烈建議與 LDAP 伺服器建立 SSL 連線。否則，密碼將以純文字傳輸至 LDAP 伺服器。

請依循下列步驟:

1. 登入已安裝 CA Performance Center 或 CA 資料來源產品的伺服器。

   以 root 使用者身分或「sudo」命令登入。

2. 在下列目錄中執行「./SsoConfig」命令，啓動單一登入配置工具：

   InstallationDirectory/CA/PerformanceCenter

   系統會提示您選取選項。 可用的選項將對應於本機伺服器上執行的 CA 應用程式。

3. 選取設定時，視需要使用下列命令：

   - q (結束)
   - b (回到上一個功能表)
   - u (更新)
   - r (重設)

4. 輸入 1 來配置 CA Performance Center。

   系統會提示您選取選項。

5. 輸入代表 LDAP 驗證的 1。

   系統會提示您指定優先順序。

   優先順序參數僅會套用至 CA Performance Center。

6. 輸入下列其中一個選項：

   1. 遠端值

   指只有管理員才能變更的設定。 這類設定會傳播至已向此 CA Performance Center 執行個體登錄的其他所有 CA 產品。 只有在對應的「本機覆寫」值不存在時，才會使用「遠端值」設定。

   2. 本機覆寫

   指可對所有產品變更的設定。 如果「本機覆寫」值存在，其優先順序高於「遠端值」和預設設定。

   系統會提示您選取要配置的內容。

7. 輸入下列其中一個或多個內容。 出現提示時，輸入 u 來更新值，然後提供新的值：

   1. 連線使用者

   定義登入伺服器用來連線至 LDAP 伺服器的使用者 ID (在此情況下是服務帳戶的使用者 ID)。 此 LDAP 使用者名稱會用來繫結至伺服器。

   重要！ 如果您未使用 GSSAPI 等驗證機制，則此參數需要是具有 LDAP 伺服器之讀取及搜尋存取權的服務帳戶。

   2. 連線密碼

   定義登入伺服器用來連線至 LDAP 伺服器的密碼。

   範例：如果登入伺服器使用固定帳戶，請輸入如下列範例所示的文字：

   ```
   SomePassword
   ```

   3. 搜尋網域

   識別 CA 單一登入所連線到的 LDAP 伺服器和連接埠。 此外，還可識別搜尋作業在驗證使用者帳戶憑證時，於目錄樹狀結構中尋找使用者的位置。 如果您未在字串中的伺服器後同時提供連接埠號碼，將使用連接埠 389。

   將下列格式使用於搜尋網域：

   LDAP://*ldap_server*:*port*/*path_to_search*

   附註：*一定要有*搜尋路徑。

4. 搜尋字串

指定用來尋找正確使用者記錄的條件。 搭配 [搜尋範圍] 參數一起使用。 如果只允許一部份的 LDAP 使用者登入，則可以使用搜尋字串來尋找記錄內的多項內容。此參數的值可包含任何有效的 LDAP 搜尋條件。

範例：

```
(saMAccountName={0})
```

5. 搜尋範圍

指定用來尋找正確使用者記錄的條件。 搭配 [搜尋字串] 參數一起使用。 決定 LDAP 伺服器針對使用者帳戶執行的搜尋範圍。 輸入下列其中一個值：

onelevel

將目前目錄包含在搜尋中。比對目前目錄中的物件，並防止意外比對位於目錄中更深層結構的項目。

subtree

將所有子目錄包含在搜尋中。 建議大部份安裝使用。

base

將搜尋限制於基本物件。

6. 使用者繫結

指定是否額外以使用者的辨別名稱 (DN) 與密碼進行一道驗證步驟 (繫結)，以驗證所提供的認證。

重要！ 如果已經在步驟 1 和 2 中輸入服務帳戶，此參數必須設定爲 [已啓用]。

預設：已停用。

7. 加密

指定第二次繫結至 LDAP 伺服器時要使用的驗證機制。

預設：簡易。

接受的值：簡易、GSSAPI、DIGEST-MD5。

8. 帳戶使用者

指定要將缺乏群組成員資格的已驗證 LDAP 使用者對應到的 CA Performance Center 預設帳戶。 搭配 [帳戶密碼] 參數一起使用。 如果某個有效使用者不符合任何群組定義，此使用者會以此欄位中指定的預設使用者 ID 進行登入。

若要允許所有使用者以自己的使用者名稱登入，請輸入：

- {saMAccountName}
- {saMAccountName} 或 {CN}

附註：[帳戶使用者] 參數會對應於此使用者之目錄項目中的某個欄位。一般而言，該值將符合您的搜尋篩選器。

9. 帳戶使用者預設複製

指定當經過驗證的 LDAP 使用者屬於 [群組] 參數所未指定群組的成員時，要複製的使用者帳戶。

範例：如果要這類使用者具有最低權限，請輸入「user」。

附註：需要現有使用者帳戶。

10. 群組

可讓您爲選取的使用者帳戶或帳戶群組決定預設的帳戶處理方式。

範例：若要讓某個群組所有的成員使用管理員帳戶登入，請輸入：

```
<LDAPGroups><Group searchTag="memberOf" searchString="CN=SEC_All
Employees,CN=Users,DC=company,DC=local" user="{saMAccountName}" passwd=""
userClone="admin"/></LDAPGroups>
```

11. 逾時

指定 CA Performance Center 對 LDAP 伺服器進行授權檢查時所等候的時間量。 如果授權檢查逾時，嘗試登入的使用者的存取就會遭拒。 若要檢視錯誤，請開啓 SSOService.log 檔案。 預設逾時爲 10000。

8. 確認 [LDAP 狀態] 設爲 [已啓用]。 如果 [LDAP 狀態] 設爲 [已停用]，則驗證會使用內部 Performance Center 使用者資料庫。
9. 輸入 q 結束。

   配置工具隨即關閉。

範例配置

1. 連線使用者：CN=********,OU=Role-Based,OU=North America,DC=ca,DC=com [伺服器帳戶的完整 DN]
2. 連線密碼：******* [伺服器帳戶的密碼]
3. 搜尋網域：LDAP://******.ca.com/DC=ca,DC=com
4. 搜尋字串：(sAMAccountName={0})
5. 搜尋範圍：Subtree
6. 使用者繫結：已啓用
7. 加密：false
8. 帳戶使用者：{sAMAccountName}
9. 帳戶使用者預設複製：user
10. 群組：「所有員工」
11. Krb5ConfigFile：krb5.conf

使用 GSSAPI 將 LDAP 伺服器連線加密

CA 單一登入可支援使用 DIGEST-MD5 或 GSSAPI 的加密連線。 使用與目錄伺服器的加密連線時，您不需要使用服務帳戶繫結至 LDAP 伺服器 (您在單一登入配置工具中設定的 UserBind 參數)。

若要使用 GSSAPI 進行加密，您必須變更配置檔案中的某些設定。

請依循下列步驟:

1. 登入已安裝 CA Performance Center 或 CA 資料來源產品的伺服器。

   以 root 使用者身分或「sudo」命令登入。
2. 切換至下列目錄：
   `[安裝目錄]/webapps/sso/Configuration/`

3. 開啓該目錄中的 krb5.conf 檔案進行編輯。
4. 設定下列必要的參數：

```
[libdefaults]
        default_realm = CA.COM
[realms]
        CA.COM  = {
                kdc = EXAMPLE.CA.COM
                default_domain = CA.COM
}

[domain_realm]
       .CA.COM = CA.COM
}
```

其中：

[libdefaults]

包含 Kerberos V5 程式庫的預設值。

default_realm

將子網域及網域名稱對應於 Kerberos 領域名稱。 讓程式按照主機的完整網域名稱決定主機的領域。 在此範例中，預設領域是 CA.COM。

領域

包含 Kerberos 領域名稱的資訊，這說明 Kerberos 伺服器的位置，並包含其他領域特定的資訊。

kdc

是支援驗證服務的 Kerberos 金鑰散佈中心。 例如，EXAMPLE.CA.COM。

default_domain

是預設的 IP 網域。 例如，CA.COM。

附註：Active Directory 或 LDAP 管理員或許可以提供 krb5.conf 檔案，或協助您建立該檔案。

5. 儲存變更。
6. 現在，遵循啓用含加密機制的 LDAP 驗證 (位於 p. 26)中的步驟，對 CA 單一登入來配置 LDAP 驗證。

啓用含加密機制的 LDAP 驗證

使用單一登入配置工具可指示登錄的資料來源使用相同的 LDAP 計劃來驗證使用者。 單一登入配置工具可讓您提供使 CA 伺服器以安全的方式連線至 LDAP 伺服器的參數。 使用 Digest-MD5 或 GSSAPI 將與 LDAP 伺服器的連線加密時，將以您指定的使用者身分進行單一繫結作業。

您也可以使用配置工具，將 LDAP 目錄中的使用者與 CA Performance Center 中預先定義或自訂的使用者帳戶相關聯。

請依循下列步驟:

1. 登入已安裝 CA Performance Center 或 CA 資料來源產品的伺服器。

   以 root 使用者身分或「sudo」命令登入。

2. 在下列目錄中執行「./SsoConfig」命令，啓動單一登入配置工具：

   InstallationDirectory/CA/PerformanceCenter

   系統會提示您選取選項。 可用的選項將對應於本機伺服器上執行的 CA 應用程式。

3. 選取設定時，視需要使用下列命令：

   - q (結束)
   - b (回到上一個功能表)
   - u (更新)
   - r (重設)

4. 輸入 1 來配置 CA Performance Center。

   系統會提示您選取選項。

5. 輸入代表 LDAP 驗證的 1。

   系統會提示您指定優先順序。

   優先順序參數僅會套用至 CA Performance Center。

6. 輸入下列其中一個選項：

   1. 遠端值

   指只有管理員才能變更的設定。 這類設定會傳播至已向此 CA Performance Center 執行個體登錄的其他所有 CA 產品。 只有在對應的「本機覆寫」值不存在時，才會使用「遠端值」設定。

   2. 本機覆寫

   指可對所有產品變更的設定。 如果「本機覆寫」值存在，其優先順序高於「遠端值」和預設設定。

   系統會提示您選取要配置的內容。

7. 輸入下列其中一個或多個內容。 出現提示時，輸入 u 來更新值，然後提供新的值：

   1. 連線使用者

   定義登入伺服器用來連線至 LDAP 伺服器的使用者 ID。 此 LDAP 使用者名稱會用來繫結至伺服器。 使用 GSSAPI 等驗證機制的連線一般不需要服務帳戶。

   範例：如果登入伺服器使用固定帳戶，請輸入使用下列語法的文字：

   ```
   CN=The User,cn=Users,dc=domain,dc=com
   ```

   另外，因爲連線使用驗證機制，您也可以輸入下列的值：

   ```
   {0}
   ```

   複雜的配置需要使用者主體名稱，才能識別使用者。 請提供「{0}」，並使用其電子郵件地址做爲網域名稱。 例如：

   ```
   {0}@domain.com
   ```

   LDAP 伺服器通常不需要有完整 DN 來進行加密連線。

   附註：基於安全考量，請勿將連線使用者設定爲靜態帳戶。 LDAP 驗證在繫結至伺服器時，只會檢查密碼。 如果您使用靜態帳戶，LDAP 樹狀結構中存在的任何使用者都能夠使用任何密碼登入。

   2. 連線密碼

   定義登入伺服器用來連線至 LDAP 伺服器的密碼。

   範例：如果登入伺服器使用固定帳戶，請輸入如下列範例所示的文字：

   ```
   SomePassword
   ```

   另外，因爲連線使用驗證機制，您也可以輸入下列的值：

   ```
   {1}
   ```

3. 搜尋網域

識別 CA 單一登入所連線到的 LDAP 伺服器和連接埠。 此外，還可識別搜尋作業在驗證使用者帳戶憑證時，於目錄樹狀結構中尋找使用者的位置。 如果您未在字串中的伺服器後同時提供連接埠號碼，將使用連接埠 389。

將下列格式使用於搜尋網域：

LDAP://*ldap_server*:*port*/*path_to_search*

附註：*一定要有*搜尋路徑。

4. 搜尋字串

指定用來在目錄中尋找正確使用者的條件。 搭配 [搜尋範圍] 參數一起使用。 如果只允許一部份的 LDAP 使用者登入，則可以使用搜尋字串來尋找記錄內的多項內容。此參數的值可包含任何有效的 LDAP 搜尋條件。

範例：

```
(saMAccountName={0})
```

5. 搜尋範圍

指定用來尋找正確使用者記錄的條件。 搭配 [搜尋字串] 參數一起使用。 決定 LDAP 伺服器針對使用者帳戶執行的搜尋範圍。 輸入下列其中一個值：

onelevel

將目前目錄包含在搜尋中。比對目前目錄中的物件，並防止意外比對位於目錄中更深層結構的項目。

subtree

將所有子目錄包含在搜尋中。 建議大部份安裝使用。

base

將搜尋限制於基本物件。

6. 使用者繫結

指定是否額外以使用者的辨別名稱 (DN) 與密碼進行一道驗證步驟 (繫結)，以驗證所提供的認證。

預設：已停用。 使用加密連線時可接受此值。

7. 加密

指定再次繫結至 LDAP 伺服器時要使用的驗證機制。

在此情況 (也就是使用驗證機制) 下，請按照 LDAP 伺服器的機制，輸入「GSSAPI」或「DIGEST-MD5」。

預設：簡易。

接受的值：簡易、GSSAPI、DIGEST-MD5。

8. 帳戶使用者

指定要將缺乏群組成員資格的已驗證 LDAP 使用者對應到的 CA Performance Center 預設帳戶。 搭配 [帳戶密碼] 參數一起使用。 如果某個有效使用者不符合任何群組定義，此使用者會以此欄位中指定的預設使用者 ID 進行登入。

若要允許所有使用者以自己的使用者名稱登入，請輸入：

- {saMAccountName}
- {saMAccountName} 或 {CN}

附註：[帳戶使用者] 參數會對應於此使用者之目錄項目中的某個欄位。一般而言，該值將符合您的搜尋篩選器。

9. 帳戶使用者預設複製

指定當經過驗證的 LDAP 使用者屬於 [群組] 參數所未指定群組的成員時，要複製的使用者帳戶。

範例：如果要這類使用者具有最低權限，請輸入「user」。

附註：需要現有使用者帳戶。

10. 群組

可讓您爲選取的使用者帳戶或帳戶群組決定預設的帳戶處理方式。

範例：若要讓某個群組所有的成員使用管理員帳戶登入，請輸入：

```
<LDAPGroups><Group searchTag="memberOf" searchString="CN=SEC_All
Employees,CN=Users,DC=company,DC=local" user="{saMAccountName}" passwd=""
userClone="admin"/></LDAPGroups>
```

11. 逾時

指定 CA Performance Center 對 LDAP 伺服器進行授權檢查時所等候的時間量。 如果授權檢查逾時，嘗試登入的使用者的存取就會遭拒。 若要檢視錯誤，請開啓 SSOService.log 檔案。 預設逾時爲 10000。

8. 確認 [LDAP 狀態] 設爲 [已啓用]。 如果 [LDAP 狀態] 設爲 [已停用]，則驗證會使用內部 Performance Center 使用者資料庫。
9. 輸入 q 結束。

   配置工具隨即關閉。

範例配置

1. SSO 配置/CA Performance Center/LDAP 驗證/遠端值：
2. 連線使用者：{0}
3. 連線密碼：{1}
4. 搜尋網域：LDAP://******.ca.com/DC=ca,DC=com
5. 搜尋字串：(sAMAccountName={0})
6. 搜尋範圍：Subtree
7. 使用者繫結：已停用
8. 加密：DIGEST-MD5
9. 帳戶使用者：{sAMAccountName}
10. 帳戶使用者預設複製：user
11. 群組：「所有員工」
12. Krb5ConfigFile：krb5.conf

更多資訊：

使用 GSSAPI 將 LDAP 伺服器連線加密 (位於 p. 24)

啓用 LDAPS 驗證

使用 [單一登入配置工具] 引導已登錄的資料來源使用 LDAP over SSL (LDAPS) 以保護使用者驗證。 按預設，LDAP 流量的傳輸不安全。 從授權單位 (CA) 安裝憑證以啓用 LDAPS。 使用 CA 單一登入，您必須將您的憑證匯入 Java 信任金鑰存放區。

單一登入配置工具可讓您提供使 CA 伺服器以安全的方式連線至 LDAP 伺服器的參數。 您也可以使用配置工具，將 LDAP 目錄中的使用者與 CA Performance Center 中預先定義或自訂的使用者帳戶相關聯。

請依循下列步驟:

1. 登入已安裝 CA Performance Center 或 CA 資料來源產品的伺服器。

   以 root 使用者身分或「sudo」命令登入。

2. 遵循「匯入 LDAP 憑證 (位於 p. 35)」主題中的指示以取得您的憑證並匯入 Java 金鑰存放區中。

3. 在下列目錄中執行「./SsoConfig」命令，啓動單一登入配置工具：

   InstallationDirectory/CA/PerformanceCenter

   系統會提示您選取選項。 可用的選項將對應於本機伺服器上執行的 CA 應用程式。

4. 選取設定時，視需要使用下列命令：

   - q (結束)
   - b (回到上一個功能表)
   - u (更新)
   - r (重設)

5. 輸入 1 來配置 CA Performance Center。

   系統會提示您選取選項。

6. 輸入代表 LDAP 驗證的 1。

   系統會提示您指定優先順序。

   優先順序參數僅會套用至 CA Performance Center。

7. 輸入下列其中一個選項：

   1. 遠端值

   指只有管理員才能變更的設定。 這類設定會傳播至已向此 CA Performance Center 執行個體登錄的其他所有 CA 產品。 只有在對應的「本機覆寫」值不存在時，才會使用「遠端值」設定。

   2. 本機覆寫

   指可對所有產品變更的設定。 如果「本機覆寫」值存在，其優先順序高於「遠端值」和預設設定。

   系統會提示您選取要配置的內容。

8. 輸入下列其中一個或多個內容。 出現提示時，輸入 u 來更新值，然後提供新的值：

1. 連線使用者

定義登入伺服器用來連線至 LDAP 伺服器的使用者 ID。 此 LDAP 使用者名稱會用來繫結至伺服器。 使用 GSSAPI 等驗證機制的連線一般不需要服務帳戶。

範例：如果登入伺服器使用固定帳戶，請輸入使用下列語法的文字：

```
CN=The User,cn=Users,dc=domain,dc=com
```

另外，因爲連線使用驗證機制，您也可以輸入下列的值：

```
{0}
```

複雜的配置需要使用者主體名稱，才能識別使用者。 請提供「{0}」，並使用其電子郵件地址做爲網域名稱。 例如：

```
{0}@domain.com
```

LDAP 伺服器通常不需要有完整 DN 來進行加密連線。

附註：基於安全考量，請勿將連線使用者設定爲靜態帳戶。 LDAP 驗證在繫結至伺服器時，只會檢查密碼。如果您使用靜態帳戶，LDAP 樹狀結構中存在的任何使用者都能夠使用任何密碼登入。

2. 連線密碼

定義登入伺服器用來連線至 LDAP 伺服器的密碼。

範例：如果登入伺服器使用固定帳戶，請輸入如下列範例所示的文字：

```
SomePassword
```

另外，因爲連線使用驗證機制，您也可以輸入下列的值：

```
{1}
```

3. 搜尋網域

識別 CA 單一登入所連線到的 LDAP 伺服器和連接埠。 此外，還可識別搜尋作業在驗證使用者帳戶憑證時，於目錄樹狀結構中尋找使用者的位置。 如果您未在字串中的伺服器後同時提供連接埠號碼，將使用連接埠 389。

將下列格式使用於搜尋網域：
LDAPS://*ldap_server*:*port*/*path_to_search*

附註：*一定要有*搜尋路徑。

若要建立 SSL 到 LDAP 伺服器的連線，請爲您的 LDAP 伺服器使用 636 或另一個 SSL 連線連接埠：

LDAPS://*LDAP Server*:636/OU=Users,OU=North America,DC=ca,DC=com

4. 搜尋字串

指定用來在目錄中尋找正確使用者的條件。 搭配 [搜尋範圍] 參數一起使用。 如果只允許一部份的 LDAP 使用者登入，則可以使用搜尋字串來尋找記錄內的多項內容。此參數的值可包含任何有效的 LDAP 搜尋條件。

範例：

```
(saMAccountName={0})
```

5. 搜尋範圍

指定用來尋找正確使用者記錄的條件。 搭配 [搜尋字串] 參數一起使用。 決定 LDAP 伺服器針對使用者帳戶執行的搜尋範圍。 輸入下列其中一個值：

onelevel

將目前目錄包含在搜尋中。比對目前目錄中的物件，並防止意外比對位於目錄中更深層結構的項目。

subtree

將所有子目錄包含在搜尋中。 建議大部份安裝使用。

base

將搜尋限制於基本物件。

6. 使用者繫結

指定是否額外以使用者的辨別名稱 (DN) 與密碼進行一道驗證步驟 (繫結)，以驗證所提供的認證。

預設：已停用。 使用加密連線時可接受此值。

7. 加密

(選用) 指定再次繫結至 LDAP 伺服器時要使用的驗證機制。

LDAPS 接受預設的簡易驗證。

8. 帳戶使用者

指定要將缺乏群組成員資格的已驗證 LDAP 使用者對應到的 CA Performance Center 預設帳戶。 搭配 [帳戶密碼] 參數一起使用。 如果某個有效使用者不符合任何群組定義，此使用者會以此欄位中指定的預設使用者 ID 進行登入。

若要允許所有使用者以自己的使用者名稱登入，請輸入：

- {saMAccountName}
- {saMAccountName} 或 {CN}

附註：[帳戶使用者] 參數會對應於此使用者之目錄項目中的某個欄位。一般而言，該值將符合您的搜尋篩選器。

9. 帳戶使用者預設複製

指定當經過驗證的 LDAP 使用者屬於 [群組] 參數所未指定群組的成員時，要複製的使用者帳戶。

範例：如果要這類使用者具有最低權限，請輸入「user」。

附註：需要現有使用者帳戶。

10. 群組

可讓您爲選取的使用者帳戶或帳戶群組決定預設的帳戶處理方式。

範例：若要讓某個群組所有的成員使用管理員帳戶登入，請輸入：

```
<LDAPGroups><Group searchTag="memberOf" searchString="CN=SEC_All
Employees,CN=Users,DC=company,DC=local" user="{saMAccountName}" passwd=""
userClone="admin"/></LDAPGroups>
```

9. 輸入 q 結束。

   配置工具隨即關閉。

範例配置

1. SSO 配置/CA Performance Center/LDAP 驗證/遠端值
2. 連線使用者：{0}
3. 連線密碼：{1}
4. 搜尋網域：LDAPS://******.ca.com:636/OU=Users,OU=North America,DC=ca,DC=com
5. 搜尋字串：(sAMAccountName={0})
6. 搜尋範圍：Subtree
7. 使用者繫結：已停用
8. 加密：簡易
9. 帳戶使用者：{sAMAccountName}
10. 帳戶使用者預設複製：user
11. 群組：「所有員工」
12. Krb5ConfigFile：krb5.conf

匯入 LDAP 憑證

若要使用 LDAPS 執行，您必須將一個 LDAP 憑證匯入 Java 金鑰存放區。

如果您尚無 SSL 憑證，可以使用 keystore 命令產生此憑證。 此程序說明如何從 CA 匯入一個憑證，並將其安裝在金鑰存放區中。

請依循下列步驟:

1. 從 LDAP 伺服器管理員取得憑證。

2. 使用下列命令，將憑證匯入 Java 信任憑證金鑰存放區中：

   ```
   keytool -importcert -keystore installDirectory/jre/
   lib/security/cacerts -storepass cacertspasswd -alias
   alias -file filename.cer
   ```

   金鑰存放區

   金鑰存放區檔案 (.ks) 的位置。

   cacertspasswd

   指定 cacerts 金鑰存放區的密碼。

   預設值：changeit

   filename.cer

   憑證的檔案名稱。

3. 建立 cacerts 檔案的備份。
4. (選用) 爲了提高安全性，請使用下列命令變更 Java 信任憑證金鑰存放區的密碼：

   ```
   keytool -storepasswd -keystore installDirectory/
   jre/lib/security/cacerts
   ```

   系統會提示您提供現有密碼及新密碼。

5. 驗證您所匯入的憑證可供使用。 使用下列命令：

   ```
   keytool -list -keystore installDirectory/jre/
   lib/security/cacerts
   ```

   重要！ 若要啓用 Web 服務，憑證必須位於 cacerts 金鑰存放區中。 若非如此，記錄中會出現錯誤，指出 PKIX 找不到憑證。

驗證 LDAP 設定

單一登入配置工具可讓您測試所提供的 LDAP 設定。 您可以確認是否正確設定 LDAP 驗證。 LDAP 測試指令碼將提示您指定要以目前 LDAP 驗證設定來測試的使用者和密碼組合。 如果尚未使用配置工具變更 LDAP 驗證設定，將使用預設值。

請依循下列步驟:

1. 登入已安裝 CA Performance Center 或受支援資料來源產品的伺服器。

   以 root 使用者身分或「sudo」命令登入。

2. 在下列目錄中執行「./SsoConfig」命令，啓動單一登入配置工具：

   [安裝目錄]/CA/PerformanceCenter

   系統會提示您選取選項。 可用的選項將對應於本機伺服器上執行的 CA 應用程式。

3. 選取設定時，視需要使用下列命令：

   - q (結束)
   - b (回到上一個功能表)
   - u (更新)
   - r (重設)

4. 輸入 1 來配置 CA Performance Center。

   系統會提示您選取選項。

5. 輸入代表 [測試 LDAP] 選項的 5。

   提示將要求您輸入使用者名稱。

6. 輸入您知道可使用 LDAP 進行驗證的使用者名稱及密碼。

   單一登入會嘗試使用您設定 LDAP 驗證時提供的參數連線至 LDAP 伺服器，並驗證使用者帳戶。 如果測試成功，將記錄許多步驟。

   有一個訊息會報告驗證成功或失敗。

7. 輸入 q 結束。

第 3 章： 設定 SAML 2.0 支援

本節包含以下主題：

關於 SAML 2.0

安全性聲明標記語言 (*SAML*) 是以 XML 爲基礎的安全通訊協定。 其中的基本概念是針對要求存取安全網域的主體 (可以是人或電腦)，交換其安全聲明。聲明內容包括主體是否能夠存取某些資源，以及是否使用外部資料來源 (例如原則存放區)。

SAML 型驗證一般用於同盟環境中，例如需要在公司網路中多加一層安全保護的雲端型服務。 不過，任何 SAML 的實作都至少需要三個元件角色：

信賴憑證者

利用其他伺服器上所儲存的身分資訊，准許獲得授權的使用者來存取系統。 也稱爲「服務提供者」。當單一登入是配置爲使用 SAML 進行驗證時，CA Performance Center 會具有此角色。

維護憑證者

負責儲存身分識別或安全資訊，並且在收到基於驗證目的索取這些資訊的要求時，提供這些資訊。此元件的 SAML 辭彙是*身分識別提供者* (*IdP*)。例如，CA SiteMinder 伺服器具有此角色。

主旨

是與 IdP 所儲存之身分識別資訊相關聯的使用者 (或電腦)。

單一登入中的 SAML 2.0 支援

CA 單一登入可支援以安全性聲明標記語言 (SAML) 2.0 版進行驗證。 單一登入服務可以接受並解碼 SAML 2.0 Token，並且再出示給遵循 SAML 標準的驗證代理程式。

單一登入的 SAML 2.0 支援包含對於單一登出的支援。 透過這項支援，登入多個使用者介面的使用者可以同時登出所有介面。 例如，登入 CA Performance Center 且稍後深入檢視 CA Network Flow Analysis 中之流程資料的使用者可以登出某個介面，並同時自動登出其他介面。

單一登入使用標準型 SAML 2.0 程式庫。 因此，其可能支援其他許多採用 SAML 2.0 標準的產品。 不過，下列 CA 產品是唯一通過 CA 單一登入測試的身分識別提供者：

- CA SiteMinder Federation Manager
- CA Arcot A-OK™ On-Demand

在 SAML 環境中，您可選取多個驗證方法。 CA Performance Center 使用者可使用單一登入的一般 (「產品」) 驗證方法登入，也可使用 SAML Token。「產品」方法對於所有使用中使用者帳戶預設爲啓用。 使用者可使用 CA 單一登入的標準 URL 存取 CA Performance Center 使用者介面。

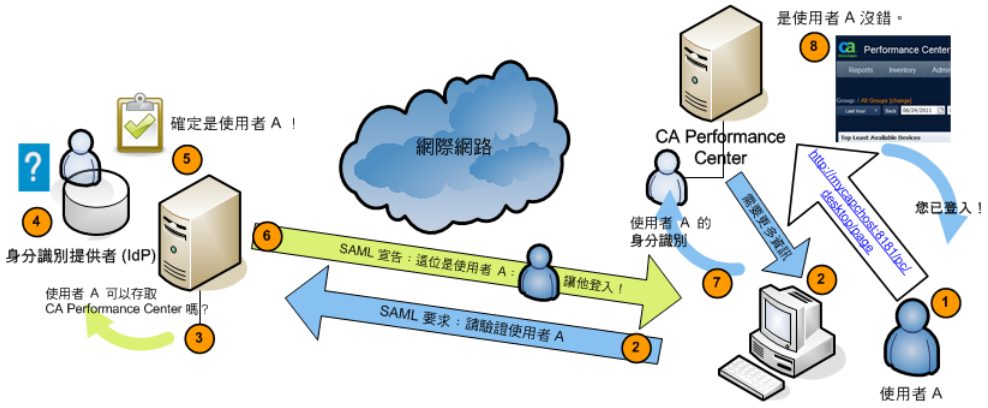
若要讓使用者使用 SAML 2.0 驗證，管理員必須使用配置工具變更某些單一登入設定。 對於所有使用者帳戶，以及所有支援 SAML 2.0 的已登錄資料來源，管理員也必須啓用外部驗證。

並非所有 CA 資料來源產品均支援 SAML 2.0。 如果您在單一登入中配置 SAML 2.0 做爲外部驗證，並登錄缺乏 SAML 支援的資料來源，CA Performance Center 使用者必須在深入檢視到該資料來源時重新驗證。

單一登入的 SAML 2.0 支援運作方式

使用單一登入的一般 CA Performance Center 驗證程序不同於採用 SAML 2.0 支援的驗證。進行 SAML 2.0 驗證時，使用者不會看見 CA Performance Center 登入頁面。使用者會被重新導向至 IdP 提供的介面。對於其他所有支援的驗證方法，單一登入會提供登入頁面。

下圖顯示使用單一登入進行的 SAML 2.0 驗證程序，以及支援 CA SiteMinder 的 IdP (例如 CA SiteMinder)：



下列一般程序說明 CA Performance Center 支援 SAML 2.0 驗證的方式。 其中已省略實作特有的選項，例如數位簽署的憑證和傳輸繫結：

1. 假設使用者嘗試導覽至 http://mycapchost:8181/pc/desktop/page 存取 CA Performance Center。
2. CA Performance Center 以 SAML 要求做爲回應，表示需向身分識別提供者 (IdP) 進行驗證。
3. 瀏覽器處理該要求，並聯繫 IdP 伺服器上執行的驗證軟體。
4. IdP 判斷使用者是否有現有的登入安全內容，也就是使用者是否已登入。
5. 如果使用者未登入，IdP 將以實作特有的方法驗證使用者。

   例如，IdP 可能與瀏覽器互動，要求使用者提供認證。此階段的驗證與 CA 單一登入無關。

6. IdP 會建立代表使用者登入安全內容的 SAML 聲明，並傳送至瀏覽器。

   該聲明包括必要屬性 subjectNameId 及選用屬性 ClonedUser。

   subjectNameId 的值對應於獲得授權的使用者。

   您可以在聲明中包含所複製使用者帳戶的名稱。 此屬性會定義獲得授權的 SAML 使用者所對應到的使用者帳戶。

7. 瀏覽器會將 SAML 聲明傳送至 CA Performance Center。
8. CA Performance Center 取得聲明並加以處理。
9. 如果聲明有效，CA Performance Center 將爲使用者建立工作階段。 瀏覽器將重新導向至目標頁面，也就是使用者的主儀表板頁面。

如何設定 SAML 驗證

若要在單一登入中啓用 SAML 2.0 驗證，管理員必須執行下列程序：

1. 按照身分識別提供者 (IdP) 的指示，建立會在 IdP 與單一登入之間建立協議的中繼資料檔案。

   如需詳細資訊，請參閱準備 IdP 協議 (位於 p. 43)。

2. (選用) 建立內容檔案，以對 IdP 與執行 CA 軟體的伺服器之間進行的通訊啓用數位簽章及加密。

   如需詳細資訊，請參閱準備安全內容檔案 (位於 p. 43)。

3. 使用單一登入配置工具，設定 SAML 驗證的參數。

   如需詳細資訊，請參閱在單一登入中配置 SAML 支援 (位於 p. 44)。

4. 在 IdP 伺服器設定參數。 例如，將所有支援 SAML 的資料來源產品網站新增至信任網站清單。

   如需詳細資訊，請參閱配置 IdP (位於 p. 48)。

5. 更新 CA Performance Center [管理] 中的使用者帳戶，新增使用外部驗證的指示。

   如需詳細資訊，請參閱完成 SAML 設定 (位於 p. 49)。

準備 IdP 協議

需要 XML 格式的中繼資料檔案，才能建立 IdP 與服務提供者之間的協議。在此情況下，CA Performance Center 及所有支援 SAML 2.0 的已登錄資料來源都需要此協議。 中繼資料檔案會描述 IdP，並包含其所支援之設定檔的相關資訊。 此檔案也包含需要向服務提供者取得之服務的相關資料。

單一登入可匯入此檔案，以設定與 IdP 之間的關係。

某些類型的 IdP (例如 CA SiteMinder) 會提供公用程式來協助您建立及匯出這些檔案。 或者，它們會依據您設定的參數，自動建立協議。

請參閱 IdP 的文件以執行此工作。

準備安全內容檔案

如果您打算將加密和數位憑證用於 CA Performance Center 與 IdP 之間的通訊，則需要有內容檔案。 在此檔案中，您將指定簽署和加密所用的憑證，以及其他啓用加密的參數。

SAML 內容檔案是儲存在單一登入主目錄：
`/opt/CA/PerformanceCenter/sso/webapps/sso`

例如，需要有如下所示的檔案：
`/opt/CA/PerformanceCenter/sso/webapps/sso/configuration/saml.properties`

內容檔案必須包含下列參數：

- 簽署憑證的目錄位置及檔案名稱。
- 存取憑證時所需的確認憑證別名及密碼。
- CA Performance Center 伺服器的主機名稱。
- 您已從 IdP 匯出之協議的目錄位置及檔案名稱。
- IdP 上設定的逾時期間長度。 該值必須符合單一登入中的 [SAML2 IdP 工作階段逾時] 參數。

以下爲語法範例：

```
# 簽署 SAML 文件時所用之憑證所在的位置
saml.sp.certificate.location=/opt/CA/saml2configuration/[Certificate filename]
saml.sp.certificate.password=[password]
saml.sp.certificate.alias=[alias]

saml.sp.metadata.hostname=[CA Performance Center 伺服器的完整主機名稱]
saml.sp.metadata.entityID=[不含 IP 網域的 CA Performance Center 伺服器名稱]
saml.sp.metadata.organizationName=[組織名稱]
saml.sp.metadata.contactPerson=[管理員的姓名]
saml.sp.metadata.email=[連絡人的電子郵件地址]

# 登入網站的中繼資料檔案所在的位置
saml.idp.metadata.file=/opt/CA/saml2configuration/[檔案名稱].xml
# IdP 工作階段逾時分鐘數。 請將此值用於自動重新驗證及登出要求
saml.idp.sessionTimeout=[逾時期間長度分鐘數]
```

每次一修改 saml.properties 檔案，就請重新匯出中繼資料檔案 (此檔案會建立與 IdP 之間的協議)。如需詳細資訊，請參閱在單一登入中配置 SAML 2.0 支援 (位於 p. 44)。 您也必須重新啓動單一登入。

在單一登入中配置 SAML 2.0 支援

CA Performance Center 管理員必須使用單一登入配置工具，設定 SAML 驗證的參數。 請在已安裝資料來源而且其使用者將使用 SAML 2.0 進行驗證的所有伺服器上，採取這些步驟。

附註：多個驗證計劃可同時並用。 例如，CA Network Flow Analysis 資料來源的使用者可以使用 LDAP 登入，而 CA Infrastructure Management 的使用者則是使用 SAML 2.0。

請依循下列步驟:

1. 登入已安裝 CA Performance Center 或 CA 資料來源產品的伺服器。

   以 root 使用者身分或「sudo」命令登入。

2. 在下列目錄中執行「./SsoConfig」命令，啓動單一登入配置工具：

   ```
   [安裝目錄]/CA/PerformanceCenter
   ```

   系統會提示您選取選項。 可用的選項將對應於本機伺服器上執行的 CA 應用程式。

3. 選取設定時，視需要使用下列命令：
   - q (結束)
   - b (回到上一個功能表)
   - u (更新)
   - r (重設)
4. 輸入與您要配置的資料來源相對應的值。 例如，輸入 1 來配置 CA Performance Center。

   系統會提示您選取選項。
5. 輸入代表 SAML 驗證的 2。

   系統會提示您指定優先順序。

   優先順序參數僅會套用至 CA Performance Center。
6. 輸入下列其中一個選項：

   1. 遠端值

   指只有管理員才能變更的設定。 這類設定會傳播至已向此 CA Performance Center 執行個體登錄的其他所有 CA 產品。 只有在對應的「本機覆寫」值不存在時，才會使用「遠端值」設定。

   2. 本機覆寫

   指可對所有產品變更的設定。 如果「本機覆寫」值存在，其優先順序高於「遠端值」和預設設定。

   系統會提示您選取要配置的內容。

   若要提供 SAML2 內容的值，請輸入 u 來更新值，然後輸入新的值。
7. 輸入 1 選取 [啓用 SAML2 驗證] 參數。

   系統會提示您選取選項。

8. 輸入 u 來變更值，然後輸入 1 以啓用 SAML 2.0 驗證。
9. 輸入 2 來設定 [複製預設使用者帳戶] 參數。

   2. 複製預設使用者帳戶

   定義獲得授權的 SAML 使用者所對應到的使用者帳戶。 與您指定的使用者帳戶相關聯的角色和產品權限將套用於所有成功驗證的使用者。

   預設：空白。

   範例：如果要所有使用者皆以使用者層級權限登入，請輸入「user」。

   附註：需要現有使用者帳戶。

   建立協議時，IdP 上配置的使用者帳戶將傳送至 CA Performance Center。它們將出現在 [管理使用者] 頁面的 [使用者清單] 中，而且可在該處受到編輯。

10. 輸入 3 來啓用安全參數。

    3. 啓用 SAML2 簽章與加密

    對 CA Performance Center 與 IdP 之間的通訊啓用安全與加密功能。

    預設：已停用

    系統會提示您選擇選項。

11. 輸入 u 來變更值，然後輸入 1 加以啓用。

    附註：此設定必須符合 IdP 上的設定。

12. 輸入 4 來啓用自動重新驗證。

    4. SAML2 自動重新驗證

    指定使用者是否需要在逾時期間到期後重新驗證。 啓用此參數將允許 IdP 執行被動式重新驗證 (「自動重新驗證」)，不需要使用者介入。

    下一個參數可讓您設定逾時期間的持續期間。

    預設：已停用。

13. 輸入 u 來變更值，然後輸入 1 加以啓用。
14. 輸入 5 來設定重新驗證逾時期間。

    5. 自動重新驗證時段

    設定執行被動式重新驗證前需經過的時間長度。如果停用 [SAML2 自動重新驗證] 參數，將忽略此參數。

    值：必須小於 [IdP 工作階段逾時] 參數。

    預設：無。

15. 輸入 u 來變更值，然後輸入新的值。
16. 輸入 6 來設定身分識別提供者工作階段的逾時期間。

    6. IdP 工作階段逾時

    設定 CA Performance Center 與身分識別提供者之間建立的工作階段自動關閉前需經過的時間長度。 例如，輸入「10」將設定 10 分鐘的逾時。

    此值必須大於對 [自動重新驗證持續期間] 參數所指定的值。 否則，不會有任何工作階段存在來執行重新驗證。 而且，此值必須符合「saml.idp.sessionTimeout」參數的安全內容檔案中設定的值。 如需詳細資訊，請參閱準備安全內容檔案 (位於 p. 43)。

    預設：無。

17. 輸入 u 來變更值，然後輸入新的值。
18. 輸入 b 兩次，返回初始提示。
19. 輸入 6 來匯出與 IdP 建立協議的中繼資料檔案。

    這個中繼資料檔案爲身分識別提供者提供了驗證使用者時要使用的參數。

    系統會要求您提供目錄路徑及檔案名稱。

20. 輸入檔案名稱。 例如，輸入下列文字：

    ```
    /tmp/CAPCMetadata.xml
    ```

    隨即按照您在配置工具中選取的設定，自動產生檔案。

    如果匯出作業成功，您將看見 XML 印出。 如果作業失敗，您將看見錯誤訊息。

21. 輸入 q 結束。

    配置工具隨即關閉。

配置 IdP

若要在 CA Performance Center 中開始使用 SAML 2.0 進行使用者驗證，請設定身分識別提供者 (IdP) 上的一些參數。 任何支援 SAML 2.0 標準的 IdP 應該都能使用，但是 CA 僅在 CA SiteMinder 上進行過測試。

您可以手動配置 IdP，也可以從「單一登入」伺服器匯入 IdP 協議。

手動配置 IdP

請依循下列步驟:

1. 在 IdP 啓用 SAML2 驗證模式。
2. 提供聲明取用者服務 (執行於已安裝單一登入的伺服器上) 的 URL。 例如：

   `http://MyServerName:8381/sso/saml2/UserAssertionService`

   其中 8381 是單一登入所使用的連接埠。
3. 將繫結方法設定爲「HTTP-Redirect」。

   附註：HTTP Redirect 是單一登入唯一支援的繫結方法。
4. 提供單一登出服務的 URL。

   需要同時有登出服務及回應位置。 這些服務都在安裝單一登入的伺服器上執行。

   使用下列範例：

   `http://MyServerName:8381/sso/saml2/LogoutService`
   `http://MyServerName:8381/sso/saml2/LogoutServiceResponse`
5. 將所有支援 SAML 2.0 的資料來源產品新增至信任網站清單。

   這個步驟可能需要將這些網站新增至同盟合夥實體清單。
6. (*選用*) 驗證數位簽章和加密設定。 您也必須在單一登入中配置這些設定。

匯入 IdP 協議檔案

請依循下列步驟:

1. 將 IdP 協議檔案從其在單一登入伺服器上的位置匯入。

   您已在使用單一登入配置工具完成其他設定步驟後，匯出這個檔案。 如需詳細資訊，請參閱在單一登入中配置 SAML 支援 (位於 p. 44)。

2. 將所有支援 SAML 2.0 的資料來源產品新增至信任網站清單。

   這個步驟可能需要將這些網站新增至同盟合夥實體清單。

3. (*選用*) 驗證數位簽章和加密設定。 您也必須在單一登入中配置這些設定。

疑難排解

問題：

您在配置 SAML 之後看到下列錯誤訊息：

```
RelayState 爲空值或空白字串。 必須設定 RelayState，SSO 才能正確運作。
語法無效，RelayState=<value>
RelayState 沒有參數 SsoRedirectUrl，RelayState=<value>
```

原因：

部份 IdP 未在驗證確認期間傳回 CA Performance Center 傳送給 IdP 的 RelayState= 值。

解決方法：

手動配置 IdP 的 RelayState。 使用下列語法：

```
SsoProductCode=pc&SsoRedirectUrl=http://[assign the value for
CAPC in your book]:8181/pc/desktop/page
```

注意：若要進行安全通訊，請將 http: 取代爲 https:，並取代連接埠號碼。

完成 SAML 2.0 設定

若要啓用 SAML 2.0 驗證，請編輯使用者帳戶來使用外部驗證。 CA Performance Center 中新的使用者帳戶預設是設爲使用 Performance Center Authentication。 管理員必須更新所有使用 SAML 2.0 進行驗證的操作員帳戶。

在 SAML2.0 配置期間，您需要指定 IdP 中要「複製」的現有 CA Performance Center 使用者帳戶。 任何已經在 IdP 上定義的使用者，都將獲得與您指定的使用者帳戶相同層級的產品權限。 這些帳戶也將散佈到 CA Performance Center，出現在 [使用者清單] 中成爲新的使用者。 通常，您必須編輯這些帳戶，確保這些使用者只能存取其工作所需的資料。

請依循下列步驟:

1. 以具有管理權限的使用者身分登入 CA Performance Center。
2. 選取 [管理] > [使用者設定]，然後按一下 [使用者]。

   [管理使用者] 頁面隨即開啓。
3. 選取要編輯的使用者帳戶。
4. 按一下 [編輯]。

   [編輯使用者] 精靈隨即開啓。
5. 選取 [外部] 驗證類型。
6. 使用精靈，對使用者帳戶進行其他任何所需的變更。 例如，移至第三個精靈對話方塊，爲這位使用者選取不同的產品權限。
7. 按一下 [儲存]。

   對使用者帳戶的變更即已儲存。

第 4 章： 對登一登入使用 HTTPS

本節包含以下主題：

安全通訊端層 (SSL) 加密：HTTPS

單一登入預設使用 HTTP (超文字傳輸通訊協定) 進行使用者瀏覽器與 CA Performance Center 之間的通訊。TLS (傳輸層安全性) 及其前身 SSL (安全通訊端層) 是廣受支援的加密通訊協定，能夠保護網際網路上的資料傳輸。TLS 與 SSL 可搭配 HTTP 使用，成爲 HTTPS (HTTP-Secure)。本指南使用 *SSL* 做爲「TLS 與 SSL」兩者的統稱。

您可以設定單一登入使用 HTTPS 而不使用 HTTP，提升監控系統的安全。

配置 CA 單一登入使用 HTTPS 是選用的。 設定單一登入網站使用 HTTPS 前，您必須取得伺服器憑證。 爲您的組織建立並實施安全性原則的團隊，或許能必須協助您進行這些步驟。

如何爲 CA 單一登入設定 HTTPS

若要啓用 SSL，必須執行幾個步驟。 首先，必須安裝用以驗證伺服器身分的憑證。 其次，必須變更資料庫，讓 CA Performance Center 能夠正確重新導向至單一登入的正確連接埠與計劃 (反之亦然)。 最後，必須變更 CA Performance Center 與單一登入兩者的服務，以反映新的連接埠與計劃。

這些步驟中有兩個重要的連接埠：CA Performance Center 連接埠 (預設爲 8181) 和單一登入連接埠 (預設爲 8381)。 連接埠 8181 是 CA Performance Center 連線連接埠。如果使用者需經過驗證，伺服器會將其重新導向至單一登入的連接埠 8381，使用者在該處會看見 [登入] 頁面。 在使用者成功登入後，伺服器會將該使用者重新導向回原始 URL 的連接埠 8181。

因此，您不能在每個配置步驟中使用相同的連接埠。如果使用相同連接埠，CA Performance Center 與單一登入間將會發生衝突。

若要爲 CA Performance Center 與單一登入啓用 HTTPS，請完成下列步驟：

1. 取得伺服器憑證，並將其安裝在 Web 伺服器金鑰存放區中 (位於 p. 52)。
2. 使用單一登入配置工具更新必要的內容 (位於 p. 57)。
3. 在 CA Performance Center 主控台上設定 HTTPS (位於 p. 59)。
4. 在單一登入中設定 HTTPS (位於 p. 61)。
5. 停止再重新啓動服務。

設定 SSL 憑證

設定單一登入網站使用 HTTPS 前，您必須取得並安裝私密金鑰以及相關聯的公用憑證。 SSL 可與自我簽署憑證或由信任的憑證授權單位所簽署的憑證搭配使用。 相關程序通常依組織及其安全團隊所採取的原則而定。 不過，這些程序會提供一些資訊來引導您。

請根據您本身的情況選取適當的程序：

- 產生並匯入新的憑證 (位於 p. 53)。
- 匯入現有的憑證 (位於 p. 56)。

附註：如需這些程序中所使用的 keytool 命令的詳細資訊，請參閱 Oracle 網站上的 Java 文件。

產生並匯入憑證

如果您尚無 SSL 憑證，可以使用 keystore 命令產生此憑證。 此程序說明如何產生自我簽署憑證，並將其安裝在金鑰存放區中。

請依循下列步驟:

1. 執行下列命令：

   ```
   cd installDirectory/PerformanceCenter/jetty/etc
   ```

2. 使用下列命令將現有 jetty 金鑰存放區檔案重新命名，以建立此檔案的備份：

   ```
   mv installDirectory/PerformanceCenter/jetty/
   etc/keystore installDirectory/PerformanceCenter/
   jetty/etc/keystore.bak
   ```

   重要！ 您必須移除舊的金鑰存放區。 如果未移除，後續步驟中將會出現錯誤訊息：「金鑰存放區遭竄改，或密碼不正確。」

3. 使用下列命令產生私密金鑰與自我簽署的公用憑證：

   ```
   keytool -genkeypair -keystore keystore_file.ks -storepass storepasswd -keyalg
   RSA -keysize 2048 -keypass keypasswd -alias alias_name
   ```

   storepasswd

   指定金鑰存放區的密碼。

   keypasswd

   指定金鑰存放區內私密金鑰的密碼。

   重要！ 請記下這些密碼，您以後無法再看到。

4. 使用下列命令，從金鑰存放區中匯出自我簽署憑證：

   ```
   keytool -exportcert -keystore keystore_file.ks -storepass storepasswd -alias
   alias_name -file filename.cer
   ```

   別名

   指定一個別名，用來指稱建立用來存放金鑰的金鑰存放區。

   filename.cer

   決定憑證要匯出成的檔案。 建議您使用不會將檔案放在現行目錄中的完整路徑名稱。

   範例：/tmp/capcCert.cer.

附註：建議您先備份 cacerts 檔案，再繼續作業。

5. 使用下列命令，將自我簽署憑證匯入 Java 信任憑證金鑰存放區中：

   ```
   keytool -importcert -keystore installDirectory/jre/lib/security/cacerts
   -storepass cacertspasswd -alias capcSelfSigned -file filename.cer
   ```

   附註：cacerts 金鑰存放區的預設密碼是「changeit」。

   cacertspasswd

   指定 cacerts 金鑰存放區的密碼。

   預設值：changeit

   filename.cer

   憑證在先前的步驟中所匯出成的檔案。

6. 備份 cacerts 檔案。
7. (選用) 爲了提高安全性，請使用下列命令變更 java 信任憑證金鑰存放區的密碼：

   ```
   keytool -storepasswd -keystore installDirectory/jre/lib/security/cacerts
   ```

   系統會提示您提供現有密碼及新密碼。

8. 確認您所匯入的金鑰存放區可以使用。 使用下列命令：

   ```
   keytool -list -keystore installDirectory/jre/lib/security/cacerts
   ```

   重要！ 若要啓用 Web 服務，自我簽署憑證必須位於 cacerts 金鑰存放區中。 若非如此，記錄中會出現錯誤，指出 PKIX 找不到憑證。

9. 使用下列命令重新啓動每個 CA Performance Center 服務：

   ```
   /sbin/service caperfcenter_sso restart
   /sbin/service caperfcenter_devicemanager restart
   /sbin/service caperfcenter_console restart
   ```

   您的自我簽署 SSL 憑證隨即產生，並安裝在金鑰存放區中。

後續步驟：

- (選用) 將自我簽署憑證轉換成憑證授權單位 SSL 憑證 (位於 p. 55)
- 設定連接埠及網站來支援 HTTPS (位於 p. 57)

將自我簽署憑證轉換成憑證授權單位 SSL 憑證

當使用者開啓 CA Performance Center 時，自我簽署憑證會引起瀏覽器跳出警告。 使用者可以手動關閉警告來繼續作業。 然而，由信任的憑證授權單位簽署的憑證，則不會引起此瀏覽器警告。 下列程序說明如何將自我簽署的憑證轉換成由信任憑證授權單位簽署的憑證。

請依循下列步驟:

1. 執行下列命令：

   `cd installDirectory/PerformanceCenter/jetty/etc`

2. 使用下列命令匯出憑證簽章要求：

   `keytool -certreq -keystore keystore_file.ks -storepass storepasswd -alias alias_name -keypass keypasswd -file requestFileName.csr`

   ***requestFileName*.csr**

   決定所匯出之簽章要求的路徑與檔案名稱。

3. 請將產生的檔案 (*requestFileName*.csr) 連同其他任何所要求的資訊，一併傳送至合格的簽署授權單位。

   憑證授權單位會傳送一個簽署後的憑證 (*signedCert*.cer) 給您。 他們可能也會提供根憑證授權單位憑證 (*rootCA*.cer)，用以驗證已簽署的憑證。

4. (*選用*) 請使用下列命令，判斷根憑證授權單位憑證是否爲預設 Java 信任授權的一部份：

   `keytool -list -v -keystore installDirectory/jre/lib/security/cacerts -storepass cacertspasswd`

5. (*選用*) 在輸出中搜尋當初簽署您憑證的憑證授權單位。 如果其中未列出該憑證授權單位，請使用下列命令將其新增至信任的授權單位清單中：

   `keytool -importcert -keystore installDirectory/jre/lib/security/cacerts -storepass cacertspasswd -alias myRootCa -file rootCA.cer`

6. 使用下列命令匯入已簽署的憑證：

   `keytool -importcert -trustcacerts -keystore keystore -storepass storepasswd -alias alias_name -keypass keypasswd -file signedCert.cer`

7. 使用下列命令，驗證 jetty 金鑰存放區的內容：

   ```
   keytool -list -keystore installDirectory/PerformanceCenter/jetty/etc/keystore
   ```

   您所匯入的單一憑證會出現在清單中。

8. 使用下列命令重新啓動每個 CA Performance Center 服務：

   ```
   /sbin/service caperfcenter_sso restart
   /sbin/service caperfcenter_devicemanager restart
   /sbin/service caperfcenter_console restart
   ```

   憑證授權單位 SSL 憑證會取代您在金鑰存放區中的自我簽署憑證。

後續步驟：設定連接埠及網站來支援 HTTPS (位於 p. 57)。

匯入金鑰與現有的憑證

您可以使用不同來源的私密金鑰與公用憑證 (可以是自我簽署憑證或憑證授權單位憑證)。 例如，您的安全團隊提供了專爲貴組織自訂的 SSL 憑證。 若要使用此 SSL 憑證，請匯入私密金鑰與已簽署的憑證。

請依循下列步驟:

1. 執行下列命令：

   ```
   cd /opt/CA/PerformanceCenter/jetty-version/etc
   ```

2. 使用下列命令移除舊的金鑰存放區：

   ```
   rm keystore
   ```

3. 使用下列命令，從私密金鑰與憑證建立 PKCS#12 金鑰存放區：

   ```
   openssl pkcs12 -export -in certificate.pem -inkey privatekey.pem -name MyAlias
   -out keystore.pkcs12
   ```

   certificate.pem

   指定已提供給您的憑證。

   privatekey.pem

   指定已提供給您的私密金鑰。

   附註：此命令只能在 Linux 上運作。

4. 使用下列命令，將金鑰與憑證匯入 CA Performance Center 金鑰存放區中：

   ```
   keytool -importkeystore -destkeystore keystore_file -deststorepass storepasswd
   -srckeystore keystore.pkcs12 -srcstoretype pkcs12 -srcalias src_alias_name
   -destalias dest_alias_name -destkeypass keypasswd
   ```

5. 使用下列命令重新啓動每個 CA Performance Center 服務：

   ```
   /sbin/service caperfcenter_sso restart
   /sbin/service caperfcenter_devicemanager restart
   /sbin/service caperfcenter_console restart
   ```

   您現有的 SSL 憑證便已匯入金鑰存放區中。

後續步驟：設定連接埠及網站來支援 HTTPS (位於 p. 57)。

附註：若憑證不包含一個可終止金鑰存放區中憑證的憑證鍊，請將憑證匯入 Java cacerts 金鑰存放區。 執行下列命令以判定憑證是否包含憑證鍊：

```
keytool -printcert -file filename
```

filename

指定憑證的名稱。

參見產生與匯入憑證 (位於 p. 53)以瞭解將憑證匯入 Java cacerts 金鑰存放區的資訊。

配置連接埠及網站使用 SSL

單一登入預設使用連接埠 8381。 若要設定 HTTPS，請使用單一登入配置工具來更新預設連接埠計劃及連接埠，以符合加密設定。

在每部已安裝資料來源的伺服器上，執行此程序中的工作。

請依循下列步驟:

1. 在下列目錄中執行「./SsoConfig」命令，啓動單一登入配置工具：

   ```
   [安裝目錄]/CA/PerformanceCenter
   ```

   系統會提示您選取選項。

2. 變更設定時，視需要使用下列命令：
   - q (結束)
   - b (回到上一個功能表)
   - u (更新)
   - r (重設)
3. 輸入 1 來選取 CA Performance Center。

4. 輸入 4 來配置單一登入。

   系統會提示您指定優先順序。

5. 輸入下列其中一個選項：

   1. 遠端值

   指只有管理員才能變更的設定。 這類設定會傳播至已向此 CA Performance Center 執行個體登錄的其他所有 CA 產品。 只有在對應的「本機覆寫」值不存在時，才會使用「遠端值」設定。

   2. 本機覆寫

   指可對所有產品變更的設定。 如果「本機覆寫」值存在，其優先順序高於「遠端值」和預設設定。

   系統會提示您選取要配置的內容。

6. 輸入代表計劃內容的 12。
7. 輸入「u」來更新值。
8. 提供「https」做爲值。
9. 輸入代表連接埠內容的 13。
10. 將值更新爲「8382」。
11. 輸入「b」兩次，返回 [SSO 配置/CA Performance Center] 功能表。
12. 輸入「3」來配置 Performance Center。

    系統會提示您指定優先順序。

13. 輸入代表遠端值的「1」，或輸入代表本機覆寫的「2」。
14. 輸入「6」來選取網站計劃。
15. 將值更新爲「https」。
16. 輸入「8」來選取網站連接埠。
17. 將值更新爲「8182」。
18. 輸入 q 結束。

現在您必須配置 CA Performance Center 檔案使用 HTTPS。

配置 CA Performance Center 使用 HTTPS

您必須編輯某些配置檔案，以反映新的網站及連接埠設定。編輯配置檔案，以 HTTPS 連接器取代 HTTP 連接器。 您也必須重新啓動 CA Performance Center 服務，變更才會生效。

請依循下列步驟:

1. 切換至下列目錄：

   ```
   cd/[安裝目錄]/CA/PerformanceCenter/PC
   ```

2. 開啓 start.ini 檔案進行編輯。

3. 找出下列一行並移除「#」，使此行產生作用：

   ```
   #/opt/CA/PerformanceCenter/PC/etc/jetty-ssl.xml
   ```

   其中「/opt/CA」是預設的安裝目錄。

4. 儲存 start.ini。

5. 切換至下列目錄：

   ```
   cd/[安裝目錄]/CA/PerformanceCenter/PC/etc
   ```

6. 在該目錄中建立名稱爲「jetty-ssl.xml」、且包含下列內容的檔案：

   ```
   <?xml version="1.0"?>
   <!DOCTYPE Configure PUBLIC "-//Jetty//Configure//EN"
   "http://www.eclipse.org/jetty/configure.dtd">
   <Configure id="Server" class="org.eclipse.jetty.server.Server">
     <Call name="addConnector">
       <Arg>
         <New class="org.eclipse.jetty.server.ssl.SslSelectChannelConnector">
            <Set name="Port">8182</Set>
            <Set name="maxIdleTime">30000</Set>
           <Set name="Keystore"><Property name="jetty.home" default="."
   />/etc/keystore</Set>
           <Set name="Password">***PASSWORD***</Set>
            <Set name="KeyPassword">***PASSWORD***</Set>
           <Set name="truststore"><Property name="jetty.home" default="."
   />/etc/keystore</Set>
           <Set name="trustPassword">***PASSWORD***</Set>
           <Set name="allowRenegotiate">true</Set>
         </New>
       </Arg>
     </Call>
   </Configure>
   ```

7. 以系統中使用的密碼取代所有出現的「***PASSWORD***」值。

8. 儲存檔案。
9. 開啓 jetty.xml 檔案進行編輯。
10. 對於預設 HTTP 連接器，移除下列各行：

```
<Call name="addConnector">
  <Arg>
      <New class="org.eclipse.jetty.server.nio.SelectChannelConnector">
          <Set name="host"><Property name="jetty.host" /></Set>
            <!-- Changed: Used to be Property -->
           <Set name="port"><SystemProperty name="jetty.port"
default="8181"/></Set>
           <Set name="maxIdleTime">300000</Set>
           <Set name="Acceptors">2</Set>
           <Set name="statsOn">false</Set>
           <Set name="confidentialPort">8443</Set>
           <Set name="lowResourcesConnections">20000</Set>
           <Set name="lowResourcesMaxIdleTime">5000</Set>
      </New>
  </Arg>
 </Call>
```

11. 儲存 jetty.xml。
12. 切換至下列目錄：

```
cd/[安裝目錄]/CA/PerformanceCenter/PC/conf
```

13. 編輯 wrapper.conf 檔案。 在下列一行中，以「8182」取代「8181」，以符合先前所述在 jetty-ssl.xml 中定義的連接埠：

```
  wrapper.java.additional.2=-Djetty.port=8181
```

14. 儲存 wrapper.conf。
15. 切換至下列目錄：

```
cd /[安裝目錄]/CA/PerformanceCenter/sso/webapps/
sso/configuration
```

16. 編輯「CAPerformanceCenter.xml」檔案。
17. 以 SSL 適用的設定取代 <Scheme> 及 <Port> 值：

```
<?xml version="1.0" encoding="utf-8" ?>
<Configuration>
     <SingleSignOnEnabled>True</SingleSignOnEnabled>
     <SingleSignOnProductCode>pc</SingleSignOnProductCode>
     <SignInPageProductDefaultUrl>
```

```
            <Scheme>https</Scheme>
            <Port>8182</Port>
            <PathAndQuery>/pc/desktop/page</PathAndQuery>
        </SignInPageProductDefaultUrl>
        <SingleSignOnWebServiceUrl>
            <Scheme>https</Scheme>
            <Port>8182</Port>
            <PathAndQuery>/pc/center/webservice/sso</PathAndQuery>
        </SingleSignOnWebServiceUrl>
</Configuration>
```

更新單一登入配置並重新啓動服務

編輯一些啓動檔，以支援單一登入中的 SSL 加密。 您也必須重新啓動所有的 CA Performance Center 及單一登入服務，才能更新設定。

請依循下列步驟:

1. 切換至下列目錄：

   ```
   cd/[安裝目錄]/CA/PerformanceCenter/sso
   ```

2. 開啓 start.ini 檔案進行編輯。

3. 找出下列一行並移除「#」，使此行產生作用：

   ```
   #/opt/CA/PerformanceCenter/sso/etc/jetty-ssl.xml
   ```

   其中「/opt/CA」是預設的安裝目錄。

4. 儲存 start.ini。

5. 切換至下列目錄：

   ```
   cd/[安裝目錄]/CA/PerformanceCenter/sso/etc
   ```

6. 在該目錄中建立名稱爲「jetty-ssl.xml」、且包含下列內容的檔案：

   ```
   <?xml version="1.0"?>
   <!DOCTYPE Configure PUBLIC "-//Jetty//Configure//EN"
   "http://www.eclipse.org/jetty/configure.dtd">
   <Configure id="Server" class="org.eclipse.jetty.server.Server">
     <Call name="addConnector">
       <Arg>
         <New class="org.eclipse.jetty.server.ssl.SslSelectChannelConnector">
            <Set name="Port">8382</Set>
            <Set name="maxIdleTime">30000</Set>
   ```

```
        <Set name="Keystore"><Property name="jetty.home" default="."
/>/etc/keystore</Set>
        <Set name="Password">***PASSWORD***</Set>
        <Set name="KeyPassword">***PASSWORD***</Set>
       <Set name="truststore"><Property name="jetty.home" default="."
/>/etc/keystore</Set>
        <Set name="trustPassword">***PASSWORD***</Set>
        <Set name="allowRenegotiate">true</Set>
      </New>
    </Arg>
  </Call>
</Configure>
```

7. 以系統中使用的密碼取代所有出現的「***PASSWORD***」值。
8. 儲存 jetty-ssl.xml。
9. 開啓 jetty.xml 檔案。
10. 對於預設 HTTP 連接器，移除下列各行：

```
<Call name="addConnector">
  <Arg>
      <New class="org.eclipse.jetty.server.nio.SelectChannelConnector">
          <Set name="host"><Property name="jetty.host" /></Set>
            <!-- Changed: Used to be Property -->
           <Set name="port"><SystemProperty name="jetty.port"
default="8181"/></Set>
           <Set name="maxIdleTime">300000</Set>
           <Set name="Acceptors">2</Set>
           <Set name="statsOn">false</Set>
           <Set name="confidentialPort">8443</Set>
           <Set name="lowResourcesConnections">20000</Set>
           <Set name="lowResourcesMaxIdleTime">5000</Set>
      </New>
  </Arg>
 </Call>
```

11. 儲存 jetty.xml。
12. 切換至下列目錄：

```
[安裝目錄]/CA/PerformanceCenter/sso/conf
```

13. 編輯 wrapper.conf 檔案。 在下列一行中，以「8382」取代「8381」，以符合先前所述在 jetty-ssl.xml 中定義的連接埠：

```
wrapper.java.additional.2=-Djetty.port=8381
```

14. 儲存 wrapper.conf。

15. 輸入下列命令來停止主控台、裝置管理員及 SSO 服務：

```
service caperfcenter_console stop
service caperfcenter_devicemanager stop
service caperfcenter_sso stop
```

16. 輸入下列命令來重新啓動服務

```
service caperfcenter_sso start
service caperfcenter_devicemanager start
service caperfcenter_console start
```

第 5 章： 疑難排解

本節包含以下主題：

瀏覽器顯示錯誤

徵狀：

我在登入頁面輸入密碼後，網頁瀏覽器將我重新導向到錯誤頁面。 我是否輸入了錯誤的密碼？

解決方法：

這個徵兆並不表示您輸入了錯誤的 SAML 認證。 這個瀏覽器錯誤 (例如 401 或 500) 只是在表示單一登入已將瀏覽器重新導向至登入 URL，但是身分識別提供者 (IdP) 伺服器不通。

執行下列步驟：

- 確認 IdP 伺服器正在執行中。
- 測試 CA Performance Center 伺服器與 IdP 伺服器之間的網路連線。

日誌

透過每天或每週查看記錄，您可以在問題開始影響正常作業前就將其解決。 所有記錄都儲存在相關服務 (或精靈) 的對應子資料夾中。 請至下列路徑中尋找記錄檔：

```
CA/PerformanceCenter/servicename/logs
```

以下列其中一個服務名稱取代 *servicename* 參數：

DM

裝置管理員。

- DMService.log--從 [裝置管理員] 輸出，主要與同步作業相關。
- wrapper.log-- caperfcenter_devicemanager 程序記錄。

EM

事件管理員。

- EMService.log--從 [事件管理員] 輸出；包含裝置與警告的詳細資料。
- wrapper.log--caperfcenter_eventmanager 程序記錄。

PC

主要的主控台程式。

- PCService.log--CA Performance Center 相關登入；包含使用者介面與檢視元件。
- wrapper.log--caperfcenter_console 程序記錄。

SSO

單一登入驗證軟體。

- SSOService.log--單一登入記錄，包括 HTTPS (安全通訊端層) 資訊，其中 HTTPS 已配置完成。
- wrapper.log--caperfcenter_sso 程序記錄。

有單一登入配置工具的相關問題，請檢查下列位置的應用程式記錄：

```
/opt/CA/PerformanceCenter/sso/logs/application.log
```

記錄檔案名稱會包含相關的日期和時間。

每天都會自動產生新的記錄檔。 舊的記錄檔會在 14 天後自動移除，以避免佔用過多磁碟空間。

存取最近的記錄檔，尋找與資料庫或資料來源同步處理相關的錯誤。 您可以從 [儀表板] 索引標籤開啓 [事件] 儀表板，然後依 [狀態] 排序。 如果想查看相關記錄檔，請記下事件類型以及失敗的日期和時間。 在記錄目錄中，開啓檔案名稱中有對應日期的記錄檔。

檢視稽核記錄

單一登入會將使用者的每日登入活動詳細資料記錄到檔案中，以支援安全稽核。 檢查記錄即可確認使用者活動。

請依循下列步驟:

1. 登入已安裝 CA 資料來源產品的伺服器。
2. 開啓命令提示字元並切換至下列目錄：

   `[安裝目錄]/PerformanceCenter/sso/logs`

   附註：稽核記錄是儲存在 Windows 伺服器的下列位置：
   `[安裝目錄]\Portal\SSO\logs`
3. 輸入 dir 查看目錄的內容。

   記錄檔的檔案名稱是 SingleSignOnAuditLogyyyy-mm-dd.log。
4. 輸入要檢視的稽核檔案名稱。

   檔案便會在本機的文字編輯器應用程式中開啓。

詞彙表

LDAP

LDAP (輕量型目錄存取通訊協定) 是一種通訊協定，可指定在 IP 網路中搜尋和編輯目錄並儲存目錄資訊的方法。 此外，LDAP 因爲包含驗證元件，因此常被用來保護網路存取。 LDAP 目錄通常會依邏輯單位群組進行分類組織。 Microsoft Active Directory 便是一個使用 LDAP 的知名目錄應用程式。

SAML

安全性聲明標記語言 (*SAML*) 是以 XML 爲基礎的安全通訊協定。 其中的基本概念是針對要求存取安全網域的主體 (可以是人或電腦)，交換其安全聲明。 聲明內容包括主體是否能夠存取某些資源，以及是否使用外部資料來源 (例如原則存放區)。

SSL

SSL (安全通訊端層) 是許多網頁瀏覽器都支援的一種加密通訊協定，可維護網際網路上的資料安全。 伺服器會交換 SSL 憑證，其中包含用於將交換資料加密的公用金鑰，以及用於將該資料解密的私密金鑰。 SSL 可讓網頁瀏覽器按照瀏覽器、用戶端電腦及伺服器能力來指定要使用的加密層級。 最高爲 256 位元加密，這是最難解密的層級。

TLS

TLS (傳輸層安全性) 及其前身 SSL (安全通訊端層) 是廣受支援的加密通訊協定，能夠保護網際網路上的資料傳輸。 SSL/TLS 可搭配 HTTP 使用，成爲 HTTPS (HTTP-Secure)。

身分識別提供者 (IdP)

身分識別提供者 (IdP) 負責儲存身分識別或安全資訊，並且會在收到基於驗證目的索取這些資訊的要求時，提供這些資訊。 也稱爲「維護憑證者」，是 SAML 驗證所需的三個元件角色之一。

配置工具

*配置工具*是一種命令列應用程式，可供管理員調整單一登入網站及相關 CA 資料來源產品所用的設定。

單一登入

*單一登入*是 CA Performance Center 及所有受支援資料來源適用的驗證計劃。一旦使用者通過 CA Performance Center 的驗證，便可在主控台和已登錄資料來源間進行導覽，而無須重新登入。