Sun™ Identity Manager 8.0
管理

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

文件號碼：820-5436

目錄

表

圖

前言

本指南說明如何使用 Sun Identity Manager 軟體來讓使用者安全存取您的企業資訊系統和應用程式。本指南以圖例說明相關程序與方案，以協助您使用 Identity Manager 系統來執行一般性與定期性的管理工作。

本書適用對象

「Identity Manager 管理」適用於使用 Sun 伺服器和軟體來實作整合的身份管理和 Web 存取平台的管理員、軟體開發者以及 IT 服務提供者。

瞭解下列技術有助於應用本書中討論的資訊：

- 簡易目錄存取協定 (LDAP)
- Java 技術
- JavaServer Pages™ (JSP™) 技術
- 超文字傳輸協定 (HTTP)
- 超文字標記語言 (HTML)
- 可延伸標記語言 (XML)

閱讀本書之前

Identity Manager 是 Sun Java Enterprise System 的一個元件，Sun Java Enterprise System 是一種軟體基礎架構，支援分散在網路或網際網路環境中的企業應用程式。您應熟悉 Sun Java Enterprise System 隨附的文件，該文件可在線上存取 (網址爲 http://docs.sun.com/coll/entsys_04q4)。

由於在 Identity Manager 部署中將 Sun Directory Server 用做資料存放區，因此您應熟悉該產品隨附的文件。Directory Server 文件可在線上存取 (網址爲 http://docs.sun.com/coll/DirectoryServer_04q2)。

本書中使用的慣例

本小節中的表格說明了本書中使用的慣例。

印刷排版慣例

下表描述本書在印刷排版上所做的變更。

表 1 印刷排版慣例

字型	含義	範例
AaBbCc123 (固定間距)	API 和語言元素、HTML 標記、網站 URL、指令名稱、檔案名稱、目錄路徑名稱、螢幕畫面輸出、範例代碼。	請編輯您的 `.login` 檔案。 使用 `ls -a` 列出所有檔案。 `% You have mail。`
AaBbCc123 (固定間距粗體)	您所鍵入的內容 (與螢幕畫面輸出相區別)。	`% su` `Password:`
術語強調變數	新的詞彙或術語、要強調的詞彙。將用實際的名稱或數值取代的指令行變數。	這些被稱爲**類別選項**。 你必須是**超級使用者**才能執行此操作。 要刪除檔案，請鍵入 **rm** 檔案名稱。
AaBbCc123 (斜體)	書籍標題、新術語、要強調的文字。 指令或路徑名稱中要由真實名稱或值替代的預留位置。	請閱讀「使用者指南」中的第 6 章。 這些稱爲類別選項。 請*勿*儲存此檔案。 該檔案位於 *install-dir*/bin 目錄中。
「AaBbCc123」	用於書名及章節名稱。	「Solaris 10 使用者指南」 請參閱第 6 章「資料管理」。

符號

下表說明了本書中使用的符號慣例。

表 2　符號慣例

符號	說明	範例	含義
[ ]	包含可選指令選項。	ls [-l]	-l 選項不是必要的選項。
{ | }	包含一組選項，您可以從中選擇所需指令選項。	-d {y|n}	-d 選項需要您使用 y 引數或 n 引數。
-	同時按下多個按鍵。	Ctrl-A	按下 Ctrl 鍵的同時按下 A 鍵。
+	連續按下多個按鍵。	Ctrl+A+N	按下 Ctrl 鍵，釋放該鍵，然後按下後續按鍵。
>	指示圖形化使用者介面中的功能表項目選取。	[檔案] > [新增] > [範本]	從 [檔案] 功能表中選擇 [新增]。從 [新增] 子功能表中選擇 [範本]。

相關文件

http://docs.sun.com℠ 網站可讓您存取 Sun 線上技術文件。您可以瀏覽歸檔檔案或搜尋特定書籍標題或主旨。

此文件集中的書籍

Sun 提供了附加文件和資訊來協助您安裝、使用和配置 Identity Manager。

- **Identity Manager Installation** - 可協助您安裝與配置 Identity Manager 和相關軟體的逐步說明與參照資訊。
- **Identity Manager Upgrade** - 可協助您升級與配置 Identity Manager 和相關軟體的逐步說明與參照資訊。
- **Identity Manager 管理** - 說明如何使用 Identity Manager，讓使用者安全存取您的企業資訊系統和管理使用者規範遵循的程序、指導和範例。
- **Identity Manager Technical Deployment Overview** - 對 Identity Manager 產品 (包括物件架構) 的概念性簡介和基本產品元件簡介。

- **Identity Manager Workflows, Forms, and Views** - 說明如何使用 Identity Manager 工作流程、表單和檢視的參照資訊和程序資訊 (包括自訂這些物件所需工具的相關資訊)。
- **Identity Manager Deployment Tools** - 說明如何使用不同 Identity Manager 部署工具的參照和程序資訊，包含規則和規則程式庫、一般作業和程序，以及由 Identity Manager 伺服器提供的 SOAP 型 Web 服務介面。
- **Identity Manager Resources Reference** - 說明如何將資源的帳號資訊載入 Identity Manager 並進行同步化的參照資訊和程序資訊。
- **Identity Manager Tuning, Troubleshooting, and Error Messages** - 說明 Identity Manager 錯誤訊息和異常，並爲追蹤和排解工作中可能遇到的疑難問題，提供參照資訊和程序資訊。
- Identity Manager Service Provider Deployment - 說明如何規劃和實作 Sun Identity Manager Service Provider 功能的參照和程序資訊。
- Identity Manager 說明 - 提供有關 Identity Manager 的完整程序、參照和術語資訊的線上指導與資訊。按一下 Identity Manager 功能表列中的 [說明] 連結即可存取說明。關鍵欄位上提供了指導 (欄位特定資訊)。

存取 Sun 線上資源

如需有關產品下載、專業服務、修補程式與支援以及其他開發者的資訊，請至以下位置：

- 下載中心
  http://wwws.sun.com/software/download/
- 專業服務
  http://www.sun.com/service/sunps/sunone/index.html
- Sun Enterprise Services、Solaris 修補程式與支援
  http://sunsolve.sun.com/
- 開發者資訊
  http://developers.sun.com/prodtech/index.html

連絡 Sun 技術支援

如果您在產品文件中找不到所需之本產品相關技術問題的解答，請至 http://www.sun.com/service/contacting。

相關協力廠商網站參照

Sun 對本文件中提到的協力廠商網站的可用性不承擔任何責任。對於此類網站或資源中的 (或透過它們所取得的) 任何內容、廣告、產品或其他材料，Sun 並不表示認可，也不承擔任何責任。對於因使用或依靠此類網站或資源中的 (或透過它們所取得的) 任何內容、產品或服務而造成的、名義上造成的或連帶產生的任何實際或名義上之損壞或損失，Sun 概不負責，也不承擔任何責任。

Sun 歡迎您提出寶貴意見

Sun 致力於提高文件品質，因此誠心歡迎您提出意見與建議。

若要分享您的意見，請至 http://docs.sun.com，並按一下 [傳送意見]。在線上表單中，請提供文件標題和文件號碼。文件號碼是一個七位或九位的數字，可以在書的標題頁面或文件的頂部找到。

第 1 章

Identity Manager 簡介

Sun Identity Manager 系統可讓您管理和稽核對帳號和資源的存取權。Identity Manager 提供權能與工具，讓您可以快速處理定期與日常的使用者佈建及稽核作業，爲內部與外部客戶提供卓越的服務。

本章將提供有關以下主題的簡介：

概述

今日的企業需要 IT 服務滿足其不斷增加的彈性以及各項權能需求。過去，對企業資訊與系統存取的管理需要直接與有限數目的帳號互動。現在，管理存取不僅意味著處理日益增加的內部客戶數目，同時也需處理您企業以外的合作夥伴與客戶。

由於此類存取需要增加所產生的管理費用或許非常龐大。身爲管理員，您必須透過有效並且安全的方式，讓所有人 (不論是企業內部或外部) 皆能執行他們的工作。而在您提供初始存取權之後，您將持續面對更複雜的挑戰，例如忘記密碼、變更角色與企業關係。

此外，今日的企業面臨管理關鍵商業資訊之安全性與完整性的嚴格需求。在受到與規範遵循相關法律約束的環境下，諸如「沙賓法案 (SOX)」、「醫療保險機動及責任法案 (HIPAA)」，以及「美國金融服務現代化法案 (GLBA)」，爲了對作業進行監控和報告而產生的費用益發龐大及昂貴。您必須能夠快速回應存取控制中的變動，以及滿足那些可確保企業安全的資料收集與報告需求。

我們特別開發出 Identity Manager 以協助您在動態環境中處理這些管理方面的挑戰。透過使用 Identity Manager 分配存取管理費用並解決規範遵循問題，您可以輕鬆建立應對主要挑戰的解決方案：我如何定義存取權？定義之後，我要如何維持靈活的彈性與控制？

Identity Manager 的設計安全而又極具靈活性，可以讓您根據您企業的結構對其進行設定，以應對這些挑戰。透過將 Identity Manager 物件對映至您管理的實體 (即使用者與資源)，將可以大幅提升作業效率。

在服務提供者環境中，Identity Manager 還將這些權能延伸至管理企業外部網路使用者。

Identity Manager 系統的目標

Identity Manager 解決方案可讓您實現以下目標：

- 對廣泛的系統與資源之帳號存取進行管理。
- 以安全方式爲每位使用者的系列帳號管理動態帳號資訊。
- 設定委託權限以建立並管理使用者帳號資料。
- 處理大量企業資源以及日益增加的大量企業外部網路客戶與合作夥伴。
- 安全地授權使用者企業資訊系統存取權。藉由 Identity Manager，您可擁有完整的整合功能，以授予、管理與撤銷內部與外部組織中的存取權限。
- 透過不保留資料的方式保持資料同步。Identity Manager 解決方案支援上層系統管理工具應當遵守的兩個主要原則：
  - 產品對受其管理的系統的影響應該減至最低，以及
  - 產品不應該因爲新增其他需要管理的資源而增加企業的複雜性。
- 定義稽核策略以管理是否遵循使用者存取權限規範，並透過自動修正動作和電子郵件警示來管理違規。
- 執行定期存取檢閱、定義驗證檢閱，以及核准自動驗證使用者權限的程序之程序。
- 透過面板監視關鍵資訊，以及稽核與檢閱統計。

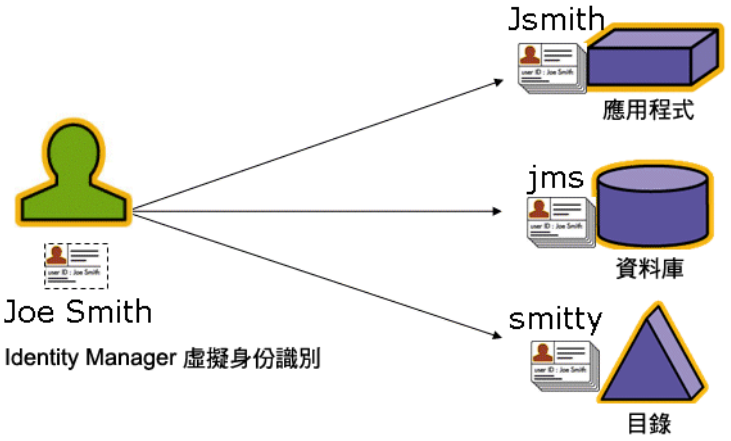
定義使用者對資源的存取權

更廣泛意義的企業使用者可以是與您公司有關聯的任何人，包括員工、用戶、夥伴、供應商或採購人員。在 Identity Manager 系統中，使用者以使用者帳號來代表。

由於使用者與您的企業和其他實體的關係各有不同，因此使用者需要存取的內容 (例如電腦系統、資料庫中儲存的資料或特定的電腦應用程式) 也會有所差異。在 Identity Manager 專有名詞中，這些內容即爲資源。

因爲通常使用者在他們存取的每個資源上都具有一個或多個身份，所以 Identity Manager 會建立單一的虛擬身份來對映到不同的資源。這可讓您將使用者當成單一實體的身份來管理。請參閱圖 1-1。

圖 1-1　Identity Manager 使用者帳號資源關係



若要以效率極高的方式管理大量使用者，您需要以邏輯的方式將使用者加以分組。在大多數公司中，使用者按職能部門或地理部門分組。一般而言，這些部門中的每個部門都需要存取不同的資源。在 Identity Manager 專有名詞中，這種類型的群組稱爲組織。

將使用者分組的另一種方式是依照類似的特性 (例如公司關係或工作職能) 進行分類。Identity Manager 將這些群組識別爲角色。

在 Identity Manager 系統中，將角色指定給使用者帳號可以提昇啓用與停用資源存取的效率。而指定帳號給組織可以使得管理責任的委派更有效率。

也可以應用策略來直接或間接管理 Identity Manager 使用者。策略可設定規則、密碼和使用者認證選項。

使用者類型

Identity Manager 提供兩種使用者類型：Identity Manager 使用者與服務提供者使用者 (若將 Identity Manager 系統配置爲可用於服務提供者實作)。這兩種類型可讓您根據使用者與公司之間的關係，區分出可能有不同佈建需求的使用者，例如區分企業外部網路使用者與企業內部網路使用者的不同需求。

服務提供者實作最常見的情況，是需要使用 Identity Manager 管理內部使用者與外部使用者 (客戶) 的服務提供者公司。如需有關配置服務提供者實作的資訊，請參閱「Identity Manager Service Provider Deployment」。

您需要在配置使用者帳號時指定 Identity Manager 使用者類型。如需有關服務提供者使用者的更多資訊，請參閱第 17 章「服務提供者管理」。

託管

若要成功地分配使用者身份管理的責任，您需要正確平衡靈活性與控制程度。透過授予選取 Identity Manager 使用者管理員特權並委託管理工作，您可將身份管理的責任交由最瞭解使用者需要的人員 (例如人力招募經理)，從而減少管理費用並提昇效率。擁有這些延伸權限的使用者稱爲 Identity Manager 管理員。

但是委派只有在安全模式中才可運作。爲了維持適當的控制層級，Identity Manager 可讓您將不同的權能層級指定給管理員。各種權能可向管理員授權系統中的不同存取權與行動層級。

Identity Manager 工作流程模型也包括一個用以確保某些操作必須經過核准的方法。使用工作流程，Identity Manager 管理員可保留對工作的控制權，並可追蹤其進度。如需有關工作流程的詳細資訊，請參閱「Identity Manager Workflows, Forms, and Views」。

Identity Manager 物件

Identity Manager 物件的明確描述以及物件如何互動對於成功的系統管理與部署非常重要。這些物件如下：

- 使用者帳號
- 角色
- 資源與資源群組
- 組織與虛擬組織
- 目錄結合
- 權能
- 管理員角色
- 策略
- 稽核策略

備註 命名 Identity Manager 物件時，請勿使用下列字元：

' (所有格符號)、. (點號)、| (管線符號)、[(左括號)、] (右括號)、, (逗號)、: (冒號)、$ (美元符號)、" (雙引號)、\ (反斜線) 或 = (等號)。

也應避免下列字元：_ (底線)、% (百分比符號)、^ (指數符號) 和 * (星號)。

使用者帳號

使用者是指擁有 Identity Manager 系統帳號的任何人。Identity Manager 爲每個使用者儲存一系列資料。這些資訊共同構成使用者的 Identity Manager 身份識別。

Identity Manager 使用者帳號：

- 提供使用者對一個或多個**資源**的存取權，並管理這些資源上的使用者帳號資料。
- 是指定的**角色**，可以設定使用者對各種資源的存取權。
- 爲**組織**的一部分，可以決定管理使用者帳號的方式和人員。

使用者帳號設定程序是動態的。根據您在帳號設定期間所進行的角色選擇，您可以提供較多或較少資源特定的資訊來建立帳號。與指定角色相關的資源的數目與類型決定了在帳號建立時需要資訊的多寡。

管理員是擁有額外權限的使用者，其可管理使用者帳號、資源以及其他 Identity Manager 系統物件與作業。Identity Manager 管理員負責管理組織，並被指定了適用於每個受管組織中之物件的一系列權能。

如需有關使用者帳號的更多資訊，請參閱第 63 頁第 3 章的 「使用者和帳號管理」。
如需有關管理員帳號的更多資訊，請參閱第 199 頁第 6 章的 「管理」。

角色

角色是 Identity Manager 物件，可將資源存取權限分組，並以效率極高的方式指定給使用者。角色分爲四種角色類型：

- 商務角色
- IT 角色
- 應用程式
- 資產。

商務角色可將組織中執行類似作業的人員執行其工作責任時所需的存取權限，進行分組。一般而言，商務角色代表使用者工作職能。

IT 角色、應用程式和資產則會將資源軟體權利文件 (或存取權限) 劃分爲不同群組。爲了提供使用者對資源的存取權，會將「IT 角色」、「應用程式」和「資產」指定給「商務角色」，讓使用者可以存取執行其工作時所需要的資源。

「IT 角色」、「應用程式」和「資產」可以是必要、條件式或選擇性項目。必要資源一律會指定給使用者。條件式資源的條件則必須計算爲 true，才會指定資源。選擇性資源可以個別請求，並在核准之後指定給使用者。

因爲資源可以是條件式或選擇性資源，所以具有相同一般工作說明的使用者可能擁有相同的「商務角色」，但仍然擁有不同的存取權限。此方式允許「商務角色」設計者定義資源的概略性存取權以遵守法規，同時仍然允許使用者管理員微調使用者存取權限的彈性。運用此方式，就不需要針對企業中的每組存取需求定義新的「商務角色」(此問題稱爲「角色擴張」)。

您可以將一個或多個角色指定給使用者，也可不指定任何角色。

如需有關角色的更多資訊，請參閱第 118 頁的「瞭解與管理角色」。

資源與資源群組

Identity Manager 會儲存如何連線至資源或系統的資訊。可透過 Identity Manager 存取的資源包括：

- 主機安全管理程式
- 資料庫
- 目錄服務 (例如 LDAP)
- 應用程式
- 作業系統
- ERP 系統 (例如 SAP™)

每個 Identity Manager 資源都會儲存下列種類的資訊：

- 資源參數
- Identity Manager 參數
- 帳號資訊 (包括帳號屬性與身份識別範本)

有兩種方式可將資源指定給使用者。您可以直接將資源指定給使用者 (這稱爲**個別**或**直接**指定)，或先將資源指定給角色，然後再將角色指定給使用者 (此爲**角色型**或**間接**指定)。

- 個別指定 - 將個別資源直接指定給使用者帳號。
- 角色型指定 - 將一個或多個資源指定給角色 (「應用程式」、「資產」或「IT 角色」)。然後再將「應用程式」、「資產」及 (或) 「IT 角色」指定給「商務角色」。最後，再將一個或多個「商務角色」指定給使用者帳號。

可以用與指定資源相同的方式將相關的 Identity Manager 物件 (資源群組) 指定給使用者帳號。資源群組可關聯個項資源，以便您可以特定的順序在資源上建立帳號。此外，它們可以簡化將多個資源指定給使用者帳號的程序。

如需有關資源群組的更多資訊，請參閱第 171 頁的「資源群組」。

組織與虛擬組織

組織是指用於啓用管理委派的 Identity Manager 容器。它們定義 Identity Manager 管理員所控制或管理的實體範圍。

組織也可代表與目錄型資源的直接連結。這些稱之爲「虛擬組織」。透過虛擬組織可直接管理資源資料，而無需將資訊載入 Identity Manager 儲存庫。透過藉由虛擬組織鏡像現有目錄結構與成員身份，Identity Manager 可消除重複且耗時的設定作業。

包含其他組織的組織爲父系組織。您可以建立平面結構的組織，或將組織排列成階層式結構。階層可以表示您用以管理使用者帳號的部門、地理區域或其他邏輯部門。

如需有關組織的更多資訊，請參閱第 207 頁的「瞭解 Identity Manager 組織」。

目錄結合

目錄結合是一組階層式的相關組織，對一個目錄資源中的一組實際階層式容器進行鏡像。**目錄資源**透過使用階層容器來使用階層名稱空間。目錄資源的範例有 LDAP 伺服器與 Windows Active Directory 資源。

目錄結合中的每個組織皆是**虛擬組織**。目錄結合中最頂層的虛擬組織是表示定義於資源中的基底環境的容器的鏡像。目錄結合中其餘的虛擬組織爲頂層虛擬組織的**直接**或**間接**子系組織，是所定義資源基底環境容器之子系目錄資源容器的鏡像。

您可以使用與組織相同的方式讓 Identity Manager 使用者成爲虛擬組織的成員或供其所用。

如需有關目錄結合的更多資訊，請參閱第 213 頁的「瞭解目錄結合與虛擬組織」。

權能

可爲每個使用者指定權能或權限群組，使其能夠透過 Identity Manager 執行管理動作。權能可允許管理使用者在系統中執行特定工作，並操作 Identity Manager 物件。

一般而言，您會根據特定的工作責任來指定權能，例如密碼重設或帳號核准。透過將權能與權限指定給個別的使用者，您可建立一個階層式的管理結構，從而提供目標存取權與特權而不會危及資料保護的安全。

Identity Manager 提供一組預設權能，可用於一般的管理功能。也可以建立與指定符合您特定需求的權能。

如需有關權能的更多資訊，請參閱第 215 頁的「瞭解與管理權能」。

管理員角色

Identity Manager 管理員角色可讓您爲管理使用者所管理的每個組織集，定義一組唯一的權能。會給管理員角色指定各種權能和所控制的組織，隨後可將該管理員角色指定給管理使用者。

權能與所控制的組織可以直接指定給管理員角色，它們也可以在管理使用者每次登入 Identity Manager 時，間接 (動態) 地指定。動態指定由 Identity Manager 規則控制。

如需有關管理員角色的更多資訊，請參閱第 218 頁的 「瞭解與管理管理員角色」。

策略

策略藉由爲帳號 ID、登入與密碼特性建立限制，以設定 Identity Manager 使用者的限制。*Identity System* 帳號策略可建立使用者、密碼和認證策略選項及限制。資源密碼和帳號 ID 策略設定長度規則、字元類型規則以及允許的文字和屬性值。字典策略可讓 Identity Auditor 根據文字資料庫來檢查密碼，以確保不會遭受簡單的字典攻擊。

如需有關策略的更多資訊，請參閱第 176 頁的 「什麼是策略？」。

稽核策略

與其他系統策略不同，稽核策略針對特定資源的使用者群組定義策略違規。稽核策略建立一個或多個規則，並根據這些規則來計算使用者的遵循性違規。這些規則需視資源所定義之一個或多個屬性而定。當系統掃描使用者時，會使用指定給該使用者的稽核策略所定義的條件來判定有無發生遵循性違規。

如需更多關於稽核策略的資訊，請參閱第 456 頁的 「關於稽核策略」。

物件關係

表 1-1 提供 Identity Manager 物件與其關係的快速參考。

表 1-1 Identity Manager 物件關係 (第 1 頁，共 2 頁)

Identity Manager 物件	它是什麼？	它適用於何處？
使用者帳號	在 Identity Manager 和一個或多個資源上的帳號。 可以從資源將使用者資料載入 Identity Manager。 擁有更多權限的特殊使用者類別，Identity Manager 管理員	角色 一般來說，每個使用者帳號都會指定一個或多個角色。 組織 使用者帳號被安排在某階層結構中，作為組織的一部份。Identity Manager 管理員同時還管理組織。 資源 可將個別資源指定給使用者帳號。 權能 會為管理員指定他們所管理之組織的權能。
角色	「商務角色」可將組織中執行類似作業的人員執行其工作責任時所需的存取權限，進行分組。「應用程式」和 「IT 角色」則會將資源分組，以透過「商務角色」將資源指定給使用者。角色型資源指定可簡化大型組織的資源管理。	資源與資源群組 將資源與資源群組指定至 「資產」、「應用程式」和「IT 角色」。 使用者帳號 將具有類似特性的使用者帳號指定至 「商務角色」。 「資產」、「應用程式」和 「IT 角色」將 「資產」、「應用程式」和「IT 角色」指定給 「商務角色」。
資源	儲存有在其中管理帳號的系統、應用程式或其他資源的資訊。	角色 將資源指定給 「應用程式」和「IT 角色」，然後再將 「應用程式」和 「IT 角色」指定給 「商務角色」。透過所指定的 「商務角色」，使用者帳號可概略 「繼承」資源存取權。 使用者帳號 可以將資源個別地指定給使用者帳號。

表 1-1 Identity Manager 物件關係 (第 2 頁，共 2 頁)

Identity Manager 物件	它是什麼？	它適用於何處？
資源群組	經過排序的資源群組。	角色 將資源群組指定給角色；透過所指定的 「商務角色」，使用者帳號可 「繼承」資源存取權。 使用者帳號 資源群組可以直接指定給使用者帳號。
組織	定義管理員所管理實體的範圍；具有階層性。	資源 組織中的管理員擁有某些或所有資源的存取權。 管理員 組織是由擁有管理特權的使用者所管理 (控制)。管理員能夠管理一個或多個組織。指定組織中的管理特權可延伸至其子組織。 使用者帳號 可將每個使用者帳號指定給一個 Identity Manager 組織，以及一個或多個目錄組織。
目錄結合	是一組階層式的相關組織，對目錄資源中的一組實際階層式容器進行鏡像。	組織 目錄結合中的每個組織都是虛擬組織。
管理員角色	為指定給管理員的每組組織定義一組唯一的權能。	管理員 管理員角色指定給管理員。 權能與組織 權能與組織會以直接或間接 (動態) 方式指定給管理員角色。
權能	定義一組系統權限。	管理員 權能會指定給管理員。
策略	設定密碼和驗證限制。	使用者帳號 策略會指定給使用者帳號。 組織 策略會指定給組織或由組織繼承。
稽核策略	設定用來計算使用者的遵循性違規的規則。	使用者帳號 稽核策略會指定給使用者帳號。 組織 稽核策略會指定給組織。

第 2 章

Identity Manager UI 入門

閱讀本章可瞭解 Identity Manager 圖形化介面，以及如何快速開始使用 Identity Manager。

涵蓋的主題包括：

Identity Manager 管理員介面

Identity Manager 系統包括兩個主要的圖形化介面，使用者可透過這些介面執行作業：**一般使用者介面**與**管理員介面**。一般使用者介面 (又稱爲使用者介面) 會於本章稍後討論 (第 54 頁)。此處將討論管理員介面。

Identity Manager 管理員介面可以作爲本產品的主要管理檢視。透過此介面，Identity Manager 管理員可以管理使用者、設定與指定資源、定義權限與存取等級，以及稽核 Identity Manager 系統中的規範遵循。

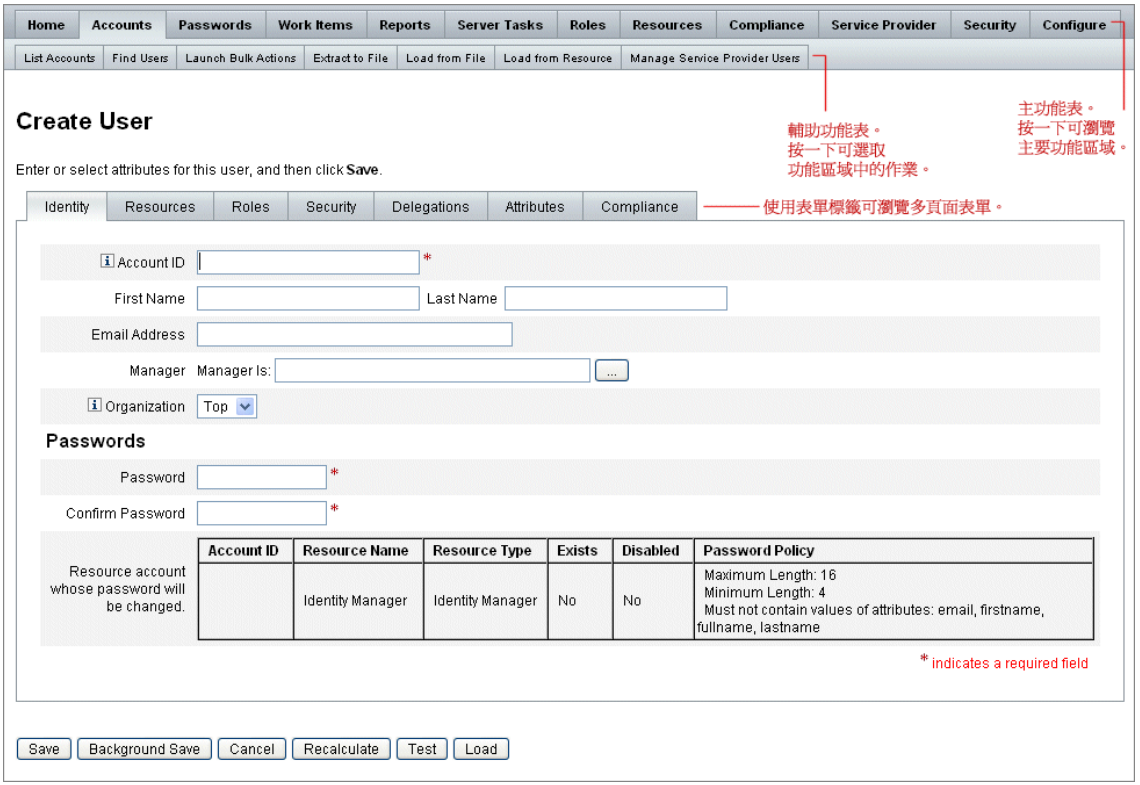
介面由以下元素組成：

- **瀏覽位址列標籤** - 這些標籤位於每個介面頁面的頂部，可讓您瀏覽主要功能區域。
- **子標籤或功能表** - 根據特定實作而定，您可能會在每個瀏覽位址列標籤下看到輔助標籤或功能表。這些子標籤或功能表選項可讓您存取功能區域中的作業。

在某些區域 (例如 [帳號]) 中，標籤式表單將較長的表單分成一頁或多頁，以使您可以更輕鬆地瀏覽這些表單。如圖 2-1 中所示。

備註 附錄 C「使用者介面快速參照」(第 613 頁) 提供在 UI 中執行管理工作的快速參照。

圖 2-1 Identity Manager 管理員介面



登入 Identity Manager 管理員介面

若要開啓管理員介面，請執行以下步驟：

1. 開啓 Web 瀏覽器，並在位址列鍵入下列 URL：

   `http://<AppServerHost>:<Port>/idm/login.jsp`

2. 輸入使用者 ID 與密碼，然後按一下 **[登入]**。

   若已對使用者 ID 指定權能及所控制的組織，管理員介面會隨即開啓。

階段作業限制與 Cookie

若在管理員的 Web 瀏覽器中啓用 Cookie，則在配置的階段作業限制所分配之時間內，管理員會在管理員介面中維持登入狀態。若瀏覽器停用了 Cookie，則某些特定動作會導致系統於階段作業期間提示管理員重新登入。這些動作如下：

- 取消重新命名管理員、角色與組織
- 取消刪除組織
- 建立使用者登入模組與管理員登入模組

若要避免出現多次登入請求，應啓用 Cookie。

忘記使用者 ID

Identity Manager 可讓管理員擷取忘記的使用者 ID。當管理員按一下登入頁面的 **[忘記使用者 ID？]** 時，即會出現查找頁面，並要求提供與帳號相關的身份識別屬性資訊，例如姓名、電子郵件地址或電話號碼。

接著，Identity Manager 會建構查詢，以尋找與所輸入的值相符的單一使用者。若找不到相符項，或找到多個相符項，則 [查找使用者 ID] 頁面上會出現錯誤訊息。

依預設，查找功能是啓用的。但您可以透過下列其中一個動作停用此功能：

- 將 login.jsp 中的 `forgotUserIdMode` 值設爲 false
- 編輯系統配置物件，並將 `admin` 屬性及 (或) `user` 屬性的 `disableForgotUserId` 屬性值，設定爲 True

  如需有關編輯系統配置物件的說明，請參閱第 197 頁。

備註

若從 Identity Manager 的舊版升級至 8.0 版時，預設會停用 [忘記使用者 ID？] 功能。

若要啓用此功能，必須修改系統配置物件中的下列屬性 (第 197 頁)：

```
ui.web.user.disableForgotUserId = false
ui.web.admin.disableForgotUserId = false
```

所顯示的使用者屬性名稱集，會透過系統配置屬性 `security.authn.lookupUserIdAttributes.<Administrator Interface | User Interface>` 進行配置。在 [IDM 模式配置] 配置物件中定義爲可查詢的屬性，即爲可指定的屬性。

找回使用者 ID 後，Identity Manager 會使用 [使用者 ID 回復] 電子郵件範本，傳送電子郵件至 ID 已找到的使用者之電子郵件地址。

Identity Manager 一般使用者介面

Identity Manager 一般使用者介面 (又稱爲「Identity Manager 使用者介面」) 只會顯示 Identity Manager 系統的一部分檢視。此檢視專爲不具備管理權能的使用者而設計。

備註 如需有關如何登入一般使用者介面的說明，請參閱第 56 頁的「登入 Identity Manager 一般使用者介面」。

使用者可以從使用者介面執行各種作業，例如變更密碼、執行自我佈建作業以及管理工作項目和委派。

Identity Manager 可配置成使用者按一下一般使用者介面登入頁面上的連結，即可申請帳號。如需詳細資訊，請參閱第 113 頁的「匿名註冊」。

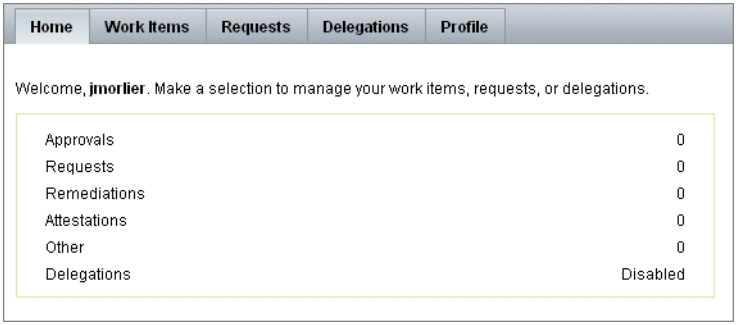
五個一般使用者介面標籤

一般使用者介面分爲五個區段 (或標籤)：**[首頁]**、**[工作項目]**、**[請求]**、**[委派]** 以及 **[設定檔]**。

首頁

當使用者登入 Identity Manager 使用者介面時，該使用者的所有擱置工作項目和委派，都會顯示在 **[首頁]** 標籤中，如下圖所示：

圖 2-2 使用者介面 ([首頁] 標籤)



[首頁] 標籤讓使用者能快速存取任何擱置項目。使用者可按一下清單中的項目，以回應工作項目請求或執行其他可用動作。

工作項目

[工作項目] 標籤可進一步分爲 **[核准]**、**[驗證作業]**、**[修正]** 以及 **[其他]** 標籤。在此使用者介面區域中，使用者可核准或拒絕其本身擁有或有權對其執行動作的所有擱置工作項目。

請求

[請求] 標籤中含有兩個子標籤：**[啓動請求]** 和 **[檢視]**。

在 **[啓動請求]** 標籤中，使用者有兩個選項：**[更新我的角色]** 和 **[更新我的資源]**。

- 在 [更新我的角色] 頁面上，使用者可從適合使用者的可用角色清單中加以請求。當一般使用者提交角色請求時，會產生工作項目，並將核准通知傳送至該角色的指定核准人。一般使用者也可請求移除或取消指定自己的一個或多個角色。

  請參閱「角色與資源」，以瞭解如何建立可讓一般使用者申請其存取權的選擇性角色。

- 在 [更新我的資源] 頁面上，使用者可從適合使用者的個別資源清單中加以請求。與角色請求相同，資源請求所產生的工作項目需要核准才可處理。

[檢視] 子標籤會顯示使用者所提交之請求的狀態詳細資訊。使用者可從此區域檢視其所提交之請求的處理狀態與作業結果。

委派

使用者可從 **[委派]** 標籤，將工作項目委託給其他 Identity Manager 使用者。例如，身爲一個或多個角色指定核准人的使用者，可委託使用者未來於休假期間將核准工作項目傳送給同事一段時間。使用者可使用 [委派] 頁面建立及管理委派，而不需要管理員的協助。

設定檔

一般使用者可從 **[設定檔]** 標籤管理其 Identity Manger 密碼與帳號屬性設定。此標籤分爲以下四個子標籤：

- **變更密碼** - 一般使用者可在所選資源或所有資源上變更其密碼。
- **帳號屬性** - 一般使用者可變更特定屬性，例如 Identity Manager 傳送帳號通知的帳號電子郵件地址。
- **認證問題** - 用於管理使用者帳號的認證問題及答案。
- **存取權限** - 列出使用者目前指定的角色及資源指定。

登入 Identity Manager 一般使用者介面

若要開啓一般使用者介面，請執行以下步驟：

1. 開啓 Web 瀏覽器，並在位址列鍵入下列 URL：

   ```
   http://<AppServerHost>:<Port>/idm/user/login.jsp
   ```

2. 輸入使用者 ID 與密碼，然後按一下 **[登入]**。

   一般使用者介面會隨即開啓

忘記使用者 ID

Identity Manager 可讓一般使用者擷取忘記的使用者 ID。如需更多資訊，請參閱登入 Identity Manager 管理員介面一節中的第 53 頁的「忘記使用者 ID」。

說明與指導

爲了能夠順利地完成某些作業，您可能需要查詢 [說明] 以及 Identity Manager 指導 (欄位層級資訊與說明)。您可以從 Identity Manager 管理員與使用者介面取得說明與指導。

Identity Manager Help

如需與作業相關的說明和資訊，請按一下 **[說明]** 按鈕，該按鈕位於每個管理員介面頁面和使用者介面頁面的頂部，如圖 2-3 所示。

圖 2-3　[說明] 按鈕，位於 Identity Manager interface

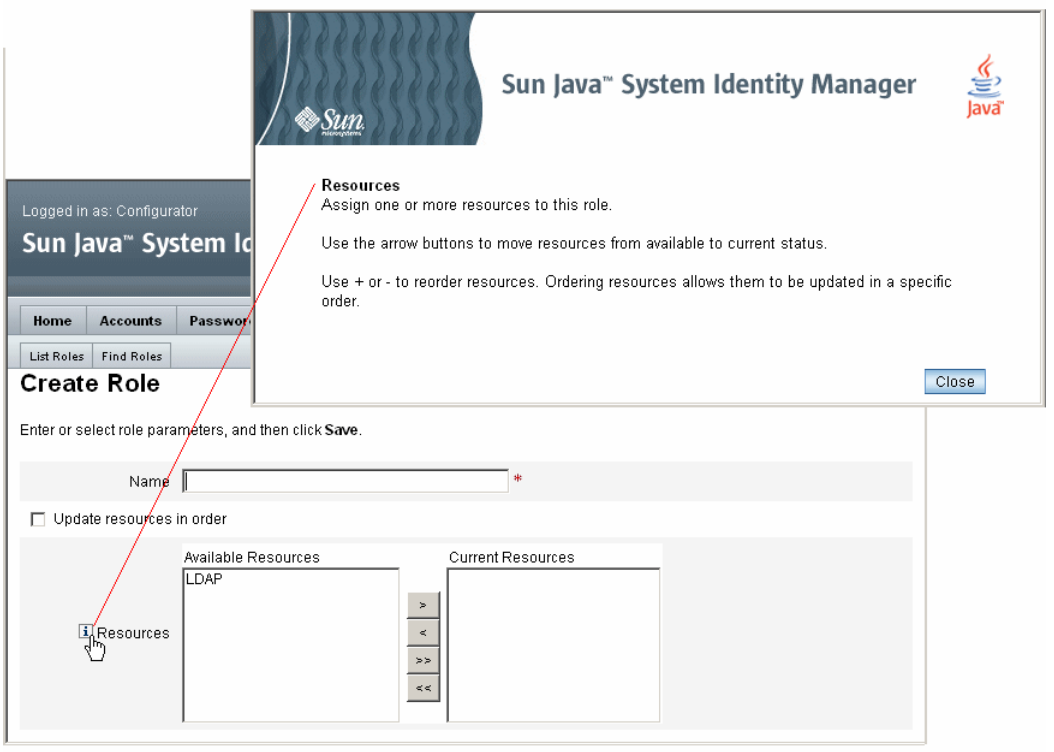
在每個 [說明] 視窗的底部爲 [內容] 連結，它可引導您至其他的 [說明] 主題以及 Identity Manager 術語字彙表。

Identity Manager 指導

Identity Manager 指導爲簡要的有目標性說明，出現在許多頁面欄位的旁邊。它的用途是當您在頁面上移動以執行工作時，可以協助您輸入資訊或進行選擇。

附有指導說明的欄位旁會顯示以字母「i」標記的符號。按一下此符號可開啓一個視窗，其中會顯示相關資訊。

圖 2-4 Identity Manager 指導



Identity Manager 除錯頁面

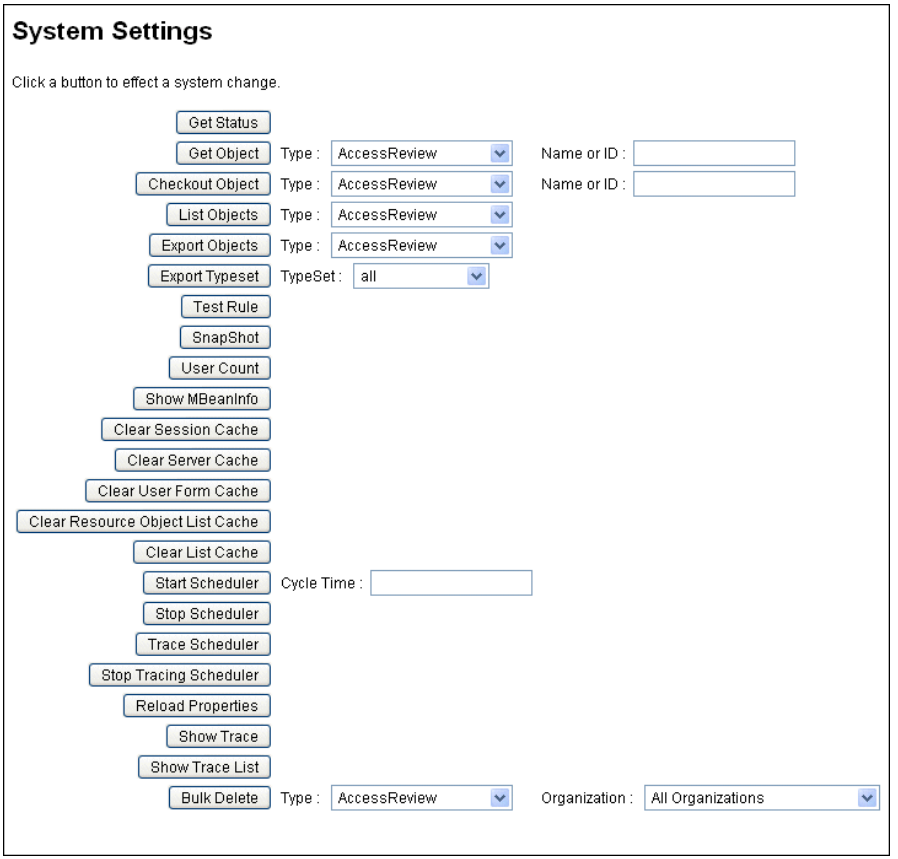
管理員介面包含有助於最佳化 Identity Manager 或疑難排解問題所需的頁面。若要存取這些頁面，請開啓 Identity Manager 的 [除錯] 頁面，又稱爲 [系統設定] 頁面。

若要開啓 Identity Manager 的 [除錯] 頁面，請在瀏覽器中鍵入以下 URL (根據您的平台與配置之不同，URL 可能會區分大小寫)。

```
http://<AppServerHost>:<Port>/idm/debug/session.jsp
```

使用者必須具有「除錯」權能才可檢視 `/idm/debug/` 頁面。如需有關權能的資訊，請參閱第 217 頁的「指定權能」。

圖 2-5　Identity Manager 除錯頁面 (系統設定)



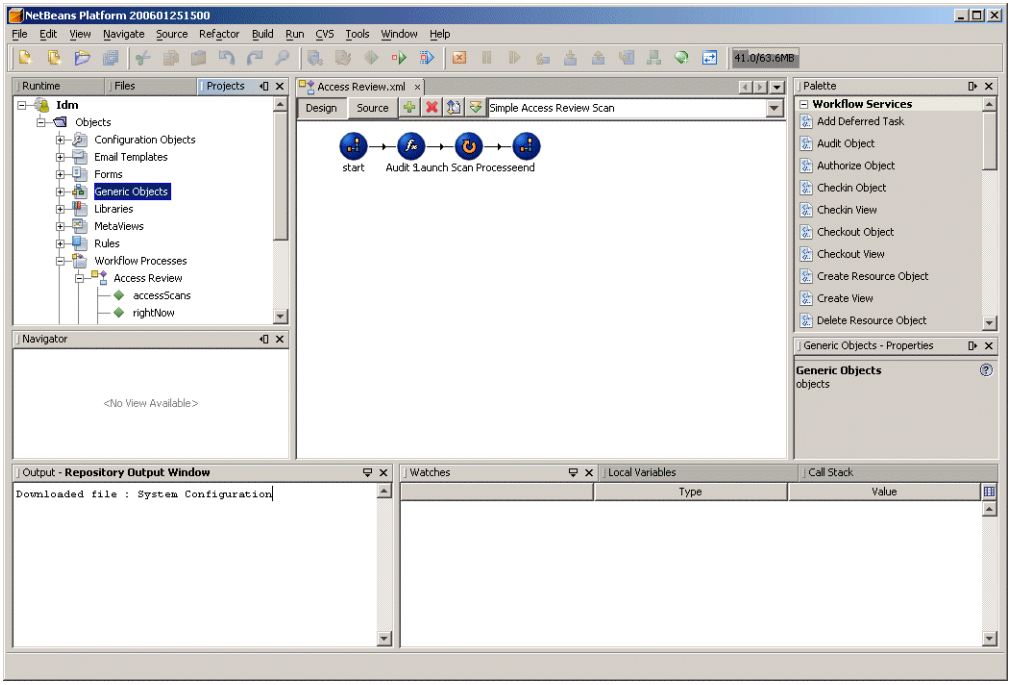
如需有關 Identity Manager 疑難排解的資訊，請參閱「Identity Manager Tuning, Troubleshooting, and Error Messages」。

Identity Manager IDE

Identity Manager 整合開發環境 (IDE) 提供了 Identity Manager 表單、規則與工作流程的圖形檢視。這是完全整合的 NetBeans 外掛程式，在 Identity Manager 發行套裝軟體中隨 Identity Manager 發行。

您可以使用 IDE 建立與編輯一些表單，這些表單可以建立可用於每個 Identity Manager 頁面的功能。您也可以修改 Identity Manager 工作流程，工作流程可定義使用 Identity Manager 使用者帳號時所遵循的動作順序或執行的作業。另外，您可以修改在 Identity Manager 中定義以用於確定工作流程運作方式的規則。

圖 2-6　Identity Manager IDE 介面



若要下載 Identity Manager IDE，請造訪此網站：

https://identitymanageride.dev.java.net/

如果您已安裝舊版 Identity Manager 所提供的業務程序編輯器 (BPE)，則也可以使用業務程序編輯器進行自訂。

下面要查看哪一個章節

熟悉 Identity Manager 介面和尋找資訊的方法之後，使用以下參照可引導您至想要重點瞭解的主題：

章節主題	描述
第 3 章「使用者和帳號管理」	說明介面的 [帳號] 區域，並提供管理使用者帳號的程序。
第 4 章「角色與資源」	說明如何使用 Identity Manager 角色與資源。
第 5 章「配置與系統維護」	說明配置作業以及如何設定 Identity Manager 物件。
第 6 章「管理」	說明如何建立與管理 Identity Manager 管理員和組織。
第 7 章「資料載入和同步化」	針對您可用於維護 Identity Manager 中目前資料的功能和工具，爲您提供指南。
第 8 章「報告」	說明報告以及如何產生報告。
第 9 章「作業範本」	說明可用於配置特定工作流程運作方式的作業範本。
第 10 章「稽核記錄」	說明稽核記錄以及稽核系統如何工作。
第 11 章「PasswordSync」	說明如何設定 PasswordSync 公用程式，以使 Windows Active Directory 網域中的密碼變更與 Identity Manager 中的變更同步。
第 12 章「安全性」	說明安全性功能以及如何使用這些功能。
第 13 章「身份識別稽核：基本概念」	說明基本稽核概念。
第 14 章「稽核：稽核策略」	說明如何建立稽核策略。
第 15 章「稽核：監視規範遵循」	說明如何執行稽核檢閱以及進行實作，協助您管理以遵循聯邦法規規範
第 16 章「資料匯出程式」	資料匯出程式功能可讓您將有關使用者、角色及其他物件類型的資訊寫入外部資料倉儲。
第 17 章「服務提供者管理」	說明用於管理服務提供者使用者的功能。
附錄 A「lh 參照」	說明 Identity Manager 指令行中的指令。
附錄 B「稽核記錄資料庫模式」	受支援資料庫類型的稽核資料模式值以及稽核記錄資料庫對映

章節主題	描述
附錄 C「使用者介面快速參照」	在 UI 中執行管理工作的快速參照。內容說明開始每項工作的主要位置，以及可用於執行相同工作的替代位置或方法 (如果適用)。
附錄 D「權能定義」	Identity Manager 的預設作業型和功能性權能清單 (含定義)。本附錄也會列出可利用各作業型權能存取的標籤及子標籤。

第 3 章

使用者和帳號管理

本章提供透過 Identity Manager 管理員介面建立及管理使用者的資訊與程序。此資訊分爲以下小節：

介面的 [帳號] 區域

使用者是指擁有 Identity Manager 系統帳號的任何人。Identity Manager 爲每個使用者儲存一系列資料。這些資訊共同構成使用者的 Identity Manager 身份識別。

Identity Manager 的 [帳號/使用者清單] 頁面可讓您管理 Identity Manager 使用者。若要存取此區域，請按一下 [管理員介面] 功能表列上的 **[帳號]**。

帳號清單會顯示所有的 Identity Manager 使用者帳號。帳號會分組爲組織與虛擬組織，在資料夾中以階層方式表示。

您可以按全名 ([名稱])、使用者姓氏 ([姓氏]) 或使用者名字 ([名字]) 對帳號清單進行排序。按一下標題列可以按照欄排序。按一下相同標題列可以在向上與向下排序順序之間切換。如果按全名 ([名稱] 欄) 排序，則階層中處於所有級別的所有項目都將按字母順序排序。

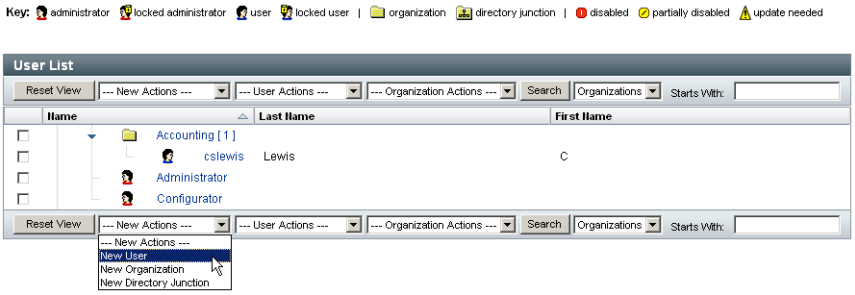
若要展開階層式檢視並察看組織中的帳號，請按一下資料夾旁邊的三角形指示器。再按一下該指示符，便會摺疊檢視。

帳號區域中的動作清單

使用動作清單 (位於 [帳號] 區域的頂部和底部，如圖 3-1 所示) 可以執行一系列動作。動作清單選項分爲：

- **新動作** - 建立使用者、組織和目錄結合。
- **使用者動作** - 編輯、檢視和變更使用者狀態；變更和重設密碼；刪除、啓用、停用、解除鎖定、移動、更新和重新命名使用者；以及執行使用者稽核報告。
- **組織動作** - 執行一系列組織和使用者動作。

圖 3-1　　帳號清單



在 [帳號清單] 區域中搜尋

使用帳號區域搜尋功能查找使用者和組織。從清單中選取 [組織] 或 [使用者]，在搜尋區域中輸入使用者或組織名稱開頭的一個或多個字元，然後按一下 **[搜尋]**。如需有關在 [帳號] 區域搜尋的更多資訊，請參閱第 76 頁的「尋找及檢視使用者帳號」。

使用者帳號狀態

顯示在每個使用者帳號旁的圖示可指示已指定帳號的目前狀態。表 3-1 說明了每個圖示的涵義。

表 3-1 使用者帳號狀態圖示說明

指示器	狀態
	使用者的 Identity Manager 帳號已鎖定。請注意，此圖示僅會反映 Identity Manager 帳號的鎖定狀態，而不會反映所有的使用者資源帳號。 超過 Identity Manager 帳號策略所定義之 Identity Manager 帳號登入嘗試失敗次數上限時，即會鎖定使用者。只有 Identity Manager 帳號發生密碼或問題登入失敗時，才會計入允許的上限。因此，若 Identity Manager 登入應用程式 (亦即管理員介面、一般使用者介面等) 的登入模組群組中不包含 Identity Manager 登入模組，則不會考慮 Identity Manager 失敗的密碼策略。但不論指定的 Identity Manager 登入應用程式所配置的登入模組堆疊為何，超過 Identity Manager 帳號策略配置上限的失敗問題登入，都可能會造成使用者鎖定，並顯示此圖示。 如需有關如何解除鎖定帳號的資訊，請參閱第 94 頁的 「解除鎖定使用者帳號」。
	管理員的 Identity Manager 帳號已鎖定。請注意，此圖示只會反映 Identity Manager 帳號的鎖定狀態，而不會反映所有的管理員資源帳號。如需更多資訊，請參閱上文中的使用者鎖定圖示說明。
	在所有已指定資源和 Identity Manager 中停用此帳號 (啟用帳號時，不出現圖示)。 如需有關如何啟用已停用帳號的資訊，請參閱第 93 頁的 「啟用使用者帳號」。
	帳號已部分停用，表示在一個或多個已指定資源上停用。
	系統嘗試在一個或多個資源上建立或更新 Identity Manager 使用者帳號，但失敗 (更新所有指定資源的帳號時，不出現圖示)。

備註 在 [管理員] 欄中，若 Identity Manager 找不到符合所列名稱的 Identity Manager 帳號，則管理員的使用者名稱即會顯示在括號中。

使用者頁面 (建立/編輯/檢視)

本節說明管理員介面中所提供的 [建立使用者]、[編輯使用者] 及 [檢視使用者] 等頁面。本章後文會說明如何使用這些頁面。

備註 本文件將說明 Identity Manager 所附之 [建立使用者]、[編輯使用者] 及 [檢視使用者] 等頁面的預設設定。但若要更佳反映您的業務程序或特定管理員權能，則應針對環境建立自訂的使用者表單。如需有關自訂使用者表單的更多資訊，請參閱「Identity Manager Workflows, Forms, and Views」。

預設 Identity Manager 使用者頁面分爲下列標籤或區段：

- 身份識別
- 指定
- 安全性
- 委派
- 屬性
- 規範遵循

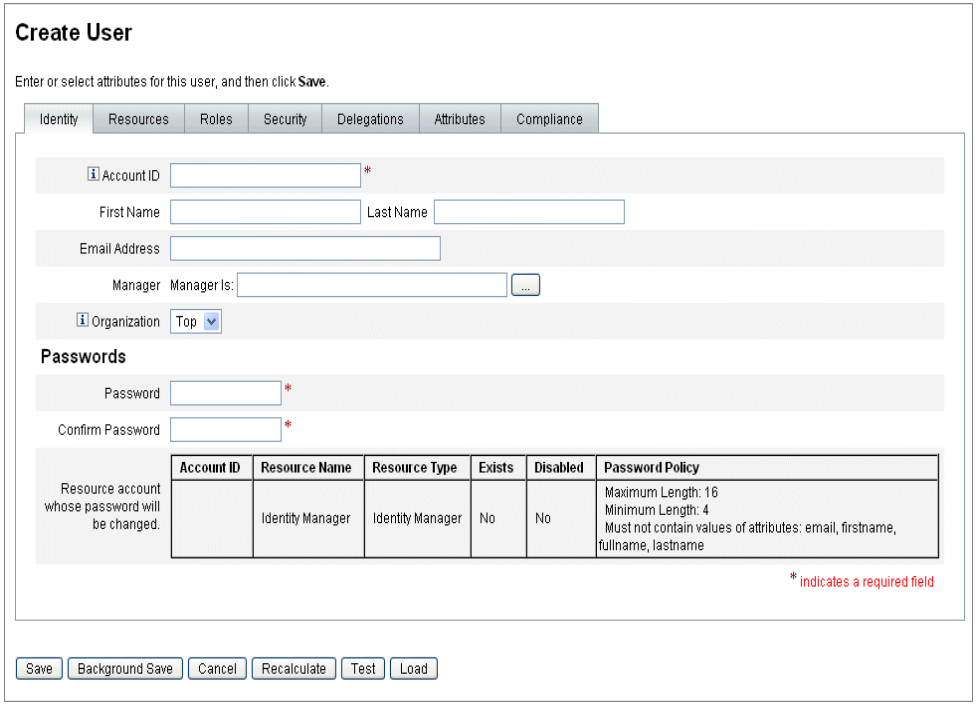
身份識別

[身份識別] 區域可定義使用者的帳號 ID、名稱、連絡人資訊、管理員、管理組織及 Identity Manager 帳號密碼。它還識別使用者可以存取的資源以及管理每個資源帳號的密碼策略。

備註 如需有關設定帳號密碼策略的資訊，請閱讀本章中標題爲「第 104 頁的「管理帳號安全性和權限」」的小節。

下圖說明 [建立使用者] 頁面的 [身份識別] 區域。

圖 3-2 建立使用者 - 身份



資源

[資源] 區域可直接將資源及資源群組指定給使用者。亦可指定資源排除。

直接指定的資源，可補充透過角色指定而間接指定給使用者的資源。

- **角色**指定 - 概括一類使用者。角色可透過間接指定的方式，定義使用者對資源的存取權。

角色

[角色] 標籤可用以將一個或多個角色指定給使用者，並管理這些角色指定。

如需有關此標籤的資訊，請參閱第 145 頁的 「指定角色給使用者」。

安全性

在 Identity Manager 術語中，爲其指定了擴充權能的使用者爲 Identity Manager 管理員。使用 [安全性] 標籤可將管理員權限指定給使用者。

如需有關使用 [安全性] 標籤建立管理員的更多資訊，請參閱第 201 頁的 「建立管理員」。

[安全性] 表單由下列區段所組成。

- **管理員角色** - 將一個或多個管理角色指定給使用者。角色是權能及受控制組織的特定配對，方便以協調的方式將管理權責指定給使用者。
- **權能** - 啓用在 Identity Manager 系統中具有的權限。通常會根據工作責任，爲每個 Identity Manager 管理員指定一項或多項權能。

  第 215 頁有針對權能加以討論。附錄 D 「權能定義」會提供依作業性質區分的權能清單及定義 (第 619 頁)。本附錄也會列出可利用各權能存取的標籤及子標籤。
- **所控制的組織** - 指定該使用者有權以管理員身份管理的組織。他可以管理已指定組織及階層中處於該組織之下的任何組織中的物件。

備註 若要讓使用者擁有管理員權能，必須爲其至少指定一個管理員角色或一項或多項權能，以及一個或多個所控制的組織。如需有關 Identity Manager 管理員的更多資訊，請參閱第 200 頁的 「瞭解 Identity Manager 管理」。

- **使用者表單** - 指定管理員在建立和編輯使用者時將使用的使用者表單。如果選取 **[無]**，則管理員將繼承指定給其組織的使用者表單。
- **檢視使用者表單** - 指定管理員在檢視使用者時將使用的使用者表單。如果選取 **[無]**，則管理員將繼承指定給其組織的檢視使用者表單。
- **帳號策略** – 建立密碼及認證限制。

委派

[建立使用者] 頁面上的 [委派] 標籤，可讓您將工作項目委託給其他使用者，讓其代爲執行一段指定的時間。如需有關委託工作項目的更多資訊，請閱讀第 230 頁的「委託工作項目」。

屬性

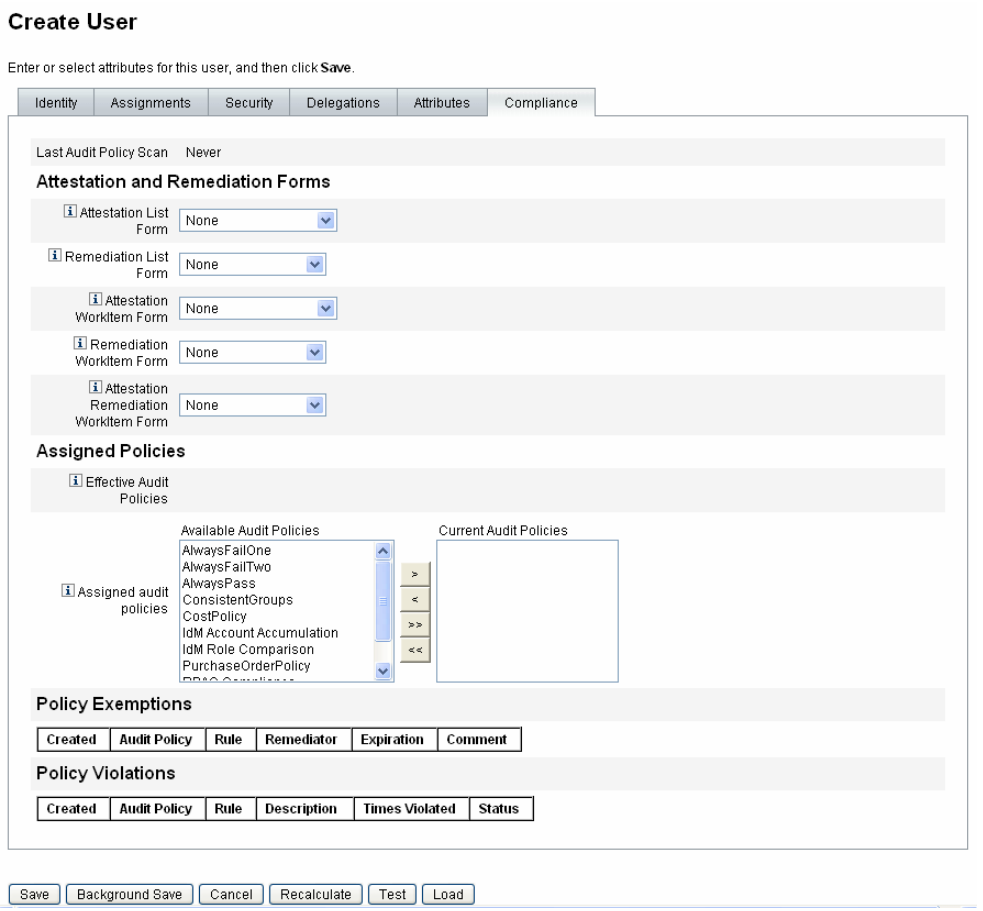
[建立使用者] 頁面上的 [屬性] 標籤定義與指定資源關聯的帳號屬性。列出的屬性按指定的資源分類，具體情況根據已指定資源的不同而異。

規範遵循

[規範遵循] 標籤：

- 可讓您選取使用者帳號的驗證作業與修正表單。
- 指定使用者帳號的指定稽核策略，包括透過使用者的組織指定而生效的稽核策略。您只能透過編輯使用者的目前組織或將使用者移至其他組織，來變更這些策略指定。
- 指示策略掃描、違規和免責的目前狀態，如下圖所示 (如果適用於使用者帳號)。資訊中包含上一次爲所選使用者進行稽核策略掃描的日期與時間。

圖 3-3 [建立使用者] 頁面 - [規範遵循] 標籤



若要指定稽核策略，請將選取的策略從 **[可用的稽核策略]** 清單移至 **[目前的稽核策略]** 清單中。

備註 您也可以在 **[使用者動作]** 清單中選取 **[檢視規範遵循狀態]**，以存取 [規範遵循] 標籤上的資訊。若要檢視針對某使用者在特定時段內所記錄的規範遵循違規，請從 **[使用者動作]** 清單中選取 **[檢視規範遵循違規記錄]**，然後指定要檢視的項目範圍。

建立使用者及使用使用者帳號

在管理員介面的 [帳號/使用者清單] 頁面，可以對以下系統物件執行一系列動作：

- **管理員及使用者** - 檢視、建立、編輯、移動、重新命名、取消佈建、啓用、停用、更新、解除鎖定、刪除、取消指定、取消連結與稽核。

  如需有關建立及編輯管理員帳號的更多資訊，請參閱第 200 頁的「瞭解 Identity Manager 管理」。

- **組織** - 針對組織成員建立、編輯、重新整理和執行使用者動作。

  如需有關組織的更多資訊，請參閱第 207 頁的「瞭解 Identity Manager 組織」。

- **目錄結合** - 建立。

  如需有關目錄結合的更多資訊，請參閱第 213 頁的「瞭解目錄結合與虛擬組織」。

啟用進程圖

進程圖係描述建立使用者帳號或對其執行其他動作時，Identity Manager 所遵循之工作流程。啓用後，Identity Manager 完成作業時所建立的結果頁或作業摘要頁面中，即會顯示進程圖。

在 Identity Manager 8.0 版中，新安裝與升級安裝皆會停用進程圖。

若要啓用進程圖於 Identity Manager 中使用，請執行以下步驟：

1. 依第 197 頁中的程序開啓系統配置物件進行編輯。
2. 找到下列 XML 元素：

   ```
   <Attribute name='disableProcessDiagrams'>
     <Boolean>true</Boolean>
   </Attribute>
   ```

3. 將 `true` 值變更爲 `false`。
4. 按一下 **[儲存]**。
5. 重新啓動伺服器，讓變更生效。

您也可以在一般使用者介面中啓用進程圖，但必須先在管理員介面中使用前文描述的步驟啓用進程圖。如需詳細資訊，請參閱第 192 頁的「啓用一般使用者介面中的進程圖」。

建立使用者

若要在 Identity Manager 中建立使用者，請執行以下步驟：

1. 在管理員介面中，按一下 **[帳號]**。
2. 若要建立特定組織的使用者，請選取該組織，再從 **[新動作]** 清單中選取 **[新使用者]**。

   否則，請從 **[新動作]** 清單中選取 **[新使用者]**，建立頂層組織的使用者帳號。
3. 在下列標籤或區段中填入資訊。
   - **身份識別** - 名稱、組織、密碼及其他詳細資訊 (請參閱第 68 頁)。
   - **資源** - 個別資源及資源群組指定，以及資源排除 (請參閱第 69 頁)。
   - **角色** - 角色指定。如需有關角色的資訊，請參閱第 118 頁的「瞭解與管理角色」。如需有關完成 [角色] 標籤的說明，請參閱第 145 頁的「指定角色給使用者」。
   - **安全性** - 管理員角色、所控制的組織和權能。以及使用者表單設定及帳號策略 (請參閱第 69 頁)。
   - **委派** - 工作項目委派 (請參閱第 70 頁)。
   - **屬性** - 指定資源的特定屬性 (請參閱第 70 頁)。
   - **規範遵循** - 選取使用者帳號的驗證作業與修正表單。規範遵循區域也可讓您指定使用者帳號的已指定稽核策略，包括透過使用者的組織指定而生效的稽核策略。指出策略掃描、違規及豁免的目前狀態，包括使用者最近稽核策略掃描的相關資訊。(請參閱第 70 頁)。

   請注意，某區域中可選擇之選項可能取決於您在其他區域中所做的選擇。

備註 若要更佳反映您的業務程序或特定管理員權能，應針對環境自訂使用者表單。如需有關自訂使用者表單的更多資訊，請參閱 「Identity Manager Workflows, Forms, and Views」。

---

4. 完成選取後，您可以使用兩個選項來儲存使用者帳號：

   - **儲存** - 儲存使用者帳號。如果您給帳號指定了大量資源，則此過程可能會花費一些時間。
   - **背景儲存** - 此程序以背景作業的方式儲存使用者帳號，以便讓您繼續使用 Identity Manager。對於每個執行中的儲存工作，[帳號] 頁面、[尋找使用者結果] 頁面以及首頁上將顯示工作狀態指示器。

   狀態指示器 (如下表所述) 可協助您監視儲存程序的進度。

表 3-2 背景儲存作業狀態指示器的說明

狀態指示器	狀態
	**儲存程序正在執行。**
	**儲存程序已暫停。通常，這表示程序正在等待核准。**
	**程序已順利完成。這並不表示使用者已成功儲存；只表示程序在無錯情況下完成。**
?	**程序尚未啟動。**
	**程序已完成，但發生一個或多個錯誤。**

將滑鼠移動到狀態指示器內部所顯示的使用者圖示上，就可以看到背景儲存程序的詳細資訊。

備註 如果已對生效進行配置，則建立使用者時，也會建立可在 [核准] 標籤中檢視的工作項目。**核准**此項目會置換生效日期並建立帳號。**拒絕**此項目會取消建立帳號。如需有關對生效進行配置的更多資訊，請參閱第 332 頁的「配置 [生效和失效] 標籤」。

為使用者建立多個資源帳號

Identity Manager 可讓您將多個資源帳號指定給單一使用者。方法是允許爲每個資源定義多個資源帳號類型或帳號類型。資源帳號類型應視需要建立，以符合資源上每項有作用的帳號類型 - 例如，*AIX SuperUser* 或 *AIX BusinessAdmin*。

為何要為每項資源的每位使用者指定多個帳號？

在某些情況下，Identity Manager 使用者在某項資源上會需要多個帳號。使用者可有與資源相關的數種不同工作職能 - 例如，使用者可同時爲某項資源的使用者及管理員。最佳實作方法建議您每項職能要使用不同的帳號。如此一來，即使有某個帳號洩漏出去，其他帳號所授權的存取權限仍然安全。

配置帳號類型

資源若要支援單一使用者使用多個帳號，必須先在 Identity Manager 中定義資源帳號類型。請使用「資源精靈」定義資源的資源帳號類型。相關資訊請參閱第 167 頁的 **「帳號類型」**。

您必須先啓用並配置資源帳號類型，再將其指定給使用者。

指定帳號類型

一旦定義帳號類型後，即可將其指定給資源。Identity Manager 會將每個指定的帳號類型視爲不同的帳號。於是，角色中每個不同的指定就會有不同的屬性集。

與每個資源單一帳號的情況相似，不論有多少個指定，所有特定類型的指定都僅會建立一個帳號。

雖然您可將使用者指定給資源上無限數量的不同帳號類型，但每位使用者只能獲得資源上指定類型的一個帳號。內建的「預設」類型是此規則的例外。使用者可有資源之預設類型的無限數量帳號。但我們不建議您如此做，因爲如此會在以表單及檢視模式參照帳號時，造成模糊不明的狀況。

尋找及檢視使用者帳號

Identity Manager 尋找功能可讓您搜尋使用者帳號。輸入和選取搜尋參數後，Identity Manager 將尋找與您的選項相符的所有帳號。

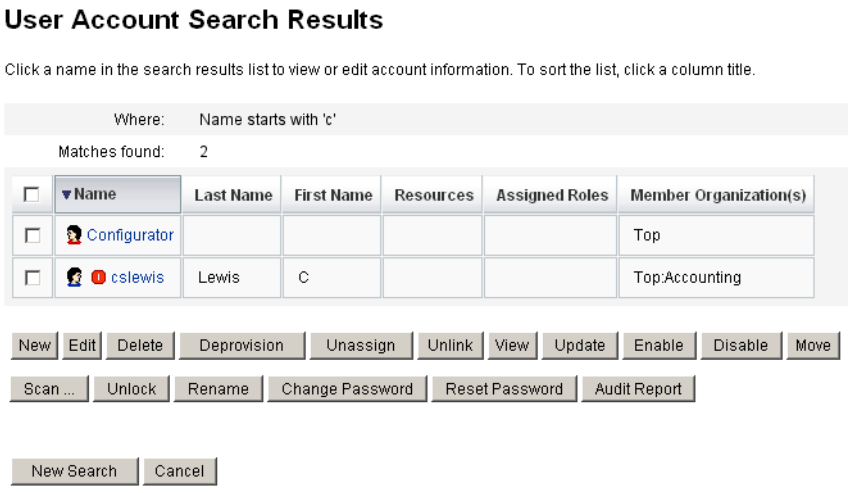
若要搜尋帳號，請從功能表列中選取 **[帳號]**，然後選取 **[尋找使用者]**。您可按下列一個或多個搜尋類型來搜尋帳號：

- 帳號詳細資訊，例如使用者名稱、電子郵件帳號，或姓氏、名字。這些選項取決於您組織所特有的 Identity Manager 實作。
- 使用者的管理員。若使用者名稱與 Identity Manager 的現有帳號不相符，管理員的使用者名稱就會出現在括號中。
- 資源帳號狀態，包括：
  - **停用** - 使用者無法存取任何 Identity Manager 或指定的資源帳號。
  - **部分停用** - 使用者無法存取一個或多個指定的資源帳號。
  - **啓用** - 使用者可以存取所有指定的資源帳號。
- 使用者帳號狀態，包括：
  - **已鎖定** - 因嘗試輸入密碼或回答認證問題失敗的次數超過所允許的最大次數，故使用者帳號被鎖定。
  - **未鎖定** - 未限制使用者帳號存取。
- 更新狀態，包括：
  - **否** - 尚未在任何資源上進行更新的使用者帳號。
  - **部分** - 已在至少一個 (但非所有) 指定資源上進行更新的使用者帳號。
  - **全部** - 已在所有指定資源上進行更新的使用者帳號。
- 指定的資源
- 角色 (請參閱第 153 頁的「尋找獲得指定角色的使用者」)
- 組織
- 組織控制
- 權能
- 管理員角色

搜尋結果清單會顯示符合您搜尋的所有帳號。從此結果頁面中，您可以：

- 選取欲編輯的使用者帳號。若要編輯帳號，請在搜尋結果清單中按一下此帳號；或在清單中選取此帳號，然後按一下 **[編輯]**。
- 在一個或多個帳號上執行動作 (例如啓用、停用、解除鎖定、刪除、更新或變更/重設密碼)。若要執行動作，請在搜尋結果清單中選取一個或多個帳號，然後按一下適當的動作。
- 建立使用者帳號。

圖 3-4　　使用者帳號搜尋結果



編輯使用者

本節資訊涵蓋檢視、編輯、重新指定及重新命名使用者帳號。

檢視使用者帳號

使用 [檢視使用者] 頁面可檢視帳號資訊。

若要檢視帳號資訊，請執行以下步驟：

1. 在管理員介面中，按一下功能表的 **[帳號]**。

   [使用者清單] 頁面會隨即開啓。

2. 選取要檢視其帳號的使用者旁之方塊。

3. 在 **[使用者動作]** 下拉式功能表中選取 **[檢視]**。

   [檢視使用者] 頁面會顯示使用者身份識別、指定、安全性、委派、屬性及規範遵循等資訊的子集合。[檢視使用者] 頁面上的資訊僅供檢視，無法編輯。

4. 按一下 **[取消]** 以返回至 [帳號] 清單。

編輯使用者帳號

使用 [編輯使用者] 頁面可編輯帳號資訊。

若要編輯帳號資訊，請執行以下步驟：

1. 在管理員介面中，按一下功能表的 **[帳號]**。

2. 選取要編輯其帳號的使用者旁之方塊。

3. 在 **[使用者動作]** 下拉式功能表中選取 **[編輯]**。

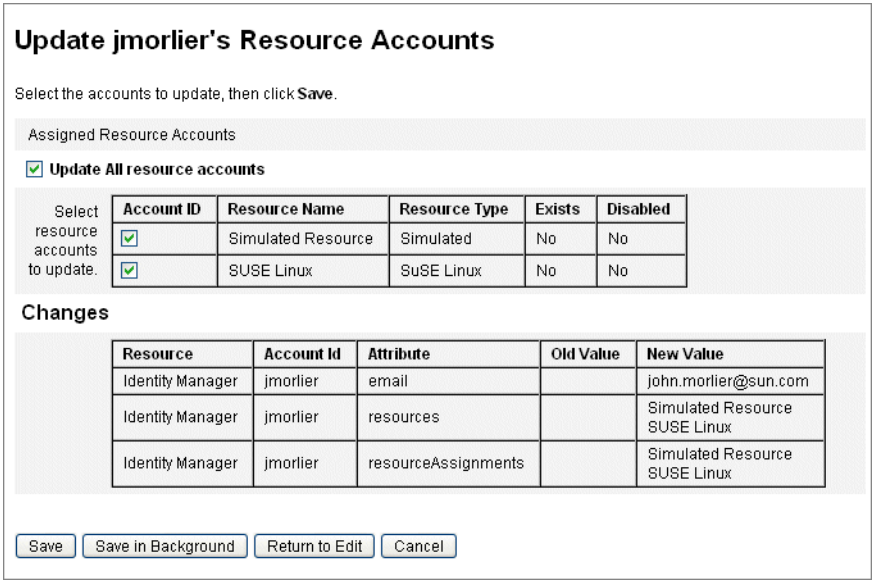
4. 進行變更並加以儲存。

   Identity Manager 會隨即顯示 [更新資源帳號] 頁面。此頁面顯示指定給使用者的資源帳號，以及將套用至帳號的變更。

5. 選取 **[更新全部資源帳號]** 將變更套用至所有已指定的資源；或不選取或選取一個或多個與使用者相關的資源帳號進行更新。

6. 再按一下 **[儲存]** 以完成編輯作業，或按一下 **[返回編輯]** 以建立更進一步的變更。

圖 3-5　　編輯使用者 (更新資源帳號)



重新將使用者指定給其他組織

移動動作可讓您移除某個組織的一或多位使用者，並重新指定；或將這些使用者移至新的組織。

若要移動使用者，請執行以下步驟：

1. 在管理員介面中，按一下功能表的 **[帳號]**。

   [使用者清單] 頁面會隨即開啓。

2. 選取要移動之使用者旁的方塊。

3. 在 **[使用者動作]** 下拉式功能表中選取 **[移動]**。

   [變更使用者的組織] 作業頁面會隨即開啓。

4. 選取要重新指定使用者的組織，然後按一下 **[啓動]**。

重新命名使用者

一般而言，重新命名資源上的帳號是一個複雜的動作。有鑑於此，Identity Manager 提供了一項單獨功能，可重新命名使用者的 Identity Manager 帳號，或重新命名一個或多個與該使用者相關的資源帳號。

若要使用重新命名功能，請在清單中選取使用者帳號，然後從 [使用者動作] 清單中選取 **[重新命名]** 選項。

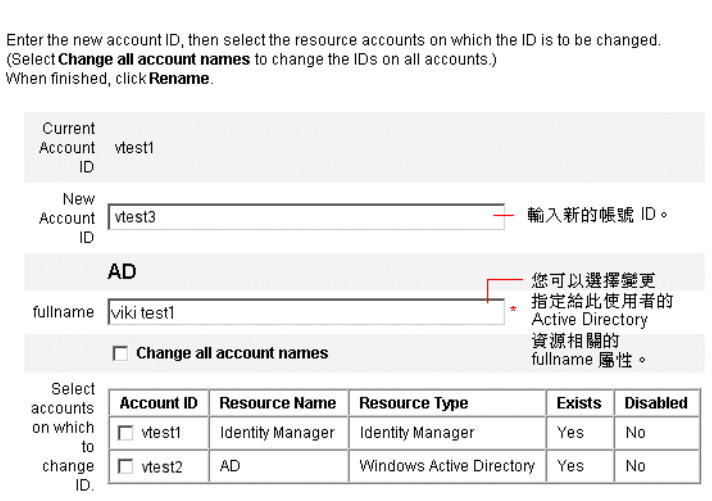
[重新命名使用者] 頁面可讓您變更使用者帳號名稱、相關的資源帳號名稱以及與使用者的 Identity Manager 帳號相關的資源帳號屬性。

備註 某些資源類型不支援帳號重新命名。

如下圖所示，使用者擁有指定的 Active Directory 資源。重新命名期間，您可以變更：

- Identity Manager 使用者帳號名稱
- Active Directory 資源帳號名稱
- Active Directory 資源屬性 (完整名稱)

圖 3-6 重新命名使用者



更新與帳號相關聯的資源

在更新動作中，Identity Manager 會更新與使用者帳號相關的資源。從帳號區域執行的更新會將任何之前爲使用者建立的擱置變更傳送至選取的資源。這個情況會在以下狀態發生：

- 建立變更時，資源不可使用。
- 對角色或資源群組進行的變更需要被推廣到指定了該角色或資源群組的所有使用者。在此狀況中，您應該使用 [尋找使用者] 頁面以搜尋使用者，然後在要執行更新動作的頁面上選取一個或多個使用者。

更新使用者帳號時，您可以：

- 選擇指定的資源帳號是否將接收更新的資訊。
- 更新所有資源帳號，或從清單中選取個別帳號。

更新單一使用者帳號的資源

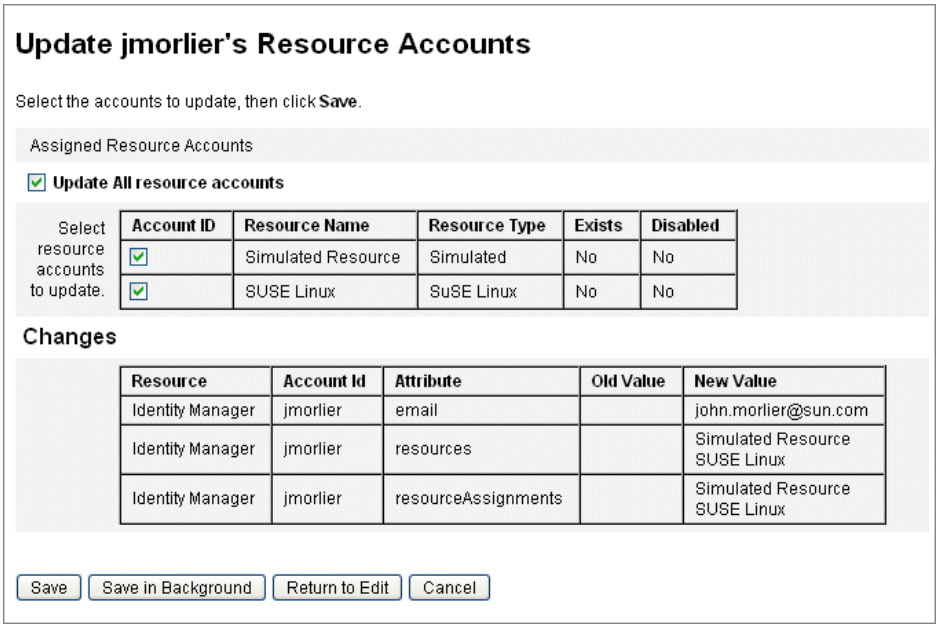
若要更新使用者帳號，請在清單中選取此帳號，然後從 [使用者動作] 清單中選取 **[更新]**。

在更新資源帳號頁面中，選取一個或多個要更新的資源，或選取 **[更新全部資源帳號]** 以更新所有已指定的資源帳號。完成後，按一下 **[確定]** 以開始更新程序。或者，按一下 **[進行背景儲存]** 以作爲背景程序執行該動作。

確認頁面會確認送至每個資源的資料。

圖 3-7 說明了更新資源帳號頁面。

圖 3-7 更新資源帳號



更新多個使用者帳號的資源

您可以同時更新兩個或多個 Identity Manager 使用者帳號。在清單中選取多個使用者帳號，然後從 [使用者動作] 清單中選取 **[更新]**。

備註 當您選擇更新多個使用者帳號時，您無法個別從每個使用者帳號中選取指定的資源帳號。此程序會更新您選取的全部使用者帳號的全部資源。

刪除 Identity Manager 使用者帳號

在 Identity Manager 中，刪除 Identity Manager 使用者帳號及刪除遠端資源帳號的方式相同。請選取 Identity Manager 帳號，依刪除資源帳號的步驟執行，而非選取遠端資源帳號予以刪除。

備註 若使用者有未完成的工作項目，或使用者有已委託給其他使用者但未完成的工作項目，Identity Manager 不會允許刪除使用者的 Identity Manager 帳號。委託的工作項目必須先行處理或移交給其他使用者，才能刪除使用者的 Identity Manager 帳號。

如需更多資訊，請參閱第 84 頁的「刪除單一使用者帳號的資源」及第 86 頁的「刪除多個使用者帳號的資源」。

刪除使用者帳號的資源

Identity Manager 提供數種刪除作業，可用以移除資源中 Identity Manager 使用者帳號存取權：

- **刪除** - 針對每個選取的資源，Identity Manager 會刪除遠端資源上的使用者帳號 (若要刪除 Identity Manager 的使用者，請將 Identity Manager 選爲資源)。
  - 已刪除的資源帳號會自動與 Identity Manager 使用者取消連結。
  - 已刪除的資源帳號不會對使用者取消指定。除非同時選取**取消指定**的動作，否則資源仍會保留在指定給使用者的狀態。
- **取消指定** - Identity Manager 會從使用者的已指定資源之清單中，移除所選的每個資源。
  - 取消指定的資源帳號會自動與 Identity Manager 使用者取消連結。
  - 遠端資源上的使用者帳號不會遭到刪除。除非同時選取**刪除**的動作，否則帳號會保持不變。
- **取消連結** - 針對每個選取的資源，移除 Identity Manager 中的使用者資源帳號資訊。
  - 除非同時選取**刪除**的動作，否則遠端資源上的使用者帳號會保持不變。
  - 除非同時選取**取消指定**的動作，否則資源仍會保持在使用者的已指定資源清單中。

- 如果您取消連結透過角色或資源群組已間接指定給使用者的帳號，則該連結可在更新使用者時復原。

備註 雖然**取消佈建**顯示爲 [使用者清單] 頁面功能表中的使用者動作，但 Identity Manager 中實際上僅有三種「刪除」動作：**刪除**、**取消指定**以及**取消連結**。

若要取消佈建遠端資源，請對資源使用**刪除**及**取消指定**動作。

刪除單一使用者帳號的資源

請使用下列程序對單一的 Identity Manager 使用者執行刪除作業。一次處理一個使用者帳號，可以爲個別的資源帳號指定不同的刪除、取消指定及 (或) 取消連結作業。

若要對單一使用者帳號執行刪除、取消指定或取消連結動作，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[帳號]**。

   [使用者清單] 頁面會隨即出現在 **[列出帳號]** 標籤上。

2. 選取一位使用者，然後按一下 **[使用者動作]** 下拉式功能表。

3. 從清單中選取 **[刪除]** 動作的任何項目 (**[刪除]**、**[取消佈建]**、**[取消指定]** 或 **[取消連結]**)。

   Identity Manager 會顯示 [刪除資源帳號] 頁面 (圖 3-8 (第 85 頁))。

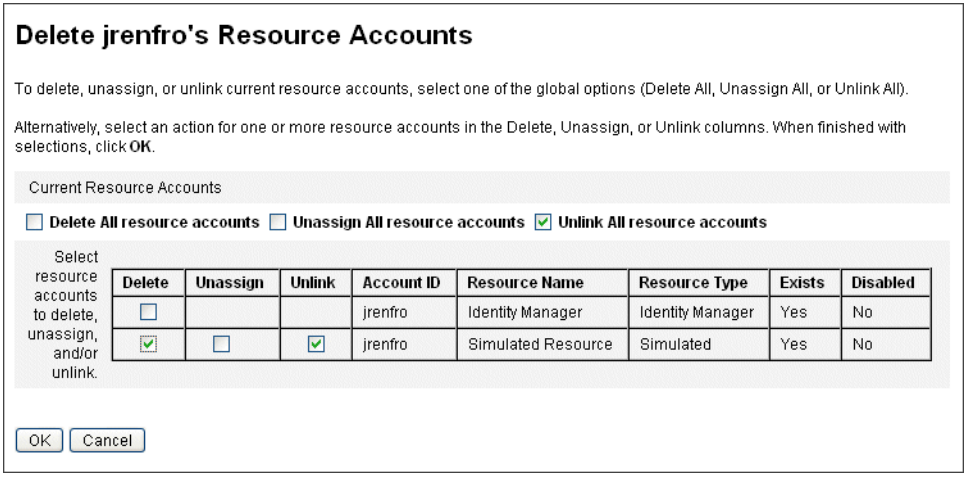
4. 填寫表單。如需有關 **[刪除]**、**[取消指定]** 及 **[取消連結]** 動作的更多資訊，請參閱第 83 頁的「刪除使用者帳號的資源」。

5. 按一下 **[確定]**。

圖 3-8 顯示 [刪除資源帳號] 頁面。在螢幕擷取中，使用者 jrenfro 在遠端資源 (虛擬資源) 上有一個使用中的帳號。已選取 **[刪除]** 動作，這表示提交表單時，會刪除資源上的 jrenfro 帳號。因爲刪除的帳號會自動取消連結，所以會移除 Identity Manager 中此資源的帳號資訊。虛擬資源會保持指定給 jrenfro 的狀態，因爲未選取 **[取消指定]** 動作。

若要刪除 jrenfro 的 Identity Manager 帳號，就應該針對 Identity Manager 選取 **[刪除]** 動作。

圖 3-8 刪除資源帳號頁



刪除多個使用者帳號的資源

您可同時對多個 Identity Manager 使用者帳號執行刪除作業，但僅能對那些使用者所有的資源帳號執行選取的刪除作業。

使用 Identity Manager 的 [批次處理帳號動作] 功能也可執行刪除作業。請參閱第 98 頁的「Delete、DeleteAndUnlink、Disable、Enable、Unassign 和 Unlink 指令」。

若要對多位使用者執行刪除、取消指定或取消連結動作，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[帳號]**。

   [使用者清單] 頁面會隨即出現在 **[列出帳號]** 標籤上。

2. 選取一或多位使用者，然後按一下 **[使用者動作]** 下拉式功能表。

3. 從清單中選取 **[刪除]** 動作的任何項目 (**[刪除]**、**[取消佈建]**、**[取消指定]** 或 **[取消連結]**)。

   Identity Manager 會隨即顯示 [確認刪除、取消指定或取消連結] 頁面 (圖 3-9 (第 87 頁))。

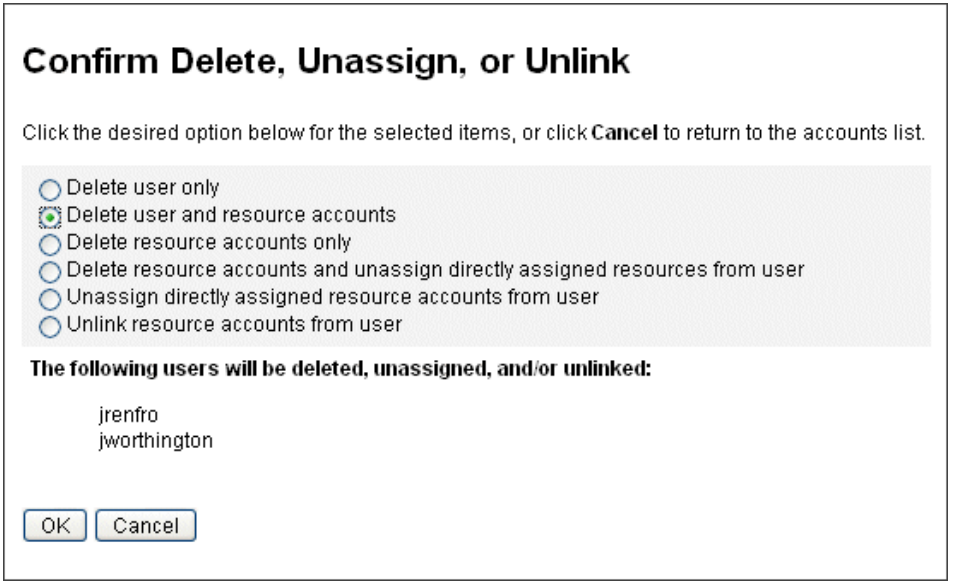
4. 請選取下列一個選項：

   - **僅刪除使用者** - 刪除使用者的 Identity Manager 帳號。此選項不會刪除或取消指定使用者的資源帳號。
   - **刪除使用者和資源帳號** - 刪除使用者的 Identity Manager 帳號及使用者的所有資源帳號。
   - **僅刪除資源帳號** - 刪除使用者的所有資源帳號。此選項不會取消指定資源帳號，也不會刪除使用者的 Identity Manager 帳號。
   - **刪除使用者的資源帳號，並取消指定直接指定的資源** - 刪除並取消指定使用者的所有資源帳號，但不會刪除使用者的 Identity Manager 帳號。
   - **取消指定直接指定給使用者的資源帳號** - 取消指定直接指定的資源帳號。此選項不會刪除使用者在遠端資源上的帳號。透過角色或資源群組指定的資源帳號不會受到影響。
   - **取消資源帳號與使用者的連結** - 移除 Identity Manager 中的使用者資源帳號資訊。不會刪除或取消指定遠端資源上的使用者帳號。更新使用者時，可能會復原透過角色或資源群組間接指定給使用者的帳號。

5. 按一下 **[確定]**。

圖 3-9 顯示 [確認刪除、取消指定或取消連結] 頁面。頁面的上半部會顯示六種能對多位使用者執行的動作。頁面的底部會顯示受到選取動作影響的使用者。

圖 3-9　　確認刪除、取消指定或 取消連結頁面



變更使用者密碼

所有 Identity Manager 使用者皆有指定的密碼。設定 Identity Manager 使用者密碼後，此密碼會用於同步化使用者的資源帳號密碼。若一個或多個資源帳號密碼無法同步化 (例如，遵循必要的密碼策略)，則可分別進行設定。

備註 如需有關帳號密碼策略的資訊以及有關使用者認證的一般資訊，請參閱第 104 頁的「管理帳號安全性和權限」。

從使用者清單頁面變更密碼

從 [使用者清單] 頁面 (**[帳號] > [列出帳號]**)，您可使用 **[變更密碼]** 使用者動作。

若要從 [使用者清單] 頁面變更使用者帳號密碼，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[帳號]**。

   [使用者清單] 頁面會隨即出現在 **[列出帳號]** 標籤上。

2. 選取一位使用者，然後按一下 [使用者動作] 下拉式功能表。
3. 若要變更密碼，請選取 **[變更密碼]**。

   [變更使用者密碼] 頁面會隨即開啓。

4. 鍵入新的密碼，然後按一下 **[變更密碼]** 按鈕。

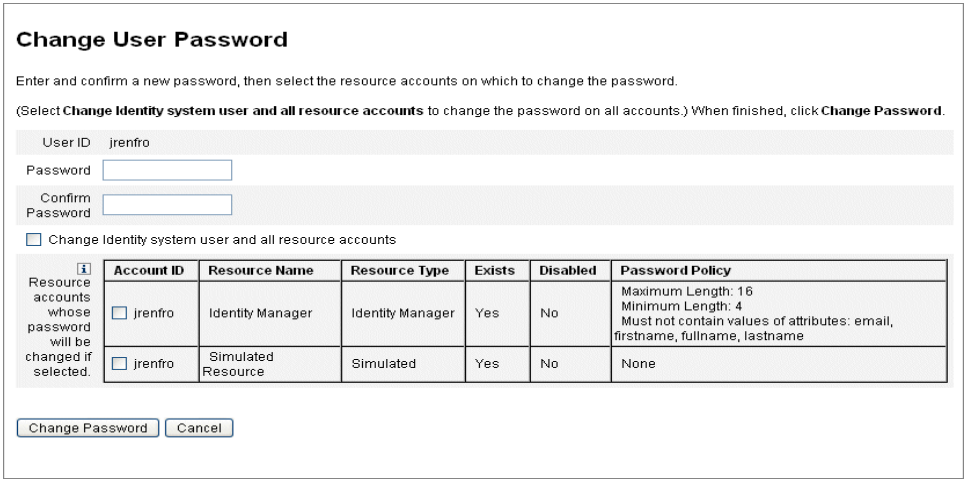
從主功能表變更密碼

若要從主功能表變更使用者帳號密碼，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[密碼]**。

   預設會出現 [變更使用者密碼] 頁面。

   圖 3-10 變更使用者密碼



2. 選取搜尋條件 (例如帳號名稱、電子郵件地址、姓氏或名字)，然後選取搜尋類型 (開頭爲、包含或是)。

3. 在輸入欄位中鍵入搜尋條件的一個或多個字母，然後按一下 **[尋找]**，Identity Manager 會傳回 ID 中包含輸入字元的所有使用者清單。按一下以選取一名使用者，然後返回 [變更使用者密碼] 頁。

4. 輸入並確認新密碼資訊，然後按一下 **[變更密碼]** 以變更所列資源帳號的使用者密碼。Identity Manager 會顯示一個工作流程圖，表示變更密碼動作的順序。

重設使用者密碼

重設 Identity Manager 使用者帳號密碼的程序與變更程序類似。重設程序與密碼變更程序不同處爲您不需指定新密碼。而是由 Identity Manager 隨機產生使用者帳號、資源帳號，或兩者組合的新密碼 (根據您的選擇與密碼策略)。

指定給使用者的策略 (直接指定或透過使用者的組織進行指定) 可控制數個重設選項，包括：

- 在停用重設之前，重設密碼的頻率爲何
- 顯示或傳送新密碼的位置。根據爲角色選取的 [重設通知選項]，Identity Manager 會使用電子郵件傳送新密碼給使用者，或 (在 [結果] 頁面) 將其顯示給要求重設的 Identity Manager 管理員。

從使用者清單頁面重設密碼

[使用者清單] 頁面 ([帳號] > [列出帳號]) 會提供 **[重設密碼]** 使用者動作。

若要從 [使用者清單] 頁面重設密碼，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[帳號]**。[使用者清單] 頁面會隨即出現在 **[列出帳號]** 標籤上。
2. 選取一位使用者，然後按一下 **[使用者動作]** 下拉式功能表。
3. 若要重設密碼，請選取 **[重設密碼]**。

   [重設使用者密碼] 頁面會隨即開啓。
4. 按一下 **[重設密碼]** 按鈕。

使用 Identity Manager 帳號策略設定密碼過期日

依預設，密碼在您重設時會立即過期。這表示當使用者在重設後第一次登入時，必須先選取新密碼才能存取。此預設值可在表單中置換，使用者密碼會根據與使用者相關聯的 [Identity Manager 帳號策略] 中，所設定的過期密碼策略決定何時過期。

若要置換變更密碼需求，請編輯 [重設使用者密碼表單]，然後將下列值設爲 `false`：

```
resourceAccounts.currentResourceAccounts[Lighthouse].expirePassword
```

透過 [Identity Manager 帳號策略] 的 [重設選項] 欄位，有兩種可讓密碼過期的方法：

- **永久的** - 會使用在 passwordExpiry 策略屬性中所指定的時期，來計算出與重設密碼時的目前日期相對應的密碼過期日期，然後爲使用者設定該日期。如果沒有指定值，則變更或重設的密碼將永不過期。
- **臨時的** - 會使用在 tempPasswordExpiry 策略屬性中指定的時期，來計算出與重設密碼時的目前日期相對應的密碼過期日期，然後爲使用者設定該日期。如果沒有指定值，則變更或重設的密碼將永不過期。如果 tempPasswordExpiry 的值設爲 0，密碼會立即過期。

  `tempPasswordExpiry` 屬性僅會在重設密碼時套用 (隨機變更)。它不適用於密碼變更。

停用、啟用及解除鎖定使用者帳號

本節說明如何停用及啓用 Identity Manager 使用者帳號。亦會說明如何協助其 Identity Manager 帳號遭鎖定的使用者。

停用使用者帳號

停用使用者帳號時，您可更改該帳號讓使用者無法再登入 Identity Manager 或其指定的資源帳號。

請注意，管理員可從管理員介面**停用**使用者帳號，但無法**鎖定**使用者帳號。只有當使用者超過 Identity Manager 帳號策略所定義的允許失敗登入嘗試次數時，帳號才會遭鎖定。

備註 若指定的資源無法從本機停用帳號，卻可變更密碼，則指定隨機產生的新密碼，即可配置 Identity Manager 停用該資源的使用者帳號。

若要確保此功能運作正常，請執行下列作業：

1. 開啓「編輯資源精靈」中的 [身份識別系統參數] 頁面 (如需有關如何開啓精靈的說明，請參閱第 169 頁的「使用資源精靈編輯資源」)。
2. 在「帳號功能配置」表中，檢查 **[密碼]** 功能及 **[停用]** 功能的 **[停用？]** 欄中是否**沒有**核取標記 (若要顯示 **[停用]** 功能，請選取 **[顯示全部功能]**)。

   若 **[停用]** 功能在 **[停用？]** 欄中**有**核取標記，即無法停用資源的帳號。

停用單一使用者帳號

若要停用使用者帳號，請在 **[使用者清單]** 中選取該帳號，然後從 **[使用者動作]** 下拉式功能表選取 **[停用]**。

在顯示的 [停用] 頁面上，選取要停用的資源帳號，然後按一下 **[確定]**。Identity Manager 顯示停用 Identity Manager 使用者帳號與全部相關資源帳號的結果。帳號清單表示使用者帳號已停用。

停用多個使用者帳號

您可以同時停用兩個或多個 Identity Manager 使用者帳號。

在清單中選取多個使用者帳號，然後從 [使用者動作] 清單中選取 **[停用]**。

備註 當您選擇停用多個使用者帳號時，您無法個別從每個使用者帳號中選取指定的資源帳號。此程序會停用您選取的全部使用者帳號的全部資源。

啟用使用者帳號

使用者帳號啓用與停用程序相反。

Identity Manager 也會依照選取的通知選項，而在管理員的結果頁上顯示密碼。

使用者接下來可重設密碼 (透過身份認證程序)，或由具有管理員權限的使用者重設。

備註 如果指定的資源無法從本機支援帳號啓用功能，但支援密碼變更，則可透過重設密碼，配置 Identity Manager 啓用該資源的使用者帳號。

若要確保此功能運作正常，請執行下列作業：

1. 開啓「編輯資源精靈」中的 [身份識別系統參數] 頁面 (如需有關如何開啓精靈的說明，請參閱第 169 頁的「使用資源精靈編輯資源」)。
2. 在「帳號功能配置」表中，檢查 **[密碼]** 功能及 **[啓用]** 功能的 **[停用？]** 欄中是否**沒有**核取標記 (若要顯示 **[啓用]** 功能，請選取 **[顯示全部功能]**)。

   若 **[啓用]** 功能在 **[停用？]** 欄中**有**核取標記，即無法啓用資源的帳號。

啟用單一使用者帳號

若要啓用使用者帳號，請在清單中選取此帳號，然後從 [使用者動作] 清單中選取 **[啓用]**。

在顯示的 [啓用] 頁面上，選取要啓用的資源，然後按一下 **[確定]**。Identity Manager 顯示啓用 Identity Manager 帳號與全部相關資源帳號的結果。

啟用多個使用者帳號

您可以同時啓用兩個或多個 Identity Manager 使用者帳號。在清單中選取多個使用者帳號，然後在 [使用者動作] 清單中選取 [啓用]。

備註 當您選擇啓用多個使用者帳號時，您無法個別從每個使用者帳號中選取指定的資源帳號。此程序會啓用您選取的全部使用者帳號的全部資源。

解除鎖定使用者帳號

若無法成功登入 Identity Manager，使用者即會遭鎖定。使用者一定會在超過 Identity Manager 帳號策略所定義的允許失敗登入嘗試次數之後，才會遭鎖定。

備註 只有 Identity Manager 使用者介面上的登入嘗試才會計入 Identity Manager 鎖定 (亦即，管理員介面、一般使用者介面、指令行介面或 SPML API 介面)。資源帳號的失敗登入嘗試不會計入，也不會造成使用者的 Identity Manager 帳號遭鎖定。

Identity Manager 帳號策略會建立**失敗密碼**或**問題**登入嘗試的次數上限。

- 超過**失敗密碼**登入嘗試次數上限的使用者會遭鎖定，無法存取所有的 Identity Manager 應用程式介面，包括 [忘記密碼] 介面。
- 超過**失敗問題**登入嘗試最大次數的使用者，可向任何 Identity Manager 應用程式介面進行認證，但 [忘記密碼] 除外。

密碼登入嘗試失敗

因爲超過失敗密碼登入嘗試次數而遭 Identity Manager 鎖定的使用者，在管理員解除鎖定帳號或鎖定過期之前，都無法登入。

- 若管理員有使用者成員組織的管理控制以及 [解除鎖定使用者] 權能，管理員即可解除鎖定帳號。
- 若 [Identity Manager 帳號策略] 中設有 [鎖定逾時] 值，則帳號的鎖定一定會過期。失敗密碼登入嘗試的 [鎖定逾時] 值由 **[密碼登入失敗後造成之帳號鎖定的到期時間]** 值所設定。

問題登入嘗試失敗

因超過失敗問題登入嘗試次數而遭 [忘記密碼] 介面鎖定的使用者，在管理員解除鎖定帳號、遭鎖定的使用者 (或具有適當權能的使用者) 變更或重設使用者密碼或鎖定過期之前，都無法登入該介面。

- 若管理員有使用者成員組織的管理控制以及 [解除鎖定使用者] 權能，管理員即可解除鎖定帳號。
- 若 [Identity Manager 帳號策略] 中設有 [鎖定逾時] 值，則帳號的鎖定一定會過期。失敗問題登入嘗試的 [鎖定逾時] 值由 **[問題登入失敗後造成之帳號鎖定的到期時間]** 值所設定。

具有適當權能的管理員可以對處於鎖定狀態的使用者執行以下作業：

- 更新 (包括資源重新佈建)
- 變更或重設密碼
- 停用或啓用
- 重新命名
- 解除鎖定

若要解除鎖定帳號，請在清單中選取一個或多個使用者帳號，然後從 **[使用者動作] 或 [組織動作]** 清單中選取 **[解除鎖定使用者]**。

批次處理帳號動作

您可以在 Identity Manager 帳號上執行數個批次處理動作，以同時處理多個帳號。

您可以啓動以下批次處理動作：

- **刪除** - 此動作會刪除、取消指定和取消連結選取的資源帳號。選取 [以 Identity Manager 帳號爲目標] 選項，可同時刪除每位使用者的 Identity Manager 帳號。
- **刪除與取消連結** - 此動作會刪除所有選取的資源帳號，並取消這些帳號與使用者的連結。
- **停用** - 停用所有選取的資源帳號。選取 [以 Identity Manager 帳號爲目標] 選項可同時停用每位使用者的 Identity Manager 帳號。
- **啓用** - 啓用所有選取的資源帳號。選取 [以 Identity Manager 帳號爲目標] 選項，可啓用每位使用者的 Identity Manager 帳號。
- **取消指定，取消連結** - 取消連結所有選取的資源帳號，並移除對這些資源的 Identity Manager 使用者帳號指定。取消指定不會移除資源的帳號。對於透過角色或資源群組間接指定給 Identity Manager 使用者的帳號，您無法取消指定該帳號。
- **取消連結** - 移除資源帳號與 Identity Manager 使用者帳號的關聯 (連結)。取消連結不會從資源中移除該帳號。如果您取消透過角色或資源群組間接指定給 Identity Manager 使用者的帳號連結，則更新使用者時該連結會還原。

如果您的檔案或應用程式中有一份使用者清單，如電子郵件用戶端或試算表程式，則批次處理動作就能有最好的執行效果。您可以將清單複製並貼上至此介面頁面的欄位中，也可以從檔案載入使用者清單。

根據使用者的搜尋結果，可以執行其中許多動作。使用 [尋找使用者] 頁面 (**[帳號] > [尋找使用者]**) 搜尋使用者。

作業完成後顯示作業結果時，按一下 **[下載 CSV]** 可將批次處理帳號作業的結果儲存至 CSV 檔案。

啟動批次處理帳號動作

若要啓動批次處理帳號動作，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[帳號]**。
2. 按一下輔助功能表的 **[啓動批次處理動作]**。
3. 填寫表單並按一下 **[啓動]**。

   Identity Manager 會啓動背景作業以執行批次處理動作。

若要監視批次處理動作作業的狀態，請按一下主功能表的 **[伺服器作業]**，再按一下 **[全部作業]**。

使用動作清單

您可以使用逗號分隔值 (CSV) 格式指定批次處理動作清單。這能讓您在一份動作清單中混用不同的動作類型。此外，您可以指定更複雜的建立和更新動作。

CSV 格式包含兩個或多個輸入行。每行包含一份以逗號分隔的值清單。第一行包含欄位名稱。剩餘的每一行對應欲對 Identity Manager 使用者、使用者的資源帳號或二者所執行的一個動作。每一行應該包含同樣數量的值。若爲空值則相應的欄位值將不會變更。

任何批次處理動作 CSV 輸入都需要兩個欄位：

- **使用者** - 包含 Identity Manager 使用者的名稱。
- **指令** - 包含對 Identity Manager 使用者所採取的動作。有效的指令有：
  - **Delete** - 刪除、取消指定以及取消連結資源帳號和 (或) Identity Manager 帳號。
  - **DeleteAndUnlink** - 刪除與取消連結資源帳號。
  - **Disable** - 停用資源帳號和 (或) Identity Manager 帳號。
  - **Enable** - 啓用資源帳號和 (或) Identity Manager 帳號。
  - **Unassign** - 取消指定與取消連結資源帳號。
  - **Unlink** - 取消連結資源帳號。
  - **Create** - 建立 Identity Manager 帳號。選擇性地建立資源帳號。
  - **Update** - 更新 Identity Manager 帳號。選擇性地建立、更新或刪除資源帳號。
  - **CreateOrUpdate** - 如果 Identity Manager 帳號尚不存在，則執行建立動作。否則執行更新動作。

Delete、DeleteAndUnlink、Disable、Enable、Unassign 和 Unlink 指令

執行 Delete、DeleteAndUnlink、Disable、Enable、Unassign 或 Unlink 動作時，需要指定的唯一額外欄位是 [資源]。使用資源欄位可指定哪些資源上的哪些帳號將受影響。

資源欄位可有下列值：

- **all** - 處理所有資源帳號，包括 Identity Manager 帳號。
- **resonly** - 處理除 Identity Manager 帳號以外的所有資源帳號。
- *resource_name* [| *resource_name ...*] - 處理指定的資源帳號。指定 Identity Manager 以處理 Identity Manager 帳號。

以下是其中幾個動作的 CSV 格式範例：

```
command,user,resources
Delete,John Doe,all
Disable,Jane Doe,resonly
Enable,Henry Smith,Identity Manager
Unlink,Jill Smith,Windows Active Directory|Solaris Server
```

Create、Update 和 CreateOrUpdate 指令

如果您正在執行 Create、Update 或 CreateOrUpdate 指令，則您除了指定 [使用者] 與 [指令] 欄位外，還可以指定 [使用者檢視] 中的欄位。使用的欄位名稱是檢視中的屬性之路徑表示式。如需有關使用者檢視中可用屬性的資訊，請參閱「Identity Manager Workflows, Forms, and Views」。如果是使用自訂的「使用者表單」，您就能使用表單的欄位名稱中的部分路徑表示式。

在批次處理動作中使用的一些較常見的路徑表示式有：

- **waveset.roles** - 一份要指定給 Identity Manager 帳號的一個或多個角色名稱之清單。
- **waveset.resources** - 一份要指定給 Identity Manager 帳號的一個或多個資源名稱之清單。
- **waveset.applications** - 一份要指定給 Identity Manager 帳號的一個或多個角色名稱之清單。
- **waveset.organization** - 放置 Identity Manager 帳號的組織名稱。
- **accounts**[*resource_name*].*attribute_name* - 資源帳號屬性。屬性的名稱列示在資源的綱目中。

以下是建立和更新動作的 CSV 格式範例：

```
command,user,waveset.resources,password.password,password.confirmPassword,a
ccounts[Windows Active Directory].description,accounts[Corporate
Directory].location
Create,John Doe,Windows Active Directory|Solaris
Server,changeit,changeit,John Doe - 888-555-5555,
Create,Jane Smith,Corporate Directory,changeit,changeit,,New York
CreateOrUpdate,Bill Jones,,,,,California
```

具有多個值的欄位

一些欄位可擁有多個值。它們稱爲多值欄位。例如，您可以使用 waveset.resources 欄位將多個資源指定給一位使用者。您可以使用垂直列 (|) 字元 (也稱爲「管道」字元) 分隔一個欄位的多個值。您可以如下指定多值語法：

```
value0 | value1 [ | value2 ... ]
```

對現有的使用者更新多值欄位時，您可能不想將目前欄位的值替代爲一個或多個新值。您可能想要移除一些值或加入現行值中。您可以使用欄位指令來指定如何處理現有欄位的值。欄位指令移到欄位值的前面，並以垂直列字元括住，如下所示：

```
|directive [ ; directive ] | field values
```

您可從下列指令中選擇：

- **Replace** - 以指定的值替代目前的值。若未指定指示詞 (或僅指定 List 指示詞)，則此指示詞是預設值。
- **Merge** - 將指定的值增加至目前的值。系統將篩選出重複值。
- **Remove** - 從目前的值中移除指定的值。
- **List** - 強制以處理多個值的方式處理欄位的值，即使該欄位只有一個值也一樣。通常不需要這個指令，因爲不論值的數量有多少，系統都會適當處理大部分的欄位。這是唯一能與其他指示詞一起指定的指示詞。

備註 欄位值區分大小寫。這在您指定 Merge 與 Remove 指示詞時特別重要。這些值必須完全符合，才能正確地移除值，或避免在合併時出現多個類似值。

欄位值的特殊字元

若欄位值中有逗號 (,) 或雙引號 (") 字元，或想要保留前導或尾隨空格，則需要在欄位值兩旁加上一對雙引號 ("欄位值")。接下來需要以兩個雙引號 (") 字元來取代欄位值中的雙引號。例如，`John "Johnny" Smith` 欄位值的結果應該是 `"John ""Johnny"" "Smith"`。

如果您的欄位值中有垂直列 (|) 或反斜線 (\) 字元，則您必須在其前面加上一條反斜線 (\| 或 \\)。

批次處理動作檢視屬性

執行 Create、Update 或 CreateOrUpdate 動作時，「使用者檢視」中有一些屬性只能在批次處理動作處理中使用。您可以在「使用者表單」中參照這些屬性，讓批次處理動作執行特定的動作。這些屬性如下所示：

- **waveset.bulk.fields.***field_name* - 這些屬性包含從 CSV 輸入中讀取的欄位值，其中 *field_name* 是欄位的名稱。例如，指令與使用者欄位分別位於路徑表示式爲 `waveset.bulk.fields.command` 與 `waveset.bulk.fields.user` 的屬性中。
- **waveset.bulk.fieldDirectives.***field_name* - 只會針對已指定指令的欄位定義這些屬性。此值爲指示字串。
- **waveset.bulk.abort** - 將此布林屬性設爲 true，以便中斷目前的動作。
- **waveset.bulk.abortMessage** - 將此屬性設爲訊息字串，以便在 waveset.bulk.abort 設爲 true 時可顯示該訊息。若未設定此屬性，則會顯示一般中斷訊息。

相互關聯與確認規則

當您沒有可用來填入動作的使用者欄位的 Identity Manager 使用者名稱時，可使用相互關聯與確認規則。若未指定使用者欄位值，啓動批次處理動作時，您就必須指定相互關聯規則。若未指定使用者欄位值，那麼就不會對該動作計算相互關聯與確認規則。

相互關聯規則會尋找符合動作欄位的 Identity Manager 使用者。確認規則會根據動作欄位來測試 Identity Manager 使用者，以便確定是否是符合的使用者。這樣的兩階段式方法可讓 Identity Manager 快速尋找可能的使用者 (根據名稱或屬性) 並且只對可能的使用者執行龐雜的檢查，藉此最佳化相互關聯。

建立相互關聯或確認規則的方法是分別建立 SUBTYPE_ACCOUNT_CORRELATION_RULE 或 SUBTYPE_ACCOUNT_CONFIRMATION_RULE 子類型的規則物件。

如需有關相互關聯與確認規則的更多資訊，請參閱「Identity Manager Technical Deployment Overview」中的「資料載入與同步化」一章。

相互關聯規則

相互關聯規則的輸入是動作欄位的對映。輸出必須爲以下其中之一：

- 字串 (包含使用者名稱或 ID)
- 字串清單元素 (各個使用者名稱或 ID)
- WSAttribute 清單元素
- AttributeCondition 清單元素

典型的相互關聯規則會根據動作中的欄位值來產生使用者名稱清單。相互關聯規則也可能會產生用來選取使用者的屬性條件清單 (參考 Type.USER 的可查詢屬性)。

相對來說，相互關聯規則應該比較簡便，但是應該盡可能縮小範圍。可能的話，將龐雜的處理留給確認規則。

屬性條件必須參考 Type.USER 的可查詢屬性。這些都是在名爲「IDM 模式配置」的 Identity Manager 配置物件中進行配置。

在擴充屬性上進行相互關聯需要特殊配置：

- 延伸屬性必須指定爲可查詢的。若要將延伸屬性設定爲可查詢，請執行以下步驟：

  a. 開啓「IDM 模式配置」。您必須有「IDM 模式配置」權能才可能檢視或編輯「IDM 模式配置」。

  b. 請找到 <IDMObjectClassConfiguration name='User'> 元素。

  c. 找到 <IDMObjectClassAttributeConfiguration name='*xyz*'> 元素，此處的 *xyz* 就是要設爲可查詢的屬性之名稱。

  d. 設定 queryable='true'

  在編碼樣例 3-1 中，電子郵件的延伸屬性皆定義爲可查詢。

編碼樣例 3-1 定義電子郵件延伸屬性爲可查詢的 XML 摘錄

```
<IDMSchemaConfiguration>
  <IDMAttributeConfigurations>
    <IDMAttributeConfiguration name='email'
                               syntax='STRING'/>
    </IDMAttributeConfiguration>
  </IDMAttributeConfigurations>
  <IDMObjectClassConfigurations>
    <IDMObjectClassConfiguration name='User'
                                 extends='Principal'
                                 description='User description'>
       <IDMObjectClassAttributeConfiguration name='email'
                                             queryable='true'/>
    </IDMObjectClassConfiguration>
  </IDMObjectClassConfigurations>
</IDMSchemaConfiguration>
```

- Identity Manager 應用程式 (或應用程式伺服器) 需要重新啓動，「IDM 模式配置」的變更才會生效。

確認規則

對確認規則的輸入如下：

- `userview` - Identity Manager 使用者的完整檢視。
- `account` - 動作欄位的對映。

如果使用者符合動作欄位，確認規則會傳回字串形式的 true 布林值；否則會傳回 false 值。

典型的確認規則會比對來自使用者檢視的內部值與動作欄位的值。確認規則還可當作相互關聯作業中的選擇性第二階段作業，也就是執行無法在相互關聯規則中表示的檢查 (或是太龐雜而無法在相互關聯規則中計算的檢查)。一般而言，只有在以下情況下才會需要確認規則：

- 相互關聯規則可能傳回多個相符的使用者。
- 無法查詢必須比對的使用者值。

系統會對相互關聯規則傳回的每個符合的使用者各執行一次確認規則。

管理帳號安全性和權限

本小節說明了爲提供對使用者帳號的安全存取權和管理 Identity Manager 中的使用者權限，您可以執行的動作。

- 設定密碼策略
- 使用者認證
- 指定管理權限

設定密碼策略

資源密碼策略可用於建立密碼限制。強密碼策略提供增強的安全性，可協助防止他人未經授權登入資源。您可以編輯密碼策略以設定或選取字元範圍值。

若要開始使用密碼策略，請按一下主功能表中的 **[安全性]**，再按一下 **[策略]**。

若要編輯密碼策略，請按一下 [策略] 清單中的密碼策略。若要建立密碼策略，請從選項的 **[新增...]** 清單中選取 **[字串品質策略]**。

備註 如需有關策略的更多資訊，請參閱第 176 頁的「配置 Identity Manager 策略」。

建立策略

密碼策略是字串品質策略的預設類型。爲新策略命名並提供選擇性說明後，請爲定義該策略的規則選取選項和參數。

長度規則

長度規則設定密碼必需的最短與最長字元長度。請選取此選項以啓用規則，然後輸入規則的限制值。

字元類型規則

字元類型規則設定密碼中可包含的某些類型字元及數字的最大與最小數目。其中包括：

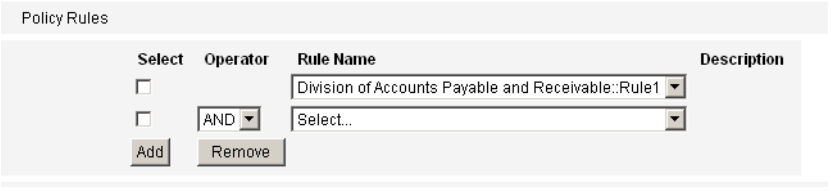
- 字母、數字、大寫、小寫與特殊字元的最小與最大數目
- 內嵌數字字元的最小與最大數目
- 重複與循序字元的最多數目
- 開始字母與數字字元的最少數目

輸入每個字元類型規則的數字限制值；或輸入「全部」以表示所有字元均必須爲該類型。

字元類型規則的最小數目。 您也可以設定必須通過驗證的字元類型規則最小數目，如圖 3-11 中所示。必須通過的最小數目爲 1。最大數目不能超過您已啓用的字元類型規則數目。

備註 若要將必須通過的最少數目設定爲最高值，請輸入「全部」。

圖 3-11 密碼策略 (字元類型) 規則



字典策略選擇

您可以選擇比照字典中的字詞來檢查密碼，針對簡單的字典攻擊提供防護。在您可以使用此選項之前，您必須：

- 配置字典
- 載入字典字詞

可以從 [策略] 頁面配置字典。如需有關如何設定字典的更多資訊，請參閱第 179 頁的「字典策略」。

密碼歷程記錄策略

可以禁止重新使用在新選密碼之前剛使用過的密碼。

在 [無法重複使用的先前密碼次數] 欄位中，輸入大於一的數值可禁止再次使用目前與之前的密碼。例如，若輸入的數值爲 3，則新密碼不可與目前密碼或其之前使用的兩個密碼相同。

您也可以禁止重複使用與曾經用過的密碼類似的字元。在 [不可重複使用之先前密碼中的類似字元上限] 欄位中，輸入新密碼不得重複先前密碼的連續字元數目。例如，若是輸入值爲 7，且舊密碼爲 password1，則新密碼便不可以是 password2 或 password3。

如果輸入的值是 0，則表示不論順序，所有字元都必須不一樣。例如，舊密碼若是 abcd，則新密碼中便不可以含有字元 a、b、c 或 d。

這個規則可以套用到之前一個或多個密碼。需要檢查的先前密碼數目在 [無法重複使用的先前密碼次數] 欄位中指定。

不得包含字詞

您可以輸入一個或多個密碼不可包含的字。在輸入方塊中，在每一行輸入一個字。

您也可以透過配置並實作字典策略來排除字詞。如需更多資訊，請參閱第 179 頁的「字典策略」。

不得包含屬性

選取一個或多個密碼不可包含的屬性。屬性包括：

- accountID
- email
- firstname
- fullname
- lastname

您可以在 `UserUIConfig` 配置物件中，變更所允許的密碼「不得包含」之屬性集。詳細資訊請參閱第 179 頁的「策略中的「不得包含」屬性」。

實作密碼策略

會爲每個資源建立密碼策略。若要將密碼策略置於特定資源中，請在 [密碼策略] 選項清單中將其選取，該清單位於 [建立或編輯資源精靈] 的 [策略配置] 區域：[Identity Manager 參數] 頁面。

使用者認證

若使用者忘記其密碼或其密碼遭重設，使用者只要回答一個或多個帳號認證問題即可存取 Identity Manager。這些問題與管理這些問題的規則是 Identity Manager 帳號策略的一部份，可以由您建立。不同於密碼策略，Identity Manager 帳號策略被直接或透過指定給使用者的組織指定給使用者 (位於 [建立與編輯使用者] 頁面)。

若要在帳號策略中設定認證，請執行以下步驟：

1. 按一下主功能表中的 **[安全性]**，再按一下 **[策略]**。
2. 從策略清單中選取 [預設的 Identity Manager 帳號策略]。

   在頁面的 [輔助身份認證策略選項] 區域中會提供認證選項。

重要事項！首次設定時，使用者應登入使用者介面，並提供其認證問題的初始答案。若未設定這些答案，則使用者無法在不使用其密碼的情況下成功登入。

認證問題策略可決定當使用者按一下 [登入] 頁面上的 **[忘記密碼？]** 按鈕，或存取 [變更我的答案] 頁面時，所會發生的情況。表 3-3 說明每一個選項。

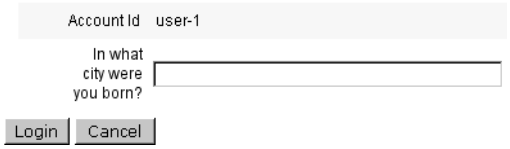
表 3-3 認證問題策略選項

選項	說明
循環	Identity Manager 會從已配置的問題清單中選取下一個問題，並將此問題指定給使用者。認證問題清單中的第一個問題會指定給第一個使用者，而第二個問題則會指定給第二個使用者。此模式會一直繼續，直到超出問題數為止。此時，會按照問題的前後順序將其指定給使用者。例如，如果總共有 10 個問題，則會將第一個問題指定給第 11 和第 21 個使用者。 僅會顯示所選取的問題。若要使用者每次回答不同的問題，請使用「隨機」策略並將問題數設定為 1。 使用者無法定義自己的認證問題。如需此功能的詳細資訊，請參閱個人化的認證問題。
隨機	此選項可讓管理員指定使用者必須回答的問題數量。Identity Manager 會從策略以及使用者所定義之問題清單中，隨機選取並顯示指定數量的問題。使用者必須回答所有顯示的問題。
任何	Identity Manager 顯示所有策略定義與個人化的問題。您必須指定使用者必須回答的問題數。
全部	使用者必須回答所有策略定義與個人化的問題。

您可以確認您的認證選擇，方法爲登入 Identity Manager 使用者介面，按一下 **[忘記密碼？]**，然後回答出現的問題。

圖 3-12 顯示了使用者帳號認證螢幕範例。

圖 3-12 使用者帳號認證

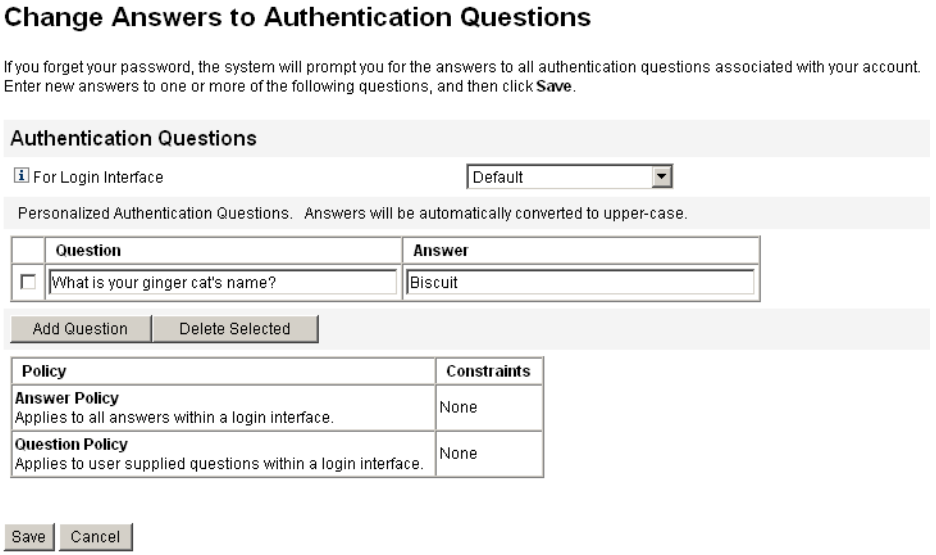


個人化的認證問題

在 Identity Manager 帳號策略中，您可以選取選項以讓使用者可以在使用者介面和管理員介面中提供自己的認證問題。此外，透過使用個性化的認證問題，您還可以設定使用者爲成功登入所必須提供和回答問題的最小數目。

然後，使用者可在 [變更認證問題的答案] 頁面中增加和變更問題。圖 3-13 中顯示了此頁面的範例。

圖 3-13 變更答案 - 個人化的認證問題



認證後略過變更密碼詢問

使用者透過回答一個或多個問題成功通過認證後，依預設，系統將要求他提供一個新密碼。然而，您可以透過爲一個或多個 Identity Manager 應用程式設定 bypassChangePassword 系統配置特性，來將 Identity Manager 配置爲略過變更密碼詢問。

如需有關編輯系統配置物件的說明，請參閱第 197 頁。

若要在成功認證後略過所有應用程式的變更密碼詢問，請在系統配置物件中將 bypassChangePassword 特性設定如下：

編碼樣例 3-2 設定用於略過變更密碼詢問的屬性

```
<Attribute name="ui"
  <Object>
    <Attribute name="web">
      <Object>
        <Attribute name='questionLogin'>
          <Object>
            <Attribute name='bypassChangePassword'>
              <Boolean>true</Boolean>
            </Attribute>
          </Object>
        </Attribute>
        ...
      </Object>
    ...
```

若要對特定應用程式停用此密碼詢問，請將其設定如下：

編碼樣例 3-3 設定用於停用變更密碼詢問的屬性

```
<Attribute name="ui">
  <Object>
    <Attribute name="web">
      <Object>
        <Attribute name='user'>
          <Object>
            <Attribute name='questionLogin'>
              <Object>
                <Attribute name='bypassChangePassword'>
                  <Boolean>true</Boolean>
                </Attribute>
              </Object>
            </Attribute>
              </Object>
        </Attribute>
        ...
      </Object>
    ...
```

指定管理權限

您可以如下將 Identity Manager 管理權限或權能指定給使用者：

- 管理員角色 - 若使用者已指定有管理員角色，則會繼承由該角色所定義的權能和所控制的組織。依預設，在建立所有 Identity Manager 使用者帳號時，會爲其指定 使用者管理員角色。如需有關管理員角色和建立管理員角色的詳細資訊，請參閱第 4 章中的「瞭解與管理資源」。
- 權能 - 權能由規則所定義。Identity Manager 提供了幾組依功能分組的權能，您可以從中進行選取。指定權能可以更詳細地指定管理權限。如需有關權能和建立權能的資訊，請參閱第 6 章中的「瞭解與管理權能」。
- 所控制的組織 - 所控制的組織可授予對指定組織所具有的管理控制權限。如需更多資訊，請參閱第 6 章中的瞭解 Identity Manager 組織。

如需有關 Identity Manager 管理員和管理責任的更多資訊，請參閱第 6 章「管理」。

使用者自我探索

Identity Manager 一般使用者介面可讓一般使用者探索資源帳號。這表示具有 Identity Manager 身份的使用者可與現有的但無關聯的資源帳號相關聯。

啟用自我探索

若要啓用自我探索，您必須編輯特殊配置物件 (一般使用者資源)，並新增至允許使用者探索帳號的每個資源的名稱。

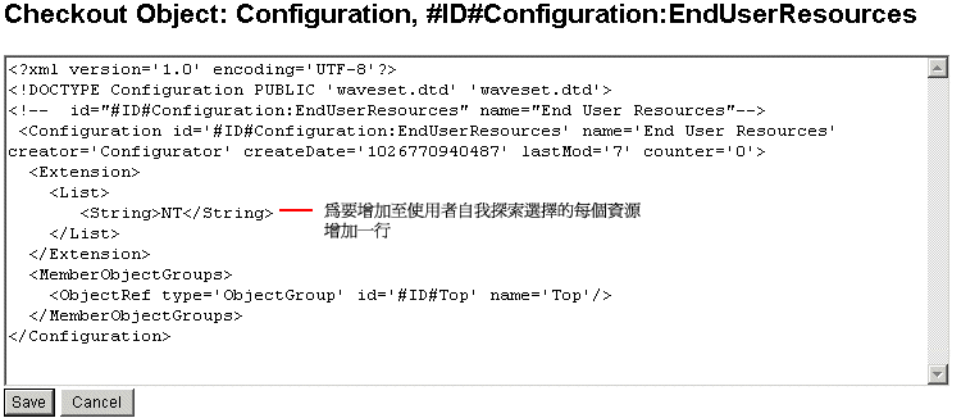
若要啓用自我探索，請執行以下步驟：

1. 編輯 [一般使用者資源] 配置物件。

   如需有關編輯 Identity Manager 配置物件的說明，請參閱第 197 頁的「編輯 Identity Manager 配置物件」。

2. 增加 `<String>`*Resource*`</String>`，其中 *Resource* 與儲存庫中資源物件的名稱相符，如圖 3-14 中所示。

   圖 3-14 一般使用者資源配置物件



3. 按一下 **[儲存]**。

啓用自我探索後，會在 Identity Manager 使用者介面上的 [設定檔] 功能表標籤下方，爲使用者提供一個新的選項 (即 [自我探索])。此區域允許該使用者從可用清單選取資源，然後輸入資源帳號 ID 與密碼，來連結帳號與其 Identity Manager 身份。

備註 管理員也可使用「一般使用者」組織，授權一般使用者存取 Identity Manager 配置物件。請參閱第 226 頁的「一般使用者組織」，以取得詳細資訊。

匿名註冊

匿名註冊功能可讓沒有 Identity Manager 帳號的使用者請求取得帳號。

啟用匿名註冊

匿名註冊功能預設爲停用。

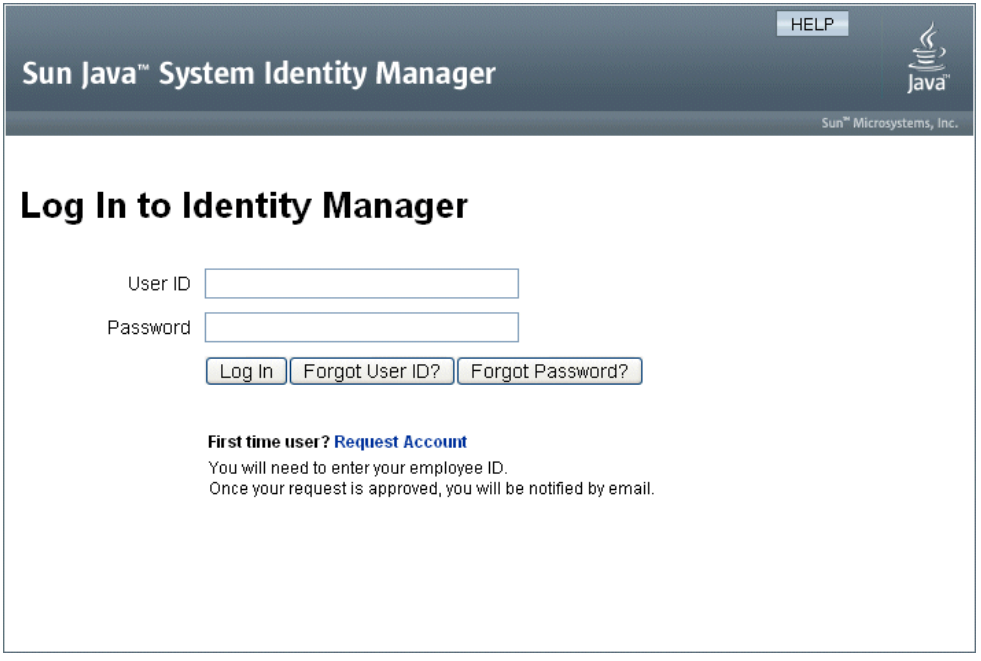
若要啓用匿名註冊功能，請執行以下步驟：

1. 在管理員介面中，按一下 **[配置]**，再按一下 **[使用者介面]**。
2. 在 **[匿名註冊]** 區域中選取 **[啓用]** 選項，然後按一下 **[儲存]**。

當使用者登入使用者介面時，[登入] 頁面會顯示 **[第一次使用嗎？]** 後接 **[申請帳號]** 連結的字樣。

備註 您可自訂**第一次使用嗎？申請帳號**的字樣。請參閱「Identity Manager Technical Deployment Overview」，以取得詳細資訊。

圖 3-15 啓用了 [申請帳號] 連結的 [使用者介面] 頁面



配置匿名註冊

從 [使用者介面] 頁面上的 [匿名註冊] 區域中，您可以配置匿名註冊程序的下列選項：

- **通知範本** - 指定電子郵件範本 ID，以便傳送通知給申請帳號的使用者。
- **需要隱私權政策** - 若選取此選項，則使用者必須先接受隱私權政策，才能申請帳號。此選項預設爲啓用。
- **啓用驗證** - 若選取此選項，則使用者必須先驗證其受僱狀態，才能申請帳號。此選項預設爲啓用。
- **處理啓動 URL** - 輸入 URL 以指定匿名註冊程序將使用的工作流程。
- **啓用通知** - 若選取此選項，則在此帳號建立之後會傳送通知電子郵件給使用者。
- **電子郵件網域** - 輸入用於建構使用者電子郵件地址的電子郵件網域名稱。

在完成時按一下 **[儲存]**。

使用者註冊程序

使用者在登入使用者介面時，按一下 [登入] 頁面上的 **[申請帳號]** 即可申請帳號。

Identity Manager 顯示第一頁註冊頁面 (共兩頁)，在此需提供全名與員工 ID。若 [啓用驗證] 屬性設爲 [是] (預設值)，則必須先驗證這項資訊，使用者才能繼續進行下一頁。

`EndUserLibrary` 中的 `verifyFirstname`、`verifyLastname`、`verifyEmployeeId` 與 `verifyEligibility` 規則，可驗證各屬性的資訊。

備註 您可能需要修改其中一個或多個規則。特別是應修改用於驗證員工 ID 的規則，以使用 Web 服務呼叫或 Java 類別驗證此類資訊。

若停用 [啓用驗證] 屬性，則不會顯示初始註冊頁面。在此情況下，您必須修改 [一般使用者匿名註冊完成] 表單，讓使用者能輸入通常由初始驗證表單擷取的資訊。

Identity Manager 可從 [註冊] 頁面上所提供的資訊產生以下項目：

- 帳號 ID (遵循名字縮寫、姓氏縮寫、員工 ID 的慣例)。
- 使用下列格式的電子郵件地址：

  FirstName.LastName@EmailDomain

  其中，*EmailDomain* 是由匿名註冊配置中的 [電子郵件網域] 屬性所設定的網域。

- 管理員屬性 (idmManager)。您可以修改 `EndUserRuleLibrary:getIdmManager` 規則，以設定此屬性。依預設，會將管理員設爲配置程式。必須在指定爲管理員 (Manager) 的管理員 (Administrator) 核准使用者請求後，才能佈建此帳號。
- 組織屬性。您可以自訂 `EndUserRuleLibrary:getOrganization` 規則，以設定此屬性。依預設，會將使用者指定至組織階層的頂端 (「Top」)。

若使用者在 [註冊] 頁面上所提供的資訊驗證正確無誤，Identity Manager 即會對使用者顯示第二頁 [註冊] 頁面。使用者在此必須輸入密碼與確認密碼。若 [需要隱私權政策] 屬性設爲 [是]，則使用者必須同時選取對應選項，以接受隱私權政策的條款。

使用者按一下 [註冊] 時，Identity Manager 即會顯示確認頁面。若 [啓用通知] 屬性設爲 [是]，則頁面中會指出使用者將在帳號建立後收到電子郵件通知。

標準 [建立使用者] 程序 (包括 `idmManager` 屬性與策略設定所需的核准) 完成後即會建立帳號。

第 4 章

角色與資源

本章討論 Identity Manager 的角色與資源。

本章的資訊分爲以下主題：

瞭解與管理角色

請閱讀本節以瞭解有關在 Identity Manager 中設定角色的資訊。在大型組織中，依角色指定資源可大幅簡化資源管理。

備註 請勿將**角色**與**管理員角色**混淆。角色可用以管理一般使用者對外部資源的存取。另一方面，管理員角色則主要用以管理管理員對內部 Identity Manager 物件 (如使用者、組織與權能) 的存取。

本節中的資訊將討論角色。如需有關管理員角色的資訊，請參閱第 218 頁的「瞭解與管理管理員角色」。

角色是甚麼？

角色是 Identity Manager 物件，可將資源存取權限分組，並以效率極高的方式指定給使用者。角色分爲四種角色類型：

- 商務角色
- IT 角色
- 應用程式
- 資產

商務角色可將組織中執行類似作業的人員執行其工作責任時所需的存取權限，進行分組。一般而言，商務角色代表使用者工作職能。例如在金融機構中，商務角色可能相當於銀行行員、貸款員、分行經理、辦事員、會計人員或行政助理等職務類別。

IT 角色、**應用程式**與**資產**可將資源軟體權利文件劃分爲不同群組。若要提供一般使用者對資源的存取權，請將 IT 角色、應用程式與資產指定給商務角色，讓使用者能夠存取他們在執行工作時所需的資源。IT 角色包含一組特定的應用程式、資產和 (或) 資源，其中包含這些指定的資源所適用的特定軟體權利文件。IT 角色亦可包含其他 IT 角色。

備註 角色類型在 Identity Manager 8.0 版中是新的概念。若您的組織從舊版 Identity Manager 升級至 8.0 版，您的舊有角色會匯入爲 IT 角色。如需更多資訊，請參閱第 119 頁的「管理在 8.0 版之前的版本中建立的角色」。

「IT 角色」、「應用程式」和「資產」可以是**必要**、**條件式**或**選擇性項目**。

- 對於一般使用者一律會指定必要角色。
- 條件式角色的條件則必須計算爲 true，才會指定該角色。
- 選擇性角色可經個別請求，在核准後指定給一般使用者。

必要、條件式與選擇性角色可讓商務角色設計者定義內含角色的概略性存取權以遵守法規，同時讓一般使用者的管理員仍可保有微調一般使用者存取權限的彈性。指定爲條件式或選擇性角色的使用者仍可共用相同的指定商務角色，但會有不同的指定存取權限。透過此方法，即不需在每次組織的存取需求有所變動時定義新的商務角色 (一般將此問題稱爲 **「角色擴張」**)。

角色類型運作

下列討論將說明如何有效使用角色類型。如需角色類型的說明，請參閱上一節。

管理在 8.0 版之前的版本中建立的角色

從舊版 Identity Manager 升級至 8.0 版的組織，其舊有角色會自動轉換成 IT 角色。這些 IT 角色仍會直接指定給使用者。在升級程序中，並不會將舊有角色指定給角色所有者。但角色所有者可於稍後指定 (如需有關角色所有者的資訊，請參閱第 131 頁)。

依預設，升級至 8.0 版的組織可直接將 IT 角色與商務角色指定給使用者 (請參閱圖 4-2 (第 122 頁))。

具有舊有角色的組織應考慮根據下節所列的指示建立新的角色。

使用角色類型設計彈性角色

IT 角色、應用程式與資產皆爲角色設計者的設計基礎。這三種角色類型可搭配運用，以組成使用者軟體權利文件 (或**存取權限**)。接著會把 IT 角色、應用程式與資產指定給商務角色。

設計商務角色

在 Identity Manager 中可爲一名使用者指定一個或多個角色，也可以不指定角色。在 Identity Manager 8.0 推出角色類型功能後，建議您只將商務角色直接指定給使用者。事實上，依預設您無法直接將任何其他角色類型指定給使用者，除非您的組織已安裝 8.0 之前的 Identity Manager 版本，並至少已升級至 8.0 版。您可以變更此預設限制，只要修改角色配置物件即可 (第 155 頁)。

若要減少複雜性，即不可使用巢式商務角色，也就是說，商務角色中不可包含其他商務角色。此外，商務角色亦不可直接包含資源與資源群組。資源與資源群組應先指定給 IT 角色或應用程式，再轉而指定給一個或多個商務角色。

設計 IT 角色

IT 角色可包含應用程式、資產與其他 IT 角色。IT 角色亦可包含資源與資源群組。

建立及管理 IT 角色的人，應該是組織的 IT 人員，或瞭解軟體權利文件 (啓用資源內特定權限時所需) 的資源所有者。

設計應用程式與資產

應用程式與資產這兩種角色類型的用途是代表常用的商業術語，以說明一般使用者工作時所需的資源。例如，應用程式角色可命名爲「客戶支援工具」或「企業內部網路 HR 工具管理員」。

- 應用程式不可包含角色，但可包含資源與資源群組。應用程式亦可定義特定的軟體權利文件，而將存取權限定於內含資源上的特定應用程式。
- 資產 (通常) 爲需要手動佈建的未連線或非數位資源 (如行動電話與可攜式電腦)。因此，資產不可包含角色、資源或資源群組。

應用程式與資產應指定給商務角色與 IT 角色。

備註 以下是應指定給角色管理員的一或多項權能：

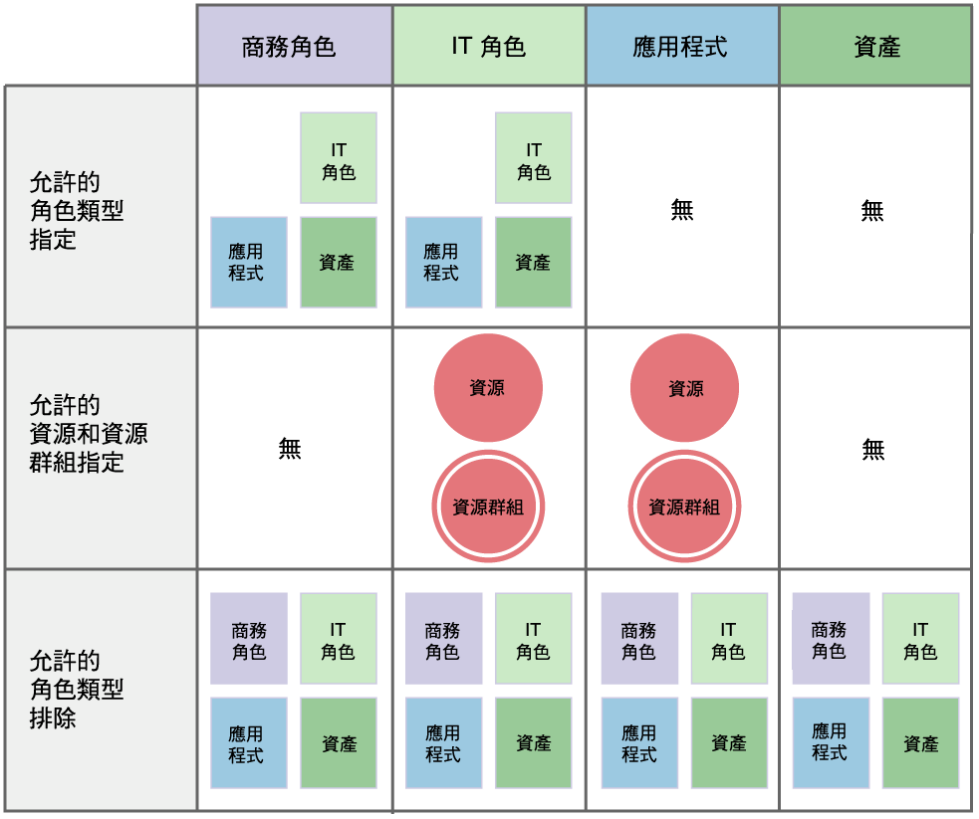
- 資產管理員
- 應用程式管理員
- 商務角色管理員
- IT 角色管理員

詳細資訊請參閱第 217 頁的「指定權能」。

角色類型摘要

圖 4-1 顯示哪些角色類型、資源與資源群組可指定給下列四種角色類型。圖中也顯示，您對四種角色類型皆可指定角色類型排除 (角色排除在第 125 頁有相關說明)。

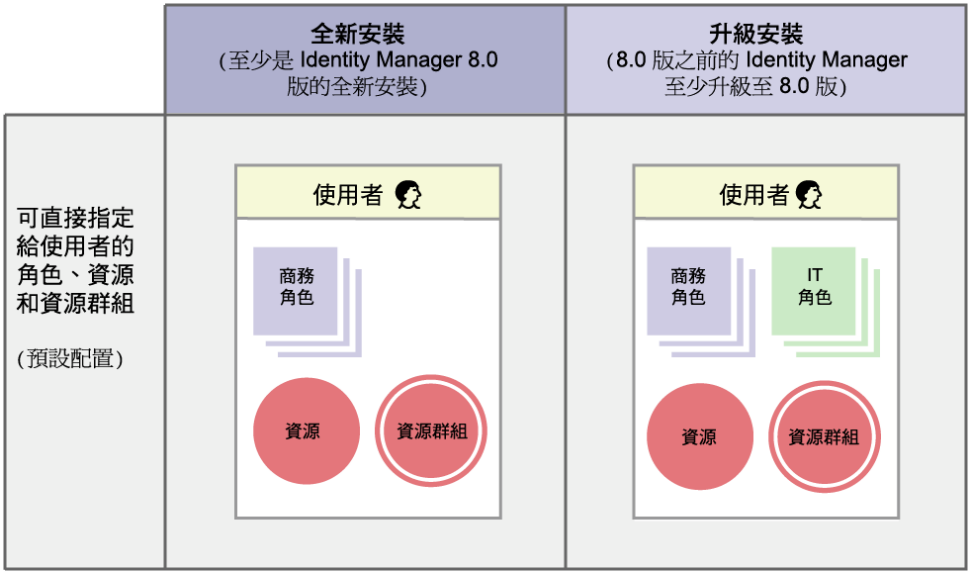
圖 4-1　　商務角色、IT 角色、應用程式與資產角色類型



選擇性、條件式與必要的內含角色 (第 118 頁) 可讓您有更大的彈性。彈性角色定義可減少您的組織所需管理的角色總數。

圖 4-2 顯示，若 8.0 之前的 Identity Manager 版本至少已升級至 8.0 版，即可直接指定商務角色與 IT 角色給使用者。升級時會將舊有角色轉換爲 IT 角色，且爲確保向下相容性，可直接將 IT 角色指定給使用者。若未升級 8.0 之前的 Identity Manager 版本，則只有直接將商務角色指定給使用者。

圖 4-2　可直接指定給使用者的角色與資源



建立角色

本節說明如何建立角色。如需有關設計角色的提示，請參閱第 119 頁的「使用角色類型設計彈性角色」。

建立或編輯角色時，Identity Manager 會啓動 ManageRole 工作流程。這個工作流程會在儲存庫中儲存新的或更新的角色，並讓您在建立或儲存角色之前插入核准或其他動作。

填寫建立角色表單

若要建立角色，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[角色]**。

   [角色] 頁面 ([列出角色] 標籤) 會隨即開啓。

2. 按一下頁面底部的 **[新增]**。

   [建立 IT 角色] 頁面會隨即開啓。若要建立其他類型的角色，請使用 **[類型]** 下拉式功能表。

3. 填寫 **[身份]** 標籤上的表單欄位。

   圖 4-3 (第 124 頁) 顯示 **[身份]** 標籤。

4. 填寫 **[資源]** 標籤上的表單欄位 (如果有)。如需填寫此標籤上各欄位的說明，請參閱線上說明以及第 125 頁的「指定資源與資源群組」。

   如需爲角色設定延伸屬性值的說明，請參閱第 127 頁的「編輯指定的資源屬性值」。

   圖 4-4 (第 126 頁) 顯示 **[資源]** 標籤。

5. 填寫 **[角色]** 標籤上的表單欄位 (如果有)。如需填寫此標籤上各欄位的說明，請參閱線上說明以及第 129 頁的「指定角色與角色排除」。

   圖 4-6 (第 130 頁) 顯示 **[角色]** 標籤。

6. 填寫 **[安全性]** 標籤上的表單欄位。如需填寫此標籤上各欄位的說明，請參閱線上說明以及第 131 頁的「指定角色所有者與角色核准人」和第 133 頁的「指定通知」。

   圖 4-7 (第 132 頁) 顯示 **[安全性]** 標籤。

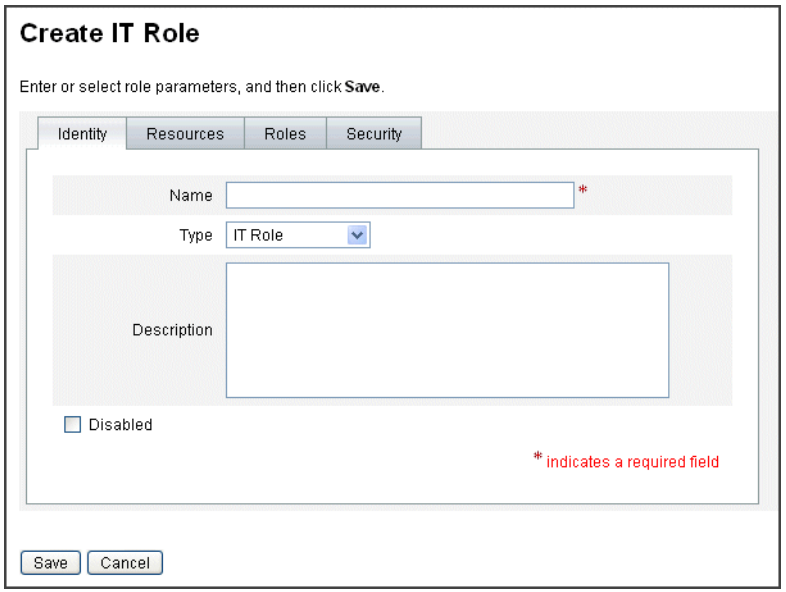
7. 按一下頁面底部的 **[儲存]**。

輸入角色的名稱與描述

在 [建立角色] 表單的 **[身份]** 標籤上，輸入角色的名稱與描述。若要建立新的角色，請使用 **[類型]** 下拉式功能表選取您要建立的角色類型。

圖 4-3 顯示 [建立角色] 表單的 **[身份]** 標籤。如需使用此表單的說明，請參閱線上說明。

圖 4-3　　[建立角色] 標籤式表單的 [身份] 部分



指定資源與資源群組

您可透過 [建立角色] 表單的 **[資源]** 標籤，直接指定資源與資源群組給 IT 角色與應用程式角色。本章稍後將有資源的相關說明 (第 161 頁)。資源群組在第 171 頁的「資源群組」一節中有相關說明。

- 您無法將資源和資源群組直接指定給商務角色，因爲僅可將角色指定給商務角色。
- 您也無法將資源和資源群組指定給資產角色，因爲資產角色會保留給需要手動佈建的未連線或非數位資源。

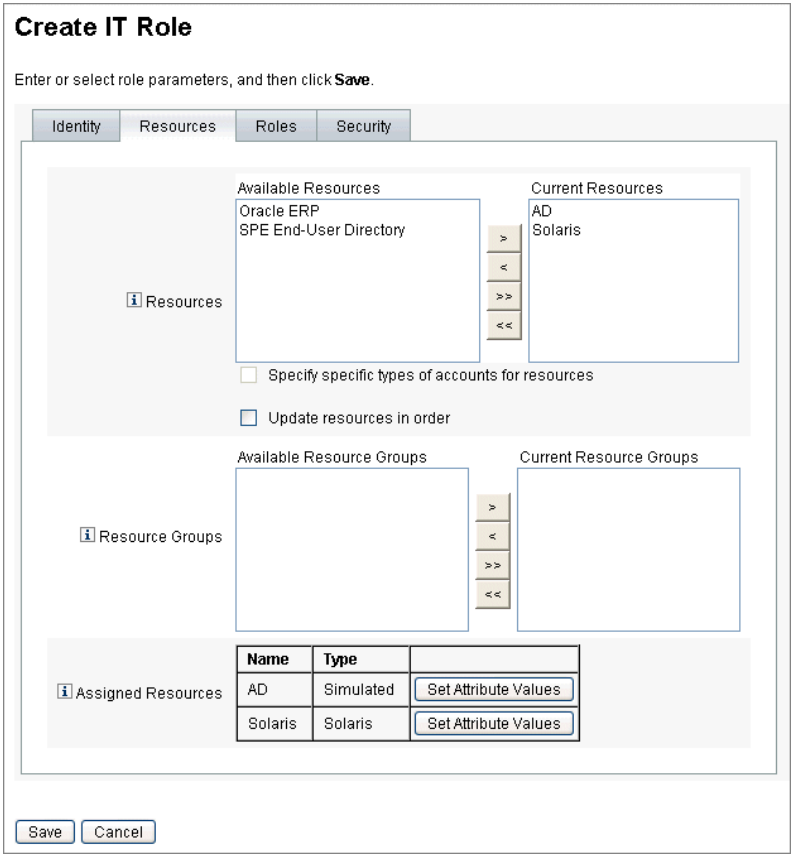
此程序說明在填寫 [建立角色] 表單時，如何指定資源與資源群組給角色。若要開始使用，請參閱第 123 頁的「填寫建立角色表單」。

若要填寫 [資源] 標籤，請執行以下步驟：

1. 按一下 [建立角色] 頁面中的 **[資源]** 標籤。
2. 若要指定資源，請在 **[可用資源]** 欄中選取資源，再按一下箭頭按鈕，將資源移至 **[目前資源]** 欄。
3. 若指定了多個資源，即可指定更新資源的順序： 選取 **[依順序更新資源]** 核取方塊，並使用 + 和 - 按鈕變更 **[目前資源]** 欄中資源的順序。
4. 若要將資源群組指定給此角色，請在 **[可用資源群組]** 欄中選取資源群組，再按一下箭頭按鈕，將資源群組移至 **[目前資源群組]** 欄。資源群組是一組資源的集合，可提供其他方式以指定建立及更新資源帳號的順序。
5. 若要爲此角色根據資源指定帳號屬性，請在 **[指定的資源]** 區段中，按一下 **[設定屬性值]**。詳細資訊請參閱第 127 頁的「編輯指定的資源屬性值」。
6. 按一下 **[儲存]** 以儲存角色，或按一下 **[身份]**、**[角色]** 或 **[安全性]** 標籤，以繼續進行角色建立程序。

圖 4-4 顯示 [建立角色] 表單的 **[資源]** 標籤。

圖 4-4 [建立角色] 標籤式表單的 [資源] 部分



編輯指定的資源屬性值

使用 **[指定的資源]** 表格，可對獲得指定角色的資源設定或修改資源屬性值。資源可就角色逐一定義不同的屬性值。按一下 **[設定屬性值]** 按鈕，可開啓 [資源帳號屬性] 頁面。

圖 4-5 (第 128 頁) 顯示 [資源帳號屬性] 頁面。

在此頁面中，您可以爲每個屬性指定新值，並決定屬性值的設定方式。Identity Manager 可讓您直接設定值，或使用規則設定值。它也可提供許多選項，用以置換現有值或合併新值與現有值。

如需有關資源屬性值的一般資訊，請參閱第 170 頁的「使用帳號屬性」。

選取用於建立各資源帳號屬性值的選項：

- **置換的值** - 選取以下任一選項：
  - **無** - 預設的選項。未建立任何值。
  - **規則** - 使用規則來設定值。如果您選取此選項，則必須從清單中選取規則名稱。
  - **文字** - 使用指定的文字來設定值。如果您選取此選項，則必須在相鄰的 **[文字]** 欄位中輸入文字。
- **設定方式** - 選取以下任一選項：
  - **預設值** - 將規則或文字設爲預設的屬性值。使用者可以變更或置換該值。
  - **設定值** - 依規則或文字指定的方式設定屬性值。系統將設定值，並置換使用者所做的任何變更。
  - **與值合併** - 將目前的屬性值與依規則或文字所指定的值合併。
  - **與值合併，清除現有** - 移除目前的屬性值，並將值設爲由這個角色和其他指定角色所指定值的合併值。
  - **從值移除** - 移除屬性值中由規則或文字所指定的值。
  - **授權設定值** - 依規則或文字所指定的方式設定屬性值。系統將設定值，並置換使用者所做的任何變更。如果您移除角色，則新值會是空值，即使此值之前爲屬性值。

- **授權與值合併** - 將目前的屬性值與依規則或文字所指定的值合併。如果移除角色，則新屬性值會是空值，即使該屬性先前具有相應值。

  對於多值屬性，您必須編輯儲存庫中的角色物件，指出其包含逗號分隔值 (CSV) 字串，例如：

  ```
  <RoleAttribute name='attrs role:Database Table:attrs' csv='true'>
  ```

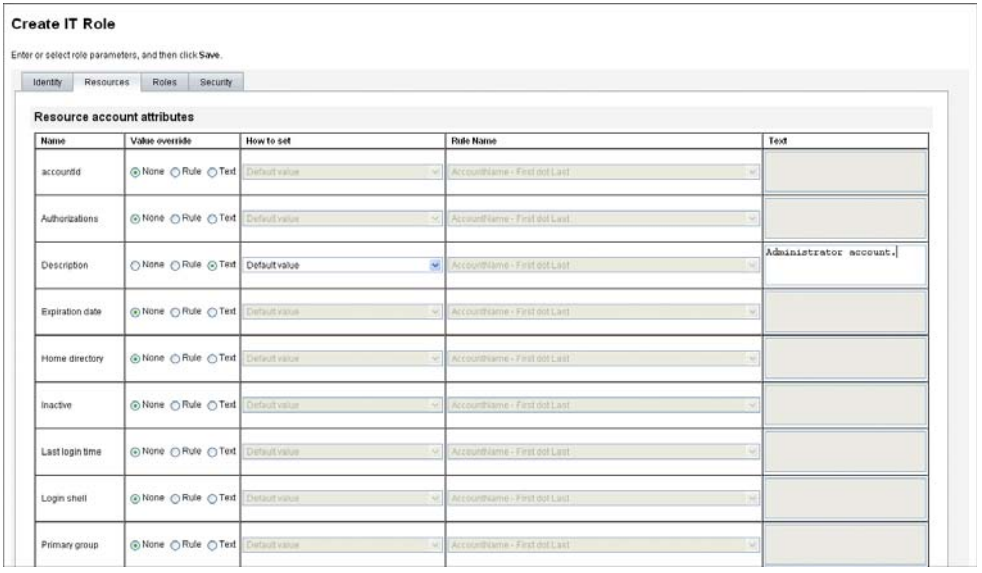
- **授權與值合併，清除現有** - 移除目前的屬性值，並將值設爲由這個角色和其他指定角色所指定值的合併值。如果移除角色，則會清除該角色指定的屬性值，即使該屬性早已有此值亦然。

- **規則名稱** - 如果您在 [置換的值] 區域中選取 [規則]，則從清單中選取規則。
- **文字** - 如果您在 [置換的值] 區域中選取 [文字]，則輸入要增加至屬性值、從屬性值中刪除或當成屬性值使用的文字。

按一下 **[確定]** 儲存變更，並返回 [建立角色] 或 [編輯角色] 頁面。

圖 4-5 顯示 [資源帳號屬性] 頁面，此頁面可讓您爲獲得指定角色的資源設定延伸屬性值。

圖 4-5 [資源帳號屬性] 頁面



指定角色與角色排除

您可以使用 [建立角色] 表單的 **[角色]** 標籤，將角色指定給商務角色與 IT 角色。指定的角色會隨即加入 **[內含角色]** 表格中。

- 您無法將角色指定給應用程式角色與資產角色。
- 您無法將商務角色指定給任何角色類型。

您可以使用 [建立角色] 表單的 **[角色]** 標籤，將角色排除指定給四種角色類型。若具有角色排除的角色已指定給某使用者，即無法將排除的角色指定給該名使用者。角色排除應增加至 **[角色排除]** 表格中。

此程序說明在填寫 [建立角色] 表單時，如何指定一個或多個角色給角色。若要開始使用，請參閱第 123 頁的「填寫建立角色表單」。

若要填寫 [角色] 標籤，請執行以下步驟：

1. 按一下 [建立角色] 頁面中的 **[角色]** 標籤。
2. 按一下 **[內含角色]** 區段中的 **[增加]**。

   此標籤會更新並顯示 **[尋找要包含的角色]** 表單。
3. 搜尋要指定給此角色的一個或多個角色。請先從**必要**角色開始 (條件式與選擇性角色將於稍後增加)。

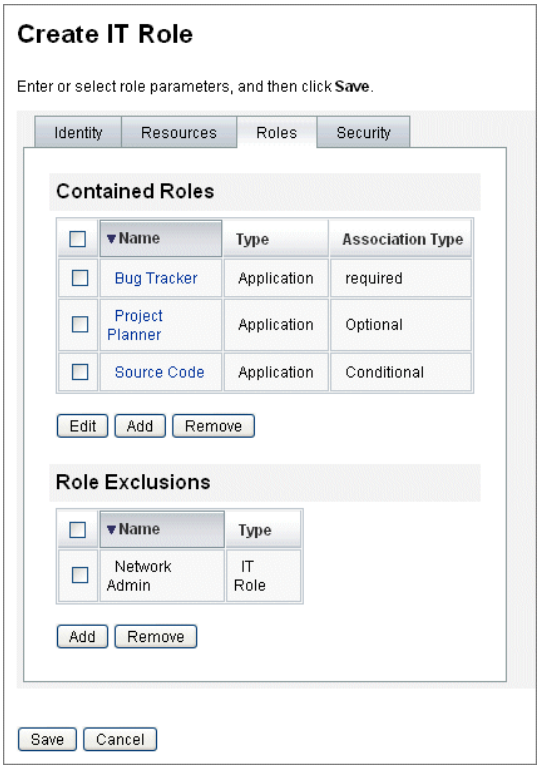
   如需使用搜尋表單的說明，請參閱第 135 頁。商務角色無法內嵌於或指定給其他角色類型。
4. 使用核取方塊選取要指定的角色，然後按一下 **[增加]**。

   此標籤會更新並顯示 **[增加內含角色]** 表單。
5. 從 **[關聯類型]** 下拉式功能表中，視需要選取 **[必要]**、**[條件式]** 或 **[選擇性]**。

   按一下 **[確定]**。
6. 重複前述四個步驟以增加條件式角色 (如果需要)。再次重複前述四個步驟以增加選擇性角色 (如果需要)。
7. 按一下 **[儲存]** 以儲存角色，或按一下 **[身份]**、**[資源]** 或 **[安全性]** 標籤，以繼續進行角色建立程序。

圖 4-6 顯示 [建立角色] 表單的 **[角色]** 標籤。如需使用此表單的說明，請參閱線上說明。

圖 4-6 [建立角色] 標籤式表單的 [角色] 部分



指定角色所有者與角色核准人

指定爲**所有者**與**核准人**的角色。只有角色所有者可授權變更用以定義角色的參數，且只有角色核准人可授權指定角色給一般使用者。

角色所有者同時也會是業務所有者，負責處理透過角色指定的基礎資源帳號權限。若管理員對角色進行變更，角色所有者必須核准變更後，才可執行這些變更。此功能可避免管理員在業務所有者不知悉且未核准的情況下，擅自變更角色。但是，若已停用角色配置物件中的變更核准，則不需要角色所有者的核准，便可執行變更。

除了核准角色變更外，未經角色所有者的核准，不可啓用、停用或刪除角色。

您可直接將所有者與核准人增加至角色中，或使用角色指定規則動態加入。在 Identity Manager 中，您可以建立不具所有者與核准人的角色 (但不建議這麼做)。

備註 角色指定規則具有 `RoleUserRule` 的 authType。如需建立自訂的角色指定規則，請參閱三項預設角色指定規則物件，並將其做爲範例：

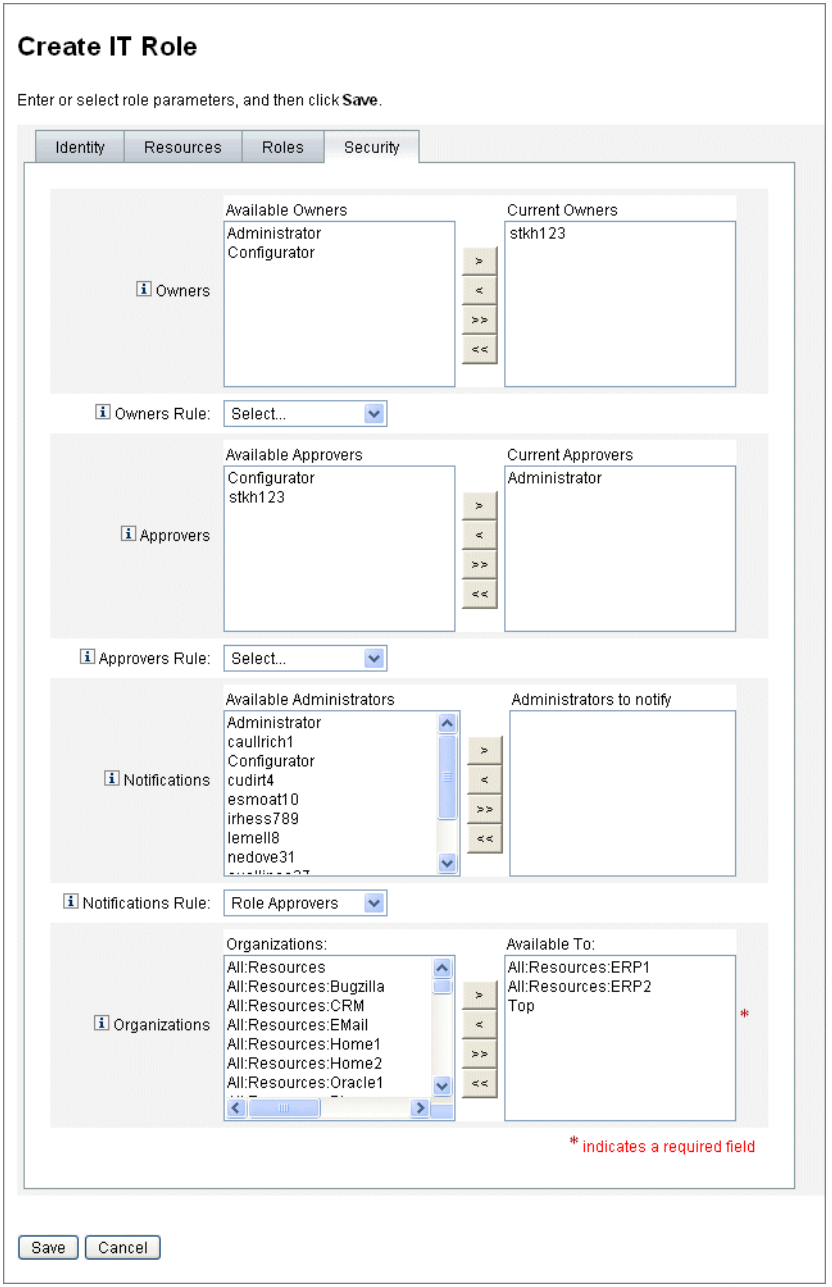
- 角色核准人
- 角色通知
- 角色所有者

所有者與核准人在有工作項目須由其核准時，會收到電子郵件通知。變更核准工作項目與核准工作項目在「啓動變更核准與核准工作項目」一節中有相關討論 (第 133 頁)。

所有者與核准人可透過 [建立角色] 表單中的 [安全性] 標籤增加至角色中。

圖 4-7 (第 132 頁) 顯示 [建立角色] 表單的 **[安全性]** 標籤。如需使用此表單的說明，請參閱線上說明。

圖 4-7 [建立角色] 標籤式表單的 [安全性] 部分



指定通知

指定角色給使用者時，可傳送**通知**給一個或多個管理員。

指定通知收件者並非必要動作。若您決定在角色指定給使用者時無需經過核准，則可以選擇通知管理員。或者，您可以指定一名管理員做爲核准人，並指定另一名管理員做爲核准後的通知收件者。

如同所有者與核准人，通知亦可直接增加至角色中，或使用角色指定規則動態加入。將角色指定給使用者時，通知收件者即會收到電子郵件通知。但此時不會建立工作項目，因爲不需進行核准。

通知可透過 [建立角色] 表單上的 [安全性] 標籤增加至角色中。圖 4-7 (第 132 頁) 顯示 [建立角色] 表單的 **[安全性]** 標籤。

啟動變更核准與核准工作項目

對角色進行變更時，角色所有者會收到**變更核准**電子郵件、**變更通知**電子郵件，或不會收到郵件。將角色指定給使用者時，角色核准人會收到角色**核准**電子郵件。

依預設，角色所有者在其擁有的角色有所變更時，會收到變更核准電子郵件。但此運作方式可就角色類型逐一配置。例如，您可以選擇啓用商務角色與 IT 角色的變更核准，而啓用應用程式與資產角色的變更通知。

如需有關啓用及停用變更核准與變更通知電子郵件的說明，請參閱第 158 頁的「啓用及停用變更核准與變更通知工作項目」。

以下是變更核准與變更通知的運作方式：

- 若啓用**變更核准**，則在管理員變更角色時將會產生工作項目，並傳送核准電子郵件給角色所有者。角色所有者必須核准工作項目，才可進行變更。您也可以委託變更核准工作項目。詳細資訊請參閱第 233 頁的「核准」。

  若停用變更核准，則不會產生任何工作項目，且不會傳送變更核准電子郵件給角色所有者。

- 若啓用**變更通知**，則在管理員變更角色時，變更將會立即生效，並傳送通知電子郵件給角色所有者。

  若停用變更通知，則不會傳送任何通知給角色所有者。

將角色指定給使用者時，角色核准人會收到角色**核准**電子郵件。在 Identity Manager 中無法停用角色核准電子郵件。

以下是角色核准的運作方式：

- 將角色指定給使用者時會產生工作項目，並傳送核准電子郵件給角色核准人。角色核准人必須核准工作項目，才會將角色指定給使用者。

您也可以委託變更核准與核准工作項目。如需有關委託工作項目的更多資訊，請參閱第 230 頁的「委託工作項目」。

編輯與管理角色

大部分的角色編輯與角色管理作業皆可透過 **[尋找角色]** 與 **[列出角色]** 子標籤執行；這些子標籤位於主功能表的 **[角色]** 標籤下。

本節包含以下主題：

搜尋角色

使用 **[尋找角色]** 標籤，可搜尋符合您所指定之搜尋條件的角色。

使用 [尋找角色] 標籤，可讓您根據角色所有者與核准人、指定的帳號類型、內含角色等各種條件搜尋角色。

如需有關尋找獲得指定角色的使用者的資訊，請參閱第 153 頁。

若要開啓 [尋找角色] 標籤，請執行以下步驟：

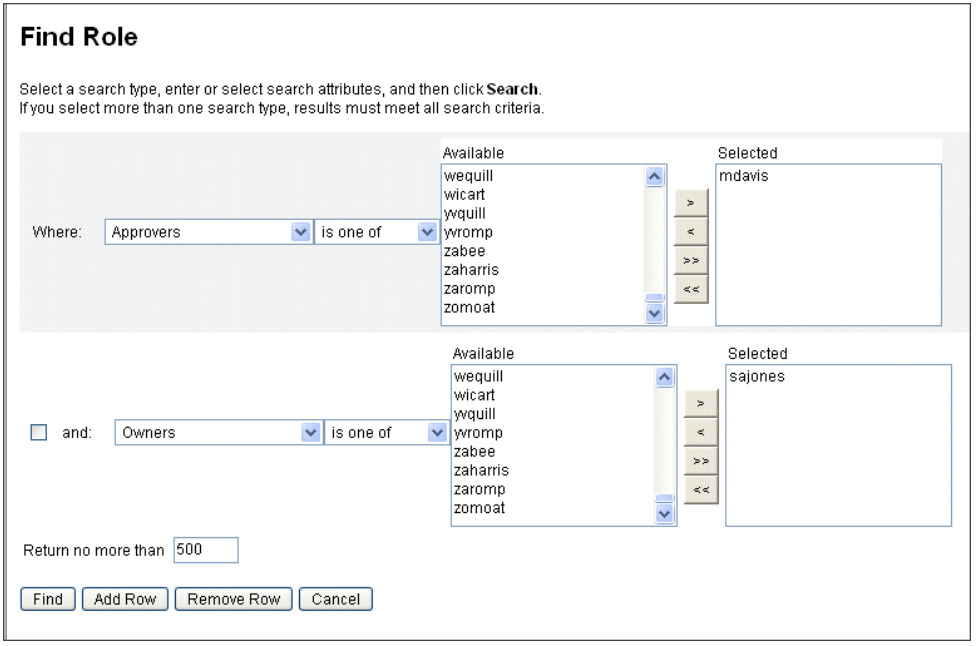
1. 在管理員介面中，按一下 **[角色]** 標籤。

   [列出角色] 標籤會隨即開啓。

2. 按一下 **[尋找角色]** 輔助標籤。

   圖 4-8 顯示 **[尋找角色]** 標籤。如需使用此表單的說明，請參閱線上說明。

圖 4-8　　[尋找角色] 標籤



使用下拉式功能表可定義搜尋的參數。按一下 **[增加列]** 按鈕可增加其他參數。

檢視角色

使用 [列出角色] 標籤可檢視角色。使用 [列出角色] 頁面頂端的篩選欄位，依名稱或角色類型尋找角色。篩選並不區分大小寫。

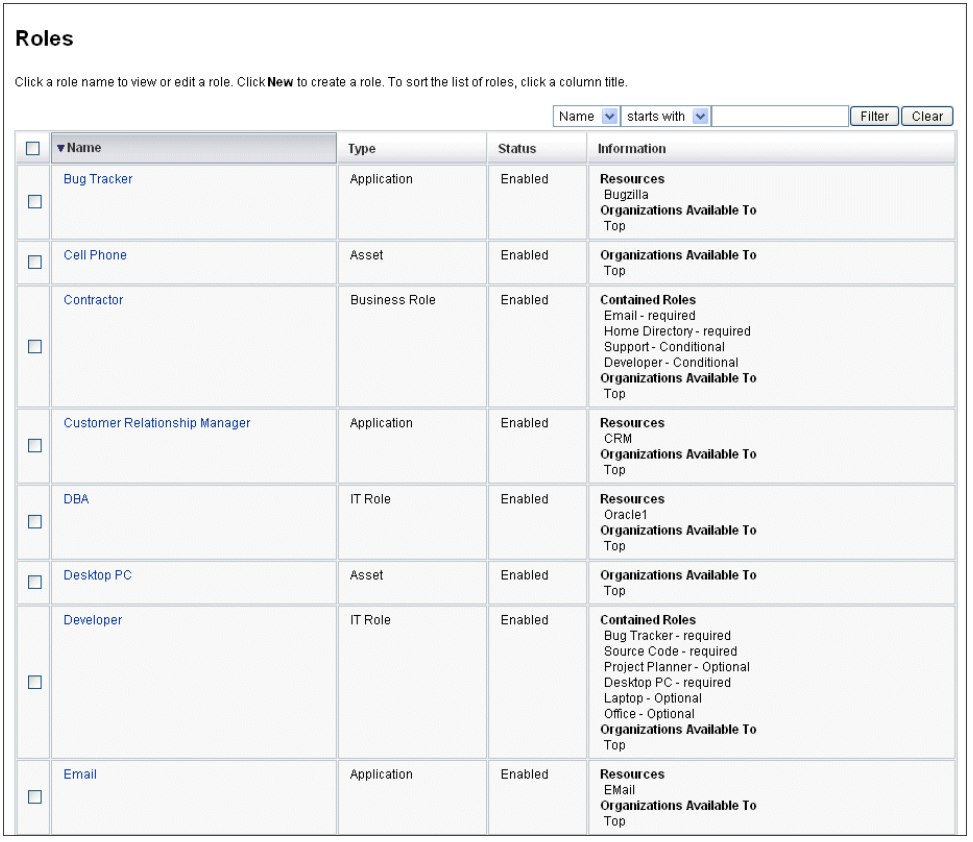
若要開啓 [列出角色] 標籤，請執行以下步驟：

1. 在管理員介面中，按一下 **[角色]** 標籤。

   [列出角色] 標籤會隨即開啓。

圖 4-9 (第 136 頁) 顯示 **[列出角色]** 標籤。如需使用此表單的說明，請參閱線上說明。

圖 4-9 [列出角色] 標籤



Roles

Click a role name to view or edit a role. Click **New** to create a role. To sort the list of roles, click a column title.

Name | starts with | Filter | Clear

	▼Name	Type	Status	Information
☐	Bug Tracker	Application	Enabled	**Resources** Bugzilla **Organizations Available To** Top
☐	Cell Phone	Asset	Enabled	**Organizations Available To** Top
☐	Contractor	Business Role	Enabled	**Contained Roles** Email - required Home Directory - required Support - Conditional Developer - Conditional **Organizations Available To** Top
☐	Customer Relationship Manager	Application	Enabled	**Resources** CRM **Organizations Available To** Top
☐	DBA	IT Role	Enabled	**Resources** Oracle1 **Organizations Available To** Top
☐	Desktop PC	Asset	Enabled	**Organizations Available To** Top
☐	Developer	IT Role	Enabled	**Contained Roles** Bug Tracker - required Source Code - required Project Planner - Optional Desktop PC - required Laptop - Optional Office - Optional **Organizations Available To** Top
☐	Email	Application	Enabled	**Resources** EMail **Organizations Available To** Top

編輯角色

使用 **[列出角色]** 或 **[尋找角色]** 標籤，搜尋您要編輯的角色。若您對角色進行變更，且變更核准設定爲 True，角色所有者必須核准變更後，才可執行這些變更。

如需有關以角色變更更新使用者的資訊，請參閱第 148 頁的「更新指定給使用者的角色」。

若要編輯角色，請執行以下步驟：

1. 依照第 135 頁或第 136 頁上的說明，搜尋您要編輯的角色。
2. 按一下您要編輯之角色的名稱。

   [編輯角色] 頁面會隨即開啓。
3. 依需要編輯角色。如需填寫 **[身份]**、**[資源]**、**[角色]** 與 **[安全性]** 標籤的說明，請參閱「填寫建立角色表單」一節中的步驟 (第 123 頁)。

   按一下 **[儲存]**。[確認角色變更] 頁面會隨即開啓。
4. 若此角色已指定給使用者，您可以選取何時要以角色變更更新使用者。詳細資訊請參閱第 148 頁的「更新指定給使用者的角色」。
5. 按一下 **[儲存]** 儲存變更。

複製角色

若要複製角色，請執行以下步驟：

1. 依照第 135 頁或第 136 頁上的說明，搜尋您要編輯的角色。
2. 按一下您要複製之角色的名稱。

   [編輯角色] 頁面會隨即開啓。
3. 在 **[名稱]** 欄位中輸入新的名稱，然後按一下 **[儲存]**。

   [角色：建立或重新命名？] 頁面會隨即開啓。
4. 按一下 **[建立]** 以複製角色。

指定角色給其他角色

Identity Manager 在角色指定方面的需求，在第 118 頁的「角色是甚麼？」與第 119 頁的「角色類型運作」中有相關說明。您在指定角色前，應先瞭解這項資訊。

Identity Manager 可在父系角色的角色所有者核准時，變更角色的角色指定。

若要指定角色給其他角色，請執行以下步驟：

1. 搜尋將被指定一個或多個**內含**角色的商務角色或 IT 角色 (角色只能指定給商務角色與 IT 角色)。請依照第 135 頁或第 136 頁的說明搜尋角色。
2. 按一下商務角色或 IT 角色加以開啓。

   [編輯角色] 頁面會隨即開啓。
3. 按一下 [編輯角色] 頁面中的 **[角色]** 標籤。
4. 按一下 **[內含角色]** 區段中的 **[增加]**。

   此標籤會更新並顯示 **[尋找要包含的角色]** 表單。
5. 搜尋要指定給此角色的一個或多個角色。請先從**必要**角色開始 (條件式與選擇性角色將於稍後增加)。

   如需使用搜尋表單的說明，請參閱第 135 頁。商務角色無法內嵌於或指定給其他角色類型。
6. 使用核取方塊選取要指定的角色，然後按一下 **[增加]**。

   此標籤會更新並顯示 **[增加內含角色]** 表單。
7. 從 **[關聯類型]** 下拉式功能表中，視需要選取 **[必要]**、**[條件式]** 或 **[選擇性]**。

   按一下 **[確定]**。
8. 重複前述四個步驟以增加條件式角色 (如果需要)。再次重複前述四個步驟以增加選擇性角色 (如果需要)。
9. 按一下 **[儲存]** 以開啓 [確認角色變更] 頁面。

   [確認角色變更] 頁面會隨即開啓。
10. 在 **[更新指定的使用者]** 區段中，選取 **[更新指定的使用者]** 功能表選項。詳細資訊請參閱第 148 頁的「更新指定給使用者的角色」。
11. 按一下 **[儲存]**，儲存您的角色指定。

從角色中移除角色

Identity Manager 可在父系角色的角色所有者核准時，移除其他角色的內含角色。使用者收到角色更新之後，就會移除使用者的角色(詳細資訊請參閱第 148 頁的「更新指定給使用者的角色」)。一旦移除角色後，使用者便失去該角色所賦予的權利。

- 如需有關移除指定給一或多名使用者的角色的資訊，請參閱第 154 頁的「移除指定給使用者的角色」。
- 如需有關停用角色的資訊，請參閱第 140 頁的「啓用及停用角色」。
- 如需有關從 Identity Manager 刪除角色的資訊，請參閱第 141 頁的「刪除角色」。

若要移除指定給其他角色的角色，請執行以下步驟：

1. 搜尋您要從中移除角色的商務角色或 IT 角色。請依照第 135 頁或第 136 頁的說明搜尋角色。
2. 按一下角色加以開啓。

   [編輯角色] 頁面會隨即開啓。
3. 按一下 [編輯角色] 頁面中的 **[角色]** 標籤。
4. 在 **[內含角色]** 區段中，選取您要移除之角色旁的核取方塊，然後按一下 **[移除]**。選取多個核取方塊可移除多個角色。

   表格會更新以顯示剩餘內含角色。
5. 按一下 **[儲存]**。

   [確認角色變更] 頁面會隨即開啓。
6. 在 **[更新指定的使用者]** 區段中，選取 **[更新指定的使用者]** 功能表選項。詳細資訊請參閱第 148 頁的「更新指定給使用者的角色」。
7. 按一下 **[儲存]** 以確認變更。

啟用及停用角色

您可透過 **[列出角色]** 標籤啓用及停用角色。角色狀態會顯示在 **[狀態]** 欄中。按一下 **[狀態]** 欄標頭，可依角色狀態排序表格。

停用的角色不會出現在 [建立使用者]/[編輯使用者] 表單的 **[角色]** 標籤中，且無法直接指定給使用者。您可以將內含已停用角色的角色指定給使用者，但無法指定已停用的角色。

已獲得指定角色的使用者若稍後停用角色，並不會失去其權利。角色停用僅會封鎖**未來進行指定角色**的動作。

停用與重新啓用角色，需要角色所有者的權限。

啓用或停用指定給使用者的角色時，Identity Manager 會提示您更新這些使用者。如需更多資訊，請參閱第 148 頁的「更新指定給使用者的角色」。

若要啓用/停用角色，請執行以下步驟：

1. 依照第 135 頁或第 136 頁的說明，搜尋您要刪除的角色。
2. 按一下需要啓用或停用之角色旁的核取方塊。
3. 按一下 [角色] 表格底部的 **[啓用]** 或 **[停用]**。

   [啓用角色] 或 **[停用角色]** 確認頁面會隨即開啓。
4. 按一下 **[確定]** 以啓用或停用角色。

刪除角色

本節說明從 Identity Manager 刪除角色的程序。

- 如需有關移除指定給其他角色的角色的資訊，請參閱第 139 頁的「從角色中移除角色」。
- 如需有關移除指定給一或多名使用者的角色的資訊，請參閱第 154 頁的「移除指定給使用者的角色」。

若刪除目前指定給使用者的角色，Identity Manager 會在您嘗試儲存角色時禁止刪除作業。您必須取消指定 (或重新指定) 原先獲得指定角色的所有使用者，Identity Manager 才可刪除角色。同時還必須從所有其他角色中移除該角色。

Identity Manager 需要角色所有者的核准，才可刪除角色。

若要刪除角色，請執行以下步驟：

1. 依照第 135 頁或第 136 頁的說明，搜尋您要刪除的角色。
2. 選取您要刪除之每個角色旁的核取方塊。
3. 按一下 **[刪除]**。

   [刪除角色] 確認頁面會隨即顯示。
4. 按一下 **[確定]** 以刪除角色。

指定資源或資源群組給角色

Identity Manager 在資源與資源群組指定方面的需求，在第 118 頁的「角色是甚麼？」與第 119 頁的「角色類型運作」中有相關說明。您在指定資源給角色前，應先瞭解這項資訊。

Identity Manager 可在角色所有者核准時，變更角色的資源與資源群組指定。

若要指定資源給角色，請執行以下步驟：

1. 搜尋要增加資源或資源群組的 IT 角色或應用程式。如需有關如何搜尋角色的說明，請參閱第 135 頁或第 136 頁。
2. 按一下角色加以開啓。
3. 按一下 [編輯角色] 頁面中的 **[資源]** 標籤。
4. 若要指定資源，請在 **[可用資源]** 欄中選取資源，再按一下箭頭按鈕，將資源移至 **[目前資源]** 欄。
5. 若指定了多個資源，即可指定更新資源的順序： 選取 **[依順序更新資源]** 核取方塊，並使用 + 和 - 按鈕變更 **[目前資源]** 欄中資源的順序。
6. 若要將資源群組指定給此角色，請在 **[可用資源群組]** 欄中選取資源群組，再按一下箭頭按鈕，將資源群組移至 **[目前資源群組]** 欄。資源群組是一組資源的集合，可提供其他方式以指定建立及更新資源帳號的順序。
7. 若要爲此角色根據資源指定帳號屬性，請在 **[指定的資源]** 區段中，按一下 **[設定屬性值]**。詳細資訊請參閱第 127 頁的「編輯指定的資源屬性值」。
8. 按一下 **[儲存]** 以開啓 [確認角色變更] 頁面。

   [確認角色變更] 頁面會隨即開啓。
9. 在 **[更新指定的使用者]** 區段中，選取 **[更新指定的使用者]** 功能表選項。詳細資訊請參閱第 148 頁的「更新指定給使用者的角色」。
10. 按一下 **[儲存]**，儲存您的資源指定。

移除角色的資源或資源群組

Identity Manager 可在角色所有者核准時，移除角色的資源或資源群組。使用者收到角色更新之後，就會移除使用者的資源 (詳細資訊請參閱第 148 頁的「更新指定給使用者的角色」)。資源移除後，除非同時將該資源直接指定給使用者，否則使用者會失去對該資源的權利。

若要移除獲得指定角色的資源或資源群組，請執行以下步驟：

1. 搜尋要從中移除資源或資源群組的 IT 角色或應用程式。請依照第 135 頁或第 136 頁上的說明搜尋角色。
2. 按一下角色加以開啓。

   [編輯角色] 頁面會隨即開啓。
3. 按一下 [編輯角色] 頁面中的 **[資源]** 標籤。
4. 若要移除資源，請在 **[目前資源]** 欄中選取資源，再按一下箭頭按鈕，將資源移至 **[可用資源]** 欄。

   若要移除資源群組，請在 **[目前資源群組]** 欄中選取資源群組，再按一下箭頭按鈕，將資源群組移至 **[可用資源群組]** 欄。
5. 按一下 **[儲存]**。

   [確認角色變更] 頁面會隨即開啓。
6. 在 **[更新指定的使用者]** 區段中，選取 **[更新指定的使用者]** 功能表選項。詳細資訊請參閱第 148 頁的「更新指定給使用者的角色」。
7. 按一下 **[儲存]** 以確認變更。

管理使用者角色指定

角色可指定給 Identity Manager [帳號] 區域中的使用者。

本節包含以下主題：

指定角色給使用者

使用下列程序可指定一個或多個角色給一或多名使用者。

一般使用者亦可爲本身提出角色指定請求 (但只能請求已將父系角色指定給使用者的選擇性角色)。如需有關一般使用者如何請求可用角色的資訊，請參閱「Identity Manager 一般使用者介面」一節中的第 55 頁的「請求」。

若要指定一個或多個角色給使用者，請執行以下步驟：

1. 在管理員介面中，按一下 **[帳號]** 標籤。

   [列出帳號] 子標籤會隨即開啓。

2. 若要指定角色給現有使用者，請執行以下步驟：

   a. 按一下 [使用者清單] 中的使用者名稱。

   b. 按一下 **[角色]** 標籤。

   c. 按一下 **[增加]**，將一個或多個角色增加至使用者帳號。

      依預設，只有商務角色可直接指定給使用者 (若您所安裝的 Identity Manager 已從 8.0 之前的版本升級，則商務角色與 IT 角色均可直接指定給使用者)。

   d. 在角色的表格中，選取要指定給使用者的角色，然後按一下 **[確定]**。

      若要依 **[名稱]**、**[類型]** 或 **[描述]** 按照字母順序排序表格，請按一下欄標頭。再按一下會依相反的順序排序。若要依角色類型篩選清單，請從 **[目前]** 下拉式功能表中進行選取。

      表格會更新以顯示選取的角色指定，以及所有與父系角色指定相關的必要角色指定。

   e. 按一下 **[增加]**，以檢視也可指定給使用者的選擇性角色指定。

      選取要指定給使用者的選擇性角色，然後按一下 **[確定]**。

   f. (選擇性) 在 **[啓用時機]** 欄中，選取角色啓用的日期。若未指定日期，角色指定將會在指定的角色核准人核准角色指定時啓用。

      若要指定臨時性角色，請在 **[停用時機]** 欄中選取角色停用的日期。角色會在選定日期的午夜過後停用。

      詳細資訊請參閱第 146 頁的「在特定日期啓用及停用角色」。

   g. 按一下 **[儲存]**。

在特定日期啟用及停用角色

將角色指定給使用者時，您可以指定啓用日期與停用日期。指定時會建立角色指定工作項目請求。但若角色指定未在排定的啓用日期前核准，即不會指定角色。角色的啓用與停用會在排定日期的午夜過後 (午夜 12:01) 生效。

依預設，只有商務角色可以有啓用日期與停用日期。其他角色類型皆會繼承直接指定給使用者之商務角色的啓用日期與停用日期。Identity Manager 可經配置而讓其他角色類型具有可直接指定的啓用與停用日期。如需說明，請參閱第 156 頁。

排程延遲作業掃描儀作業

延遲作業掃描儀可掃描使用者角色指定，並視需要啓用及停用角色。延遲作業掃描儀作業預設每小時執行一次。

若要編輯延遲作業掃描儀的排程，請執行以下步驟：

1. 在管理員介面中，按一下 **[伺服器作業]**。
2. 按一下輔助功能表的 **[管理排程]**。
3. 在 **[可用於排程的作業]** 區段中，按一下 **[延遲作業掃描儀]** TaskDefinition。

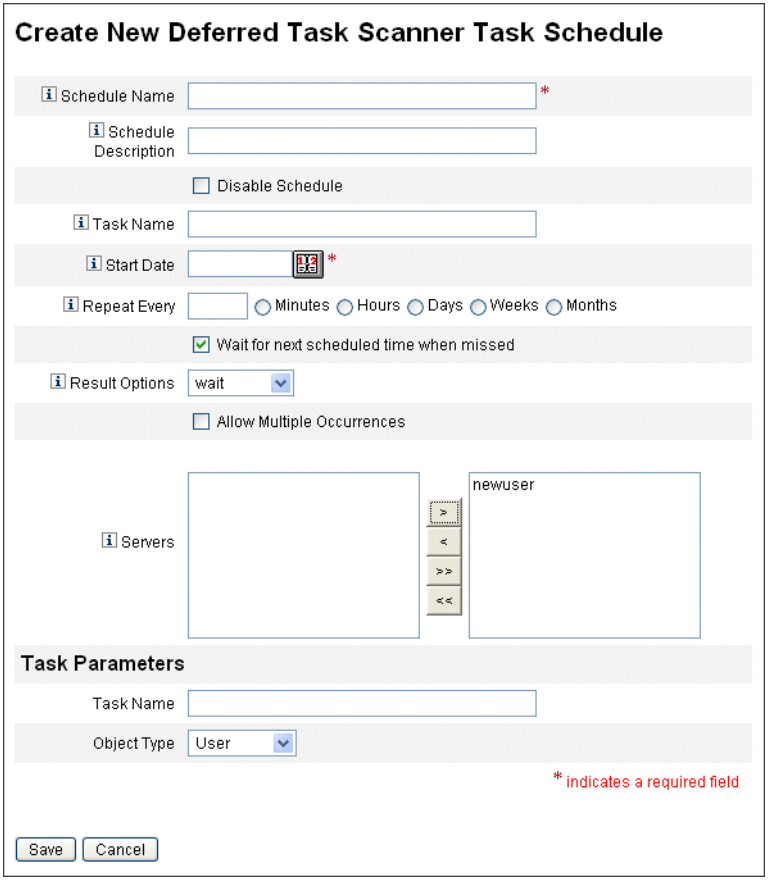
   [建立新的延遲作業掃描儀作業排程] 頁面會隨即開啓。
4. 填寫表單。如需說明，請參閱 i-Helps 與線上說明。

   若要指定執行作業的日期與時間，請在 **[開始日期]** 中使用格式 `mm/dd/yyyy hh:mm:ss`。例如，若要排程在 2008 年 9 月 29 日下午 7:00 開始執行作業，請輸入 `09/29/2008 19:00:00`。

   在 **[結果選項]** 下拉式功能表中，選取 **[重新命名]**。若您選取 **[等待]**，則必須在您移除之前的結果後，此作業未來的實例才會執行。如需有關各項 **[結果選項]** 設定的更多資訊，請參閱線上說明。
5. 按一下 **[儲存]** 以儲存作業。

圖 4-10 顯示 [延遲作業掃描儀] 作業的排定作業表單。

圖 4-10 [延遲作業掃描儀] 的排定作業表單



更新指定給使用者的角色

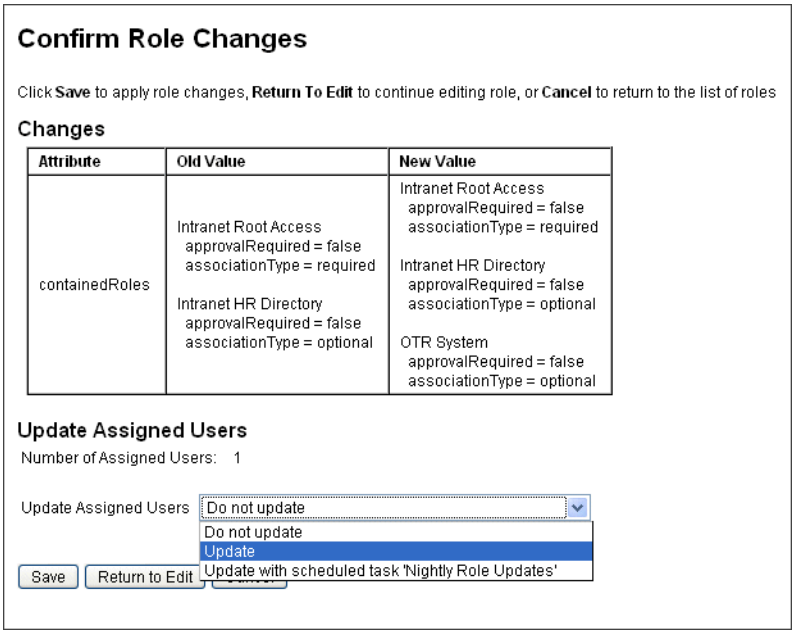
編輯指定給使用者的角色時，您可以選擇立即更新使用者至新的角色變更狀態，或延遲到排定的維護時間執行更新。

對角色進行變更時，會開啓 [確認角色變更] 頁面。[確認角色變更] 頁面如圖 4-11 所示 (第 149 頁)。

- 此頁面的 **[更新指定的使用者]** 區段會顯示目前已獲得該指定角色的使用者人數。
- 使用 **[更新指定的使用者]** 功能表，可選取是要立即更新使用者至新的角色變更狀態 (**[更新]**)、延遲到稍後再更新使用者 (**[不更新]**)，或選取自訂的排程更新作業。
    - 因爲 **[更新]** 動作會立即更新使用者，所以若影響的使用者人數眾多，應避免選擇此選項。更新使用者是耗時與耗資源的作業。如需更新許多使用者，建議排程在離峰時更新。
    - 若爲角色選取了 **[不更新]**，在管理員檢視使用者的使用者設定檔或在「更新角色使用者」作業更新使用者之前，獲得該指定角色的使用者將不會收到角色更新。如需有關排程 [更新角色使用者] 作業的資訊，請參閱下一節。
    - 若已建立「更新角色使用者」作業排程，則可從功能表加以選取。選取的「更新角色使用者」作業將根據爲作業所定義的排程，更新獲得指定角色的使用者。詳細資訊請參閱下一節。

圖 4-11 顯示 [確認角色變更] 頁面。**[更新指定的使用者]** 區段會顯示目前已獲得此指定角色的使用者人數。**[更新指定的使用者]** 下拉式功能表有兩個預設選項：**[不更新]** 與 **[更新]**。您也可以從排定的 [更新角色使用者] 作業清單中選取。如需有關建立排定的 [更新角色使用者] 作業的說明，請參閱第 151 頁的「排程更新角色使用者作業」。

圖 4-11 [確認角色變更] 頁面



手動更新指定的使用者

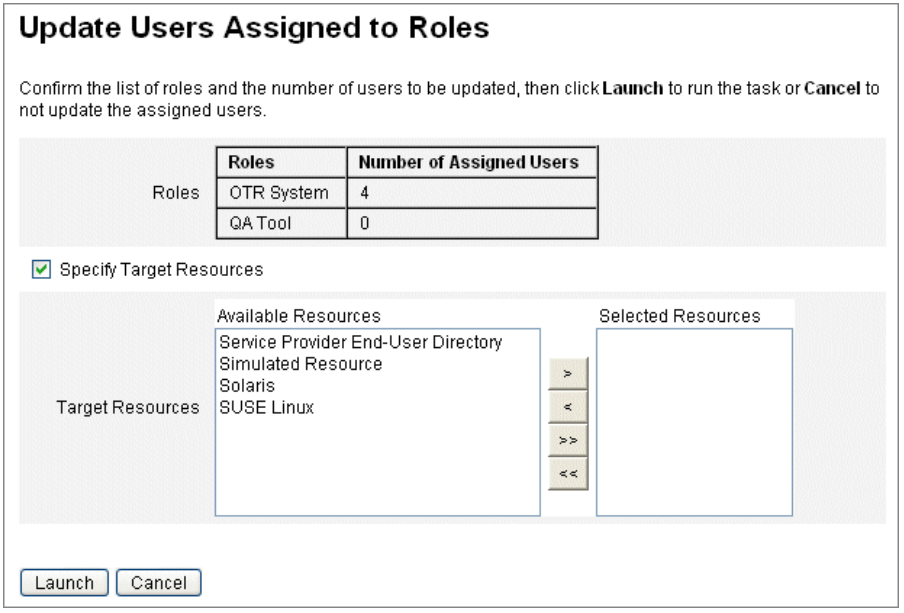
您可以選取一個或多個角色，再按一下 **[更新指定的使用者]** 按鈕，以更新獲得指定角色的使用者。此程序會執行指定角色的 [更新角色使用者作業] 實例。

若要開始更新獲得指定角色的使用者，請執行以下步驟：

1. 依照第 135 頁或第 136 頁的說明，搜尋應更新指定使用者的一個或多個角色。
2. 使用核取方塊選取一個或多個角色。
3. 按一下 **[更新指定的使用者]**。

   [更新獲得指定角色的使用者] 頁面 (圖 4-12) 會隨即顯示。
4. 按一下 **[啓動]** 開始更新。
5. 按一下主功能表中的 **[伺服器作業]**，再按一下輔助功能表中的 **[全部作業]**，以檢查 [更新角色使用者] 作業的狀態。

圖 4-12　更新獲得指定角色的使用者頁面



排程更新角色使用者作業

建議您將 [更新角色使用者] 作業排程爲定期執行。

若要更新使用者至未完成的角色變更狀態，請使用以下步驟排程 [更新角色使用者] 作業：

1. 在管理員介面中，按一下 **[伺服器作業]**。
2. 按一下輔助功能表的 **[管理排程]**。
3. 在 **[可用於排程的作業]** 區段中，按一下 **[更新角色使用者]** TaskDefinition。

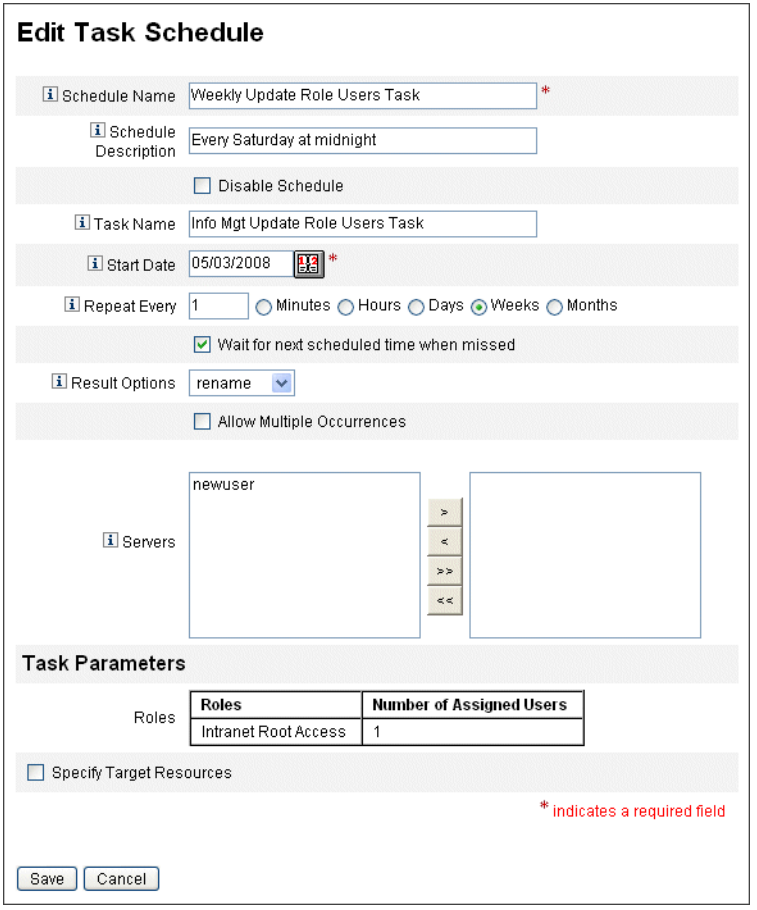
   [建立新的更新角色使用者作業排程] 頁面會隨即開啓；若您編輯現有作業，則會開啓 [編輯作業排程] 頁面 (圖 4-13 (第 152 頁))。
4. 填寫表單。如需說明，請參閱 i-Helps 與線上說明。

   若要指定執行作業的日期與時間，請在 **[開始日期]** 中使用格式 `mm/dd/yyyy hh:mm:ss`。例如，若要排程在 2008 年 9 月 29 日下午 7:00 開始執行作業，請輸入 `09/29/2008 19:00:00`。

   在 **[結果選項]** 下拉式功能表中，選取 **[重新命名]**。若您選取 **[等待]**，則必須在您移除之前的結果後，此作業未來的實例才會執行。如需有關各項 **[結果選項]** 設定的更多資訊，請參閱線上說明。
5. 按一下 **[儲存]** 以儲存作業。

圖 4-13 顯示 [更新角色使用者] 作業的排定作業表單。對於特定的 [更新角色使用者] 作業，可指定特定的角色 (如 **[作業參數]** 區段中所示)。詳細資訊請參閱第 148 頁的「更新指定給使用者的角色」。

圖 4-13　更新角色使用者的排定作業 表單



尋找獲得指定角色的使用者

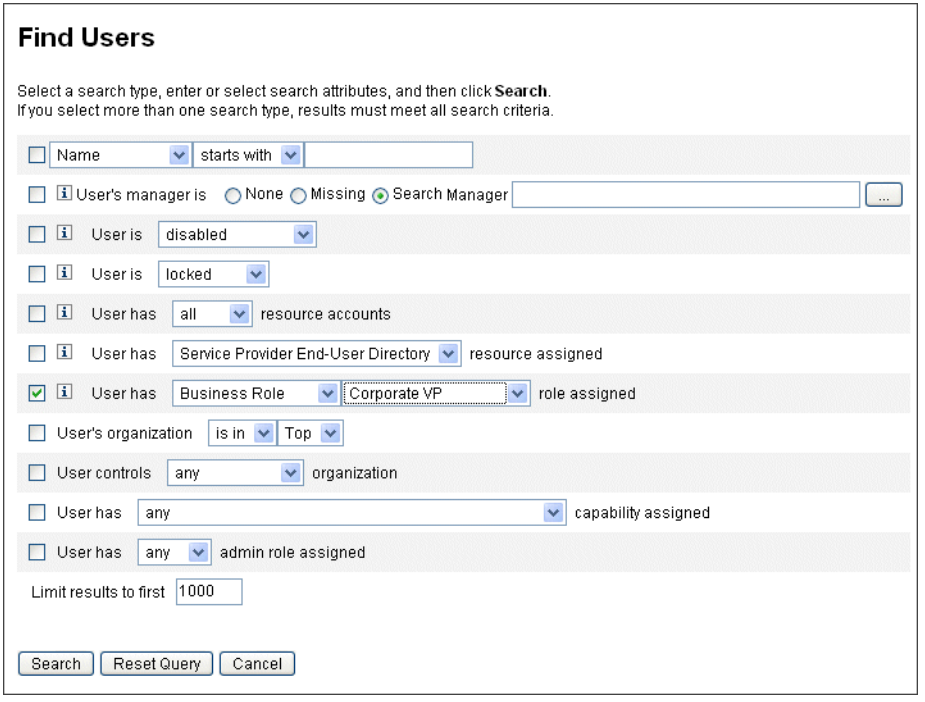
您可以搜尋具有特定指定角色的使用者。

若要尋找具有特定指定角色的使用者，請執行以下步驟：

1. 在管理員介面中，按一下 **[帳號]**。
2. 按一下輔助功能表的 **[尋找使用者]**。[尋找使用者] 頁面會隨即開啓。
3. 尋找搜尋類型 **[已獲得 (選取角色類型...) 指定角色的使用者]**。
4. 選取選項方塊，並使用 **[選取角色類型...]** 下拉式功能表篩選可用角色清單。

   第二個角色功能表會隨即開啓。
5. 選取角色。
6. 除非您要進一步縮小搜尋範圍，否則請清除其他搜尋類型核取方塊。
7. 按一下 **[搜尋]**。

圖 4-14　使用 [尋找使用者] 頁面搜尋具有指定角色的使用者



移除指定給使用者的角色

使用 [編輯使用者] 頁面，可從使用者帳號中移除一個或多個角色。僅可移除直接指定的角色。間接指定的角色 (亦即條件式和 (或) 必要**內含角色**) 會在移除父系角色時一起移除。另一個移除使用者的間接指定角色方法，是移除父系角色的角色 (請參閱第 139 頁的「從角色中移除角色」)。

一般使用者亦可請求移除自身使用者帳號中的指定角色。請參閱「Identity Manager 一般使用者介面」一節中的第 55 頁的「請求」。

如需有關使用排定的停用日期移除角色的資訊，請參閱第 146 頁的「在特定日期啓用及停用角色」。

若要移除使用者的一個或多個角色，請執行以下步驟：

1. 在管理員介面中，按一下 **[帳號]** 標籤。

   [列出帳號] 子標籤會隨即開啓。

2. 按一下您要從中移除一或多項規則的使用者。

   [編輯使用者] 頁面會隨即開啓。

3. 按一下 **[角色]** 標籤。

4. 在角色的表格中，選取要移除的使用者角色，然後按一下 **[確定]**。

   若要依 **[名稱]**、**[類型]**、**[啓用時機]**、**[停用時機]**、**[指定者]** 或 **[狀態]** 按照字母順序排序表格，請按一下欄標頭。再按一下會依相反的順序排序。若要依角色類型篩選清單，請從 **[目前]** 下拉式功能表中進行選取。

   表格會顯示父系角色指定 (可選取的角色)，以及所有與父系角色指定相關的角色指定 (無法選取的角色)。

5. 按一下 **[移除]**。

   指定角色的表格會更新，以顯示剩餘指定角色。

6. 按一下 **[儲存]**。

   [更新資源帳號] 頁面會隨即開啓。取消選取不需要移除的所有資源帳號。

7. 按一下 **[儲存]** 儲存變更。

配置角色類型

欲修改 [角色類型] 功能，請編輯 [角色] 配置物件。

配置可直接指定給使用者的角色類型

依預設，只有特定角色類型可直接指定給使用者。若要變更這些設定，請使用以下步驟。

備註 建議您最好僅直接將商務角色指定給使用者。詳細資訊請參閱第 119 頁的「使用角色類型設計彈性角色」。

若要變更可直接指定給使用者的角色類型，請執行以下步驟：

1. 開啓 [角色] 配置物件，使用第 197 頁的「編輯 Identity Manager 配置物件」中的步驟加以編輯。
2. 尋找與您要編輯之角色類型相對應的角色物件。
   - 若要編輯 IT 角色，請尋找 `Object name='ITRole'`
   - 若要編輯應用程式角色，請尋找 `Object name='ApplicationRole'`
   - 若要編輯資產角色，請尋找 `Object name='AssetRole'`
3. 根據您要以何種方式更新配置，挑選一組適當的指令：
   - 若要修改角色類型使其可直接指定給使用者，請在角色物件中尋找下列 `userAssignment` 屬性：

     ```
     <Attribute name='userAssignment'>
         <Object/>
     </Attribute>
     ```

     並以下一行替代此行：

     ```
     <Attribute name='userAssignment'>
         <Object>
             <Attribute name='manual' value='true'/>
         </Object>
     </Attribute>
     ```

- 若要修改角色類型使其無法直接指定給使用者，請在角色物件中尋找 userAssignment 屬性，然後刪除 manual 屬性，如下所示：

```
<Attribute name='userAssignment'>
    <Object>
    </Object>
</Attribute>
```

4. 儲存 [角色] 配置物件。您無需重新啓動應用程式伺服器，變更即可生效。

啟用角色類型指定啟用日期與停用日期的功能

依預設，只有商務角色能在指定角色時，指定啓用日期與停用日期。其他角色皆會從直接指定給使用者的商務角色，繼承啓用日期與停用日期。

備註 建議您最好僅直接將商務角色指定給使用者。詳細資訊請參閱第 119 頁的「使用角色類型設計彈性角色」。

若您選擇可將其他角色類型直接指定給使用者 (例如 IT 角色類型)，您可能也需要爲該角色類型指定啓用與停用日期。

若要變更可指定啓用日期與停用日期的角色類型，請執行以下步驟：

1. 開啓 [角色] 配置物件，使用第 197 頁的「編輯 Identity Manager 配置物件」中的步驟加以編輯。
2. 尋找與您要編輯之角色類型相對應的角色物件。
   - 若要編輯商務角色，請尋找 `Object name='BusinessRole'`
   - 若要編輯 IT 角色，請尋找 `Object name='ITRole'`
   - 若要編輯應用程式角色，請尋找 `Object name='ApplicationRole'`
   - 若要編輯資產角色，請尋找 `Object name='AssetRole'`

3. 根據您要以何種方式更新配置，挑選一組適當的指令：

   - 若要修改角色類型使其可直接指定啓用日期與停用日期，請在角色物件中尋找下列 userAssignment 屬性：

     ```
     <Attribute name='userAssignment'>
         <Attribute name='manual' value='true'/>
     </Attribute>
     ```

     並以下一行替代此行：

     ```
     <Attribute name='userAssignment'>
         <Object>
             <Attribute name='activateDate' value='true'/>
             <Attribute name='deactivateDate' value='true'/>
             <Attribute name='manual' value='true'/>
         </Object>
     </Attribute>
     ```

   - 若要修改角色類型使其無法直接指定啓用日期與停用日期，請在角色物件中尋找 userAssignment 屬性，然後刪除 activateDate 與 deactivateDate 屬性，如下所示：

     ```
     <Attribute name='userAssignment'>
         <Object>
         </Object>
     </Attribute>
     ```

4. 儲存 [角色] 配置物件。您無需重新啓動應用程式伺服器，變更即可生效。

啟用及停用變更核准與變更通知工作項目

預設會啓用所有角色類型的變更核准工作項目。這表示每次角色有所變更時 (無論是商務角色、IT 角色、應用程式或資產)，若角色具有所有者，所有者必須核准變更，變更才會生效。

如需有關變更核准與變更通知工作項目的更多資訊，請參閱第 133 頁的「啓動變更核准與核准工作項目」。

若要啓用或停用角色類型的變更核准與變更通知工作項目，請執行以下步驟：

1. 開啓 [角色] 配置物件，使用第 197 頁的「編輯 Identity Manager 配置物件」中的步驟加以編輯。
2. 尋找與您要編輯之角色類型相對應的角色物件。
   - 若要編輯商務角色，請尋找 `Object name='BusinessRole'`
   - 若要編輯 IT 角色，請尋找 `Object name='ITRole'`
   - 若要編輯應用程式角色，請尋找 `Object name='ApplicationRole'`
   - 若要編輯資產角色，請尋找 `Object name='AssetRole'`
3. 尋找下列位於 `<Object>` 元素中的屬性 (該元素位於 `<Attribute name=features>` 元素中)：

   ```
   <Attribute name='changeApproval' value='true'/>
   <Attribute name='changeNotification' value='true'/>
   ```

4. 視需要將屬性值設定爲 True 或 False。
5. 必要時，請重複步驟 2 - 4 以配置其他角色類型。
6. 儲存 [角色] 配置物件。您無需重新啓動應用程式伺服器，變更即可生效。

配置角色清單頁面將載入的最大列數

您可針對管理員介面中的 [列出角色] 頁面，配置可顯示的最大列數。預設數目爲 500。您可以使用本節中的步驟變更此數目。

若要變更 [列出角色] 頁面可顯示的最大列數，請執行以下步驟：

1. 開啓 [角色] 配置物件，使用第 197 頁的「編輯 Identity Manager 配置物件」中的步驟加以編輯。
2. 尋找下列屬性，並變更其值：

   ```
   <Attribute name='roleListMaxRows' value='500'/>
   ```

3. 儲存 [角色] 配置物件。您無需重新啓動應用程式伺服器，變更即可生效。

同步化 Identity Manager 角色和資源角色

您可以將 Identity Manager 角色與原本在資源中建立的角色同步化。依預設，在進行同步時，資源將獲得指定角色。角色可以是同步化作業所建立的角色，也可以是符合其中一個資源角色名稱的現有 Identity Manager 角色。

若要同步化 Identity Manager 角色與資源角色，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[伺服器作業]**。
2. 按一下 **[執行作業]**。[可用的作業] 頁面會隨即開啓。
3. 按一下 **[將識別系統角色與資源角色同步]** 作業。
4. 填寫表單。如需更多資訊，請按一下 **[說明]**。
5. 按一下 **[啓動]**。

瞭解與管理資源

請閱讀本節以獲得協助您設定 Identity Manager 資源的資訊和程序。

甚麼是資源？

Identity Manager 資源儲存有關如何連結到建立帳號之資源或系統的資訊。Identity Manager 資源定義關於資源的相關屬性並協助指定資源資訊在 Identity Manager 中如何顯示。

Identity Manager 提供廣泛資源類型的資源，包括：

- 主機安全管理程式
- 資料庫
- 目錄服務
- 作業系統
- 企業資源規劃 (ERP) 系統
- 訊息平台

介面中的 [資源] 區域

Identity Manager 顯示關於 [資源] 頁中現有資源的資訊。

若要存取資源，請選取功能表列上的 **[資源]**。

資源清單中的資源按類型分組。每個資源類型皆會以資料夾圖示表示。若要查看目前定義的資源，請按一下資料夾旁的指示器。再按一下該指示符，便會摺疊檢視。

當您展開資源類型資料夾時，它會動態更新並顯示其包含的資源物件數目 (如果它是支援群組的資源類型)。

有些資源具有其他您可以管理的物件，包括：

-  組織
-  組織單位
-  群組
-  角色

從資源清單中選取一個物件，然後從以下選項清單之一中進行選取以啟動管理作業：

- **資源動作** - 對資源執行一系列動作，包括編輯、啓用同步化、重新命名與刪除；還包括處理資源物件和管理資源連線。
- **資源物件動作** - 編輯、建立、刪除、重新命名、另存新檔與尋找資源物件。
- **資源類型動作** - 編輯資源策略、處理帳號索引以及配置受管資源。

建立或編輯資源時，Identity Manager 會啓動 `ManageResource` 工作流程。這個工作流程會在儲存庫中儲存新的或更新的資源，並讓您在建立或儲存資源之前插入核准或其他動作。

管理資源清單

建立新的資源之前，您必須告知 Identity Manager 需要管理的資源類型。若要啓用資源及建立自訂資源，請使用 [配置受管資源] 頁面。

開啟配置受管資源頁面

若要開啓 [配置受管資源] 頁面，請執行以下步驟：

1. 登入管理員介面，然後按一下 **[資源]** 標籤。
2. 尋找 **[資源類型動作]** 下拉式清單，然後選取 **[配置受管資源]**。

   [配置受管資源] 頁面會隨即開啓。

[配置受管資源] 頁面有兩個區段：

- **資源** - 此區段會列出大型企業環境中常見的資源類型。連線至資源的 Identity Manager 配接卡版本，會列示在 **[版本]** 欄中。
- **自訂資源** - 此區段可將自訂資源加入 [資源] 清單中。

啟用資源類型

從 [配置受管資源] 頁面啓用資源類型。

若要啓用資源類型，請執行下列作業：

1. [配置受管資源] 頁面應開啓。若未開啓，請加以開啓 (第 163 頁)。
2. 在 **[資源]** 區段中，針對您要啓用的資源類型，選取 **[受管理？]** 欄中的方塊。

   若要啓用所有列出的資源類型，請選取 **[要管理所有資源]**。
3. 按一下頁面底部的 **[儲存]**。

   資源會隨即加入 [資源] 清單中。

增加自訂資源

從 [配置受管資源] 頁面增加自訂資源。

若要增加自訂資源，請執行下列作業：

1. [配置受管資源] 頁面應開啓。若未開啓，請加以開啓 (第 163 頁)。
2. 在 **[自訂資源]** 區段中，按一下 **[增加自訂資源]** 在表格中增加一列。
3. 輸入資源的資源類別路徑，或輸入您自訂開發的資源。對於 Identity Manager 所提供的配接卡，請參閱 「Identity Manager 資源參照」以取得完整類別路徑。
4. 按一下 **[儲存]** 將資源新增到 [資源] 清單。

建立資源

啓用資源類型後，您即可在 Identity Manager 中建立該資源的實例。若要建立資源，請使用 **「資源精靈」**。「資源精靈」會引導您設定下列項目：

- **資源專用參數** - 當建立此資源類型的特定實例時，您可以從 Identity Manager 介面修改這些值。
- **帳號屬性** - 在資源模式對映中所定義。這些決定 Identity Manager 使用者屬性如何對映到資源中的屬性。
- **帳號 DN 或身份識別範本** - 包括使用者的帳號名稱語法，這對階層式名稱空間特別重要。
- **用於資源的 Identity Manager 參數** - 可設定策略、建立資源核准人，以及設定組織對資源的存取權。

使用資源精靈建立資源

「資源精靈」會指導您完成配置 Identity Manager 資源配接卡的過程，然後您就可以使用該配接卡來管理資源上的物件。

若要建立資源，請執行以下步驟：

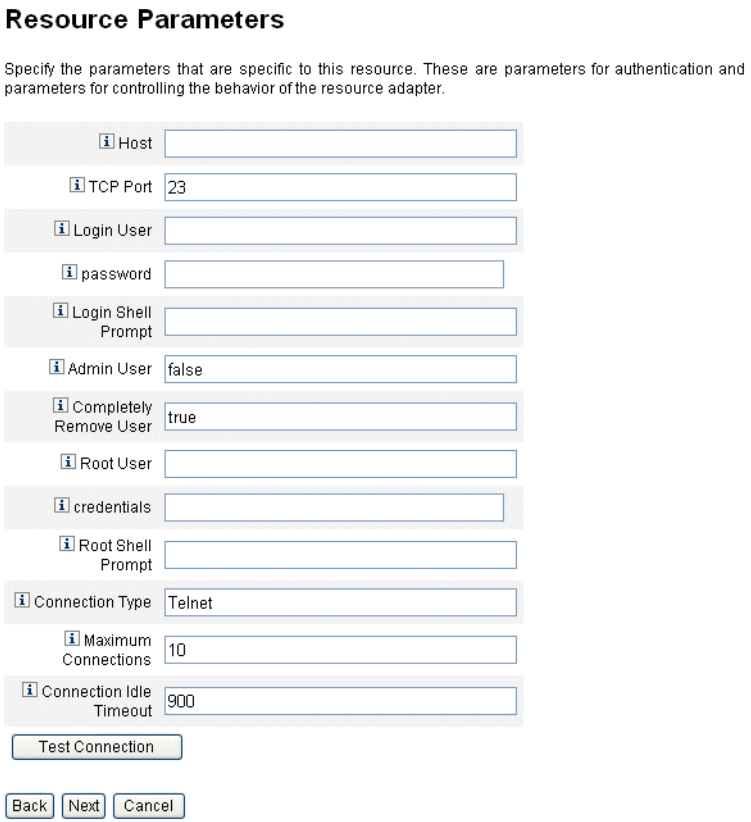
1. 登入管理員介面。
2. 按一下 **[資源]** 標籤。驗證是否已選取 **[列出資源]** 子標籤。
3. 尋找 **[資源類型動作]** 下拉式清單，然後選取 **[新資源]**。

   [新資源] 頁面會隨即開啓。

4. 從下拉式清單中選取資源類型 (若您所尋找的資源類型並未列出，您必須加以啓用。請參閱第 163 頁的 「管理資源清單」)。
5. 按一下 **[新增]** 以顯示 「資源精靈」的 [歡迎] 頁面。
6. 按 **[下一頁]** 開始定義資源。資源精靈的步驟和頁面以如下順序顯示：
   - **資源參數** - 設定用於控制認證和資源配接卡運作方式的資源專用參數。輸入參數，然後按一下 **[測試連線]** 來確保連線有效。確認後，按一下 **[下一頁]** 以設定帳號屬性。

圖 4-15 顯示 Solaris 資源的 [資源參數] 頁面。不同的資源在此頁面上會有不同的表單欄位。

圖 4-15 資源精靈：資源參數

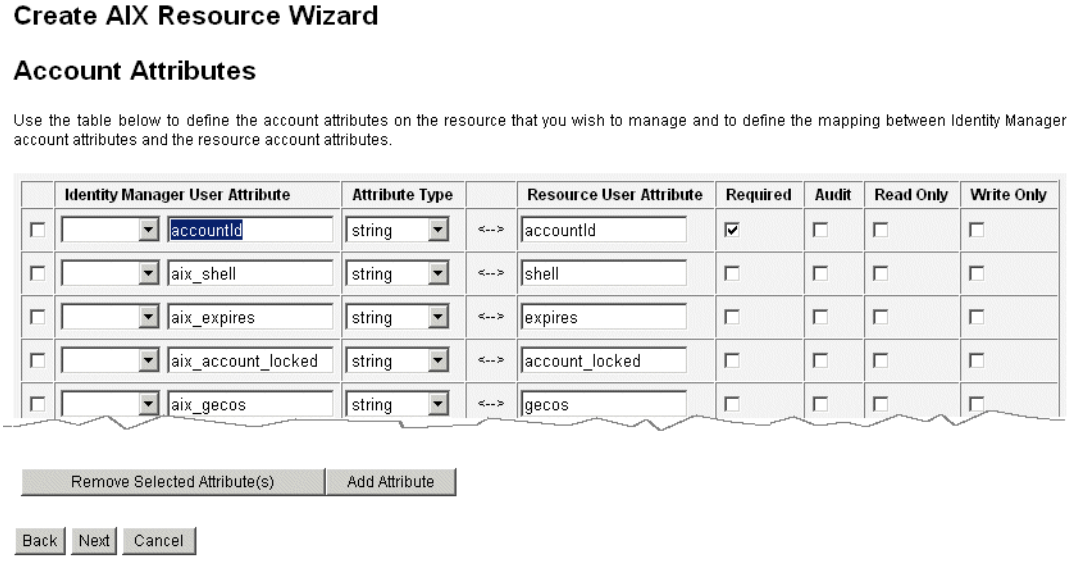


- **帳號屬性 (模式對映)** - 將 Identity Manager 帳號屬性對映到資源帳號屬性。如需有關資源帳號屬性的更多資訊，請參閱第 170 頁的「使用帳號屬性」。
  - 若要新增屬性，按一下 **[增加屬性]**。
  - 若要移除一個或多個屬性，請選取屬性旁的方塊，然後按一下 **[移除選取的屬性]**。

  完成後，請按 **[下一步]** 設定 [身份識別範本]。

  圖 4-16 顯示了資源精靈中的 [帳號屬性] 頁面。

圖 4-16　資源精靈：帳號屬性 (模式對映)



- **身份識別範本** - 爲使用者定義帳號名稱語法。此功能對階層式名稱空間特別重要。

  - 若要在範本中增加屬性，請從 **[插入屬性]** 清單中選取屬性。
  - 若要刪除屬性，請在字串中加以反白顯示，並使用鍵盤上的 Delete 鍵。刪除屬性名稱以及前置與後置的 $ (美元符號) 字元。
  - **帳號類型** - Identity Manager 可讓您將多個資源帳號指定給單一使用者。例如，使用者可能同時需要管理員層級的帳號，以及特定資源上的一般使用者帳號。若要支援此資源的多個帳號類型，請選取 **[帳號類型]** 核取方塊。

    備註： 若尚未建立可由 **IdentityRule** 子類型識別的一個或多個「產生身份識別」規則，即無法選取 [帳號類型] 核取方塊。由於帳號 ID 必須不同，因此不同的帳號類型必須爲指定使用者產生不同的帳號 ID。「產生身份識別」規則可指定應如何建立這些唯一的帳號 ID。

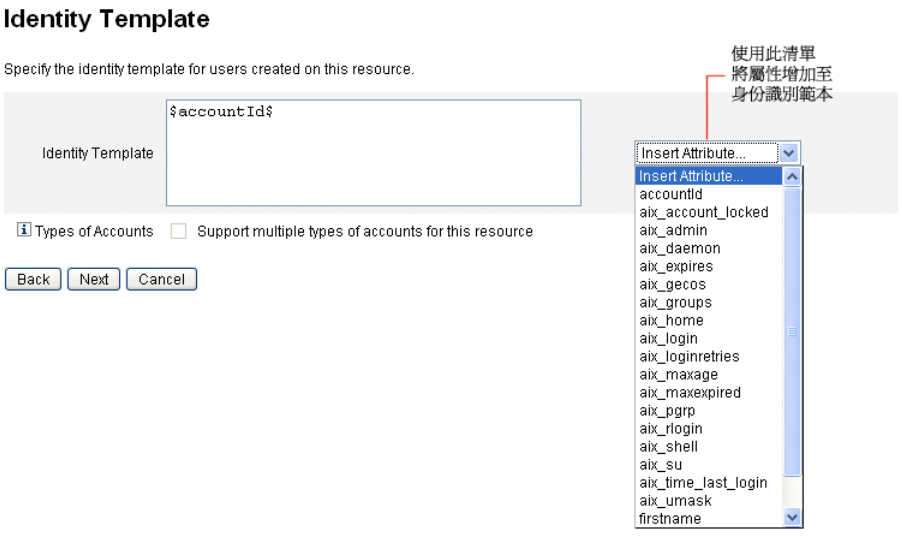
    `sample/identityRules.xml` 中提供有身份識別規則範例。

    您必須在 Identity Manager 內沒有其他物件參照帳號類型時，才可移除該帳號類型。您無法重新命名帳號類型。

    如需有關填寫 **[帳號類型]** 表單的更多資訊，請參閱線上說明。

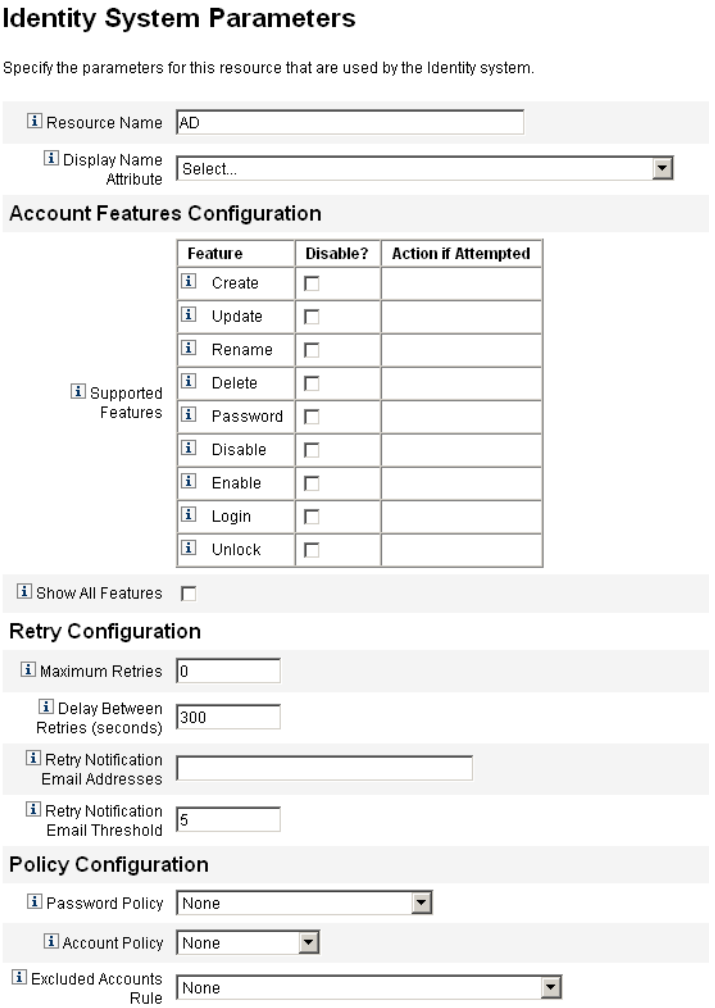
    如需有關爲使用者建立多個資源帳號的更多資訊，請參閱第 75 頁。

圖 4-17 資源精靈：身份識別範本



- **身份識別系統參數** - 設定資源的 Identity Manager 參數，包括重試配置和策略配置，如圖 4-18 所示。

圖 4-18　資源精靈：身份識別系統參數



使用 **[下一頁]** 和 **[上一步]** 在頁面中移動。當您完成所有選項後，請按一下 **[儲存]** 來儲存資源並回到清單頁。

管理資源

本節說明如何管理現有資源。

檢視資源清單

使用 **[資源清單]** 可檢視現有資源。**[資源清單]** 指令可對資源執行多種編輯動作。

若要檢視 [資源清單]，請執行以下步驟：

1. 登入管理員介面。
2. 按一下主功能表中的 **[資源]**。

   [資源清單] 會顯示在 **[列出資源]** 子標籤上。

使用資源精靈編輯資源

使用「資源精靈」編輯資源參數、帳號屬性與身份識別系統參數。您也可以指定資源上建立的使用者所應使用的身份識別範本。

若要使用「資源精靈」編輯資源，請執行以下步驟：

1. 在 Identity Manager 的管理員介面中，按一下主功能表的 **[資源]**。

   [資源清單] 會顯示在 **[列出資源]** 子標籤上。
2. 選取您要編輯的資源。
3. 在 **[資源動作]** 下拉式功能表中，選取 **[資源精靈]** (在 **[編輯]** 下)。

   資源精靈會以 [編輯] 模式開啓，供選取的資源使用。

使用資源清單指令選項編輯資源

除了編輯資源精靈以外，您還可以使用**「資源清單」**指令對資源執行多種編輯動作：

- **刪除資源** - 選取一個或多個資源，然後從 [資源動作] 清單中選取 [刪除]。同時您可以選取多種類型的資源。如果有任何角色或資源群組跟資源相關聯，則無法刪除該資源。
- **搜尋資源物件** - 選取資源，然後從 [資源物件動作] 清單中選取 [尋找資源物件]，以便依物件特性來尋找資源物件 (例如組織、組織單位、群組或人員)。
- **管理資源物件** - 對於某些資源類型，您可以爲其建立新的物件。選取資源，然後從 [資源物件動作] 清單中選取 [建立資源物件]。
- **重新命名資源** - 選取資源，然後從 [資源動作] 清單中選取 [重新命名]。在出現的輸入方塊中輸入新名稱，然後按一下 **[重新命名]**。

- **複製資源** - 選取資源，然後從 [資源動作] 清單中選取 [另存新檔]。在出現的輸入方塊中輸入新的名稱。複製資源會以您選取的名稱出現在資源清單中。
- **對資源執行批次處理作業** - 指定資源清單，以及指定要 (從 CSV 格式的輸入) 套用至此清單中所有資源的動作。然後啓動批次作業，以啓動批次處理作業背景作業。

使用帳號屬性

資源帳號屬性 (或模式對映) 提供抽象的方法以參照受管資源上的屬性。模式對映可讓您指定如何在 Identity Manager (模式對映左側) 內參照屬性，以及該名稱如何對映至實際資源上的屬性名稱 (模式對映右側)。接著，您即可在表單或工作流程定義內參照 Identity Manager 屬性名稱，並有效參照資源上的屬性本身。

圖 4-16 (第 166 頁) 顯示 [資源帳號屬性] 頁面。

以下範例說明 Identity Manager 中的屬性與 LDAP 資源的屬性對映：

Identity Manager 屬性		LDAP 資源屬性
`firstname`	`<-->`	`givenName`
`lastname`	`<-->`	`sn`

對該資源採取動作時，任何對 Identity Manager 屬性 `firstname` 的參照，實際上皆是對 LDAP 屬性 `givenName` 的參照。

從 Identity Manager 管理多個資源時，若將一般 Identity Manager 帳號屬性對映至許多資源屬性，將可大幅簡化資源管理作業。例如，Identity Manager `fullname` 屬性可對映至 Active Directory 資源屬性 `displayName`。同時，在 LDAP 資源上，相同的 Identity Manager `fullname` 屬性可對映至 LDAP 屬性 `cn`。因此，管理員只需提供 `fullname` 值一次。儲存使用者後，`fullname` 值會接著傳送至具有不同屬性名稱的資源。

在「資源精靈」的 [帳號屬性] 頁面上設定模式對映，可讓您執行下列作業：

- 爲來自受管資源的屬性定義屬性名稱與資料類型
- 將資源屬性限定爲只有您的公司或組織所需的屬性
- 建立用於多個資源的共用 Identity Manager 屬性名稱
- 辨認所需的使用者屬性和屬性類型

編輯資源帳號屬性

若要檢視或編輯資源帳號屬性，請執行以下步驟：

1. 在管理員介面中，按一下 **[資源]**。
2. 選取您要檢視或編輯帳號屬性的資源。
3. 在 **[資源動作]** 清單中，按一下 **[編輯資源模式]**。

   [編輯資源帳號屬性] 頁面會隨即開啓。

   圖 4-16 (第 166 頁) 顯示 [資源帳號屬性] 頁面。

模式對映的左欄 (標題爲 **「識別系統使用者屬性」**) 包含 Identity Manager 帳號屬性的名稱，這些屬性由 Identity Manager 管理員和使用者介面中所使用的表單參照。模式對映的右欄 (標題爲 **「資源使用者屬性」**) 包含來自外部來源的屬性名稱。

資源群組

使用資源區來管理資源群組，這可讓您對資源進行分組以按特定順序更新這些資源。在群組中加入資源並對資源進行排序，然後將該群組指定給使用者，即可確定該使用者之資源的建立、更新和刪除順序。

依次對每個資源執行作業。如果對某一資源執行的動作失敗，則不會更新其餘資源。這種類型的關係對相關資源很重要。

例如，Exchange Server 2007 資源依賴現有的 Windows Active Directory 帳號。此帳號必須存在，才可成功建立 Exchange 帳號。(依序) 以 Windows Active Directory 資源和 Exchange Server 2007 資源建立資源群組，即可確保按正確的順序建立使用者。反之，此順序也確保您在刪除使用者時以正確的序列刪除資源。

選取 **[資源]**，然後選取 **[列出資源群組]** 以顯示目前定義的資源群組之清單。在該頁中，按一下 **[新增]** 定義資源群組。在定義資源群組時，選項區可讓您選擇並排序選取的資源，以及選取可使用該資源群組的組織。

全域資源策略

您可以在 [全域資源策略] 中編輯資源的特性。在 [編輯全域資源策略屬性] 頁面中，您可以編輯以下策略屬性：

- **預設擷取逾時** - 輸入一個值 (以毫秒爲單位)，以指定在指令行提示之後，介面應等待多長時間後逾時。此值僅適用於 GenericScriptResourceAdapter 或 ShellScriptSourceBase 介面。當指令或程序檔的結果很重要且將由介面剖析時，請使用此設定。

  此設定的預設值爲 30000 (30 秒)。

- **預設等待逾時** - 輸入一個值 (以毫秒爲單位)，以指定在檢查指令是否具有就緒字元 (或結果) 之前，程序檔介面兩次輪詢之間應等待的最長時間。此值僅適用於 GenericScriptResourceAdapter 或 ShellScriptSourceBase 介面。當介面不檢查指令或程序檔結果時，請使用此設定。

- **等待忽略大小寫** - 輸入一個值 (以毫秒爲單位)，以指定在逾時之前介面應等待指令行提示的最長時間。此值僅適用於 GenericScriptResourceAdapter 或 ShellScriptSourceBase 介面。當不區分大小寫 (大寫或小寫) 時，請使用此設定。

- **資源帳號密碼策略** - 選取要套用至所選資源的資源帳號密碼策略 (如果適用)。預設選項爲 **[無]**。

- **排除的資源帳號規則** - 選取用於管理已排除資源帳號的規則 (如果適用)。預設選項爲 **[無]**。

您必須按一下 **[儲存]** 才能儲存對策略所做的變更。

設定其他逾時值

您可以編輯 Waveset 特性檔案，以修改 `maxWaitMilliseconds` 特性。`maxWaitMilliseconds` 特性可控制監視作業逾時的頻率。如果未指定該值，系統將使用預設值 50。

若要設定該值，請將以下內容增加到 Waveset 特性檔案中：

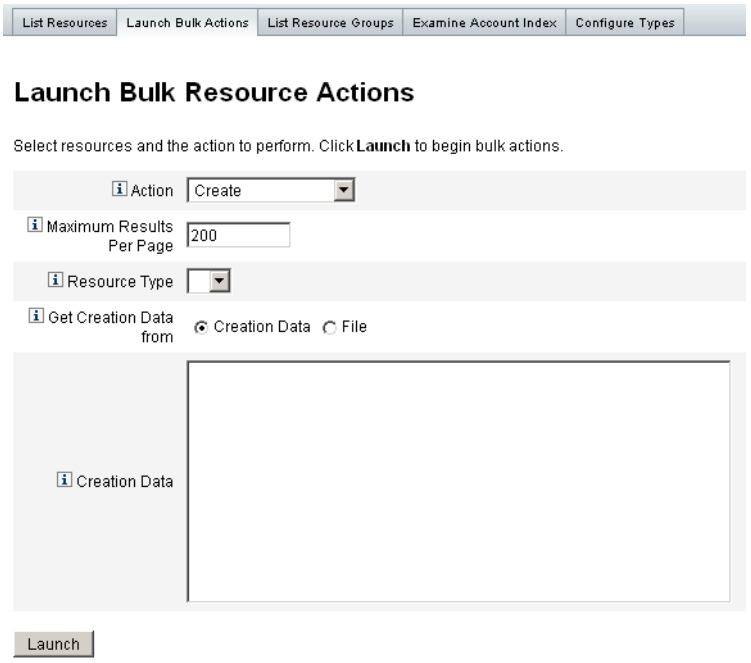
```
com.waveset.adapter.ScriptedConnection.ScriptedConnection.maxwaitMilliseconds.
```

批次處理資源動作

您可以透過使用 CSV 格式的檔案或透過建立或指定作業要套用的資料，在資源上執行批次處理作業。

圖 4-19 顯示了使用建立動作的批次處理作業的啓動頁面。

圖 4-19　　啓動批次處理資源動作頁面



批次處理資源作業的可用選項取決於您選取的作業動作。您可以指定要套用至作業的單一動作，或選取 **[從動作清單]** 以指定多個動作。

- **動作** - 若要指定單一動作，請選取以下任一選項：[建立]、[複製]、[更新]、[刪除]、[變更密碼]、[重設密碼]。

  對於單一動作選項，將會向您提供用於指定動作所涉及資源的選項。對於 [建立] 動作，您將指定資源類型。

  如果您指定 [從動作清單]，請使用 **[動作清單取得來源]** 區域指定要使用的含動作檔案或您在 [輸入] 區域中指定的動作。

備註 您在 [輸入] 區域清單中或在檔案中輸入的動作必須爲逗號分隔值 (CSV) 格式。

- **每頁最多結果數** - 使用此選項即可指定在每個作業結果頁面上，要顯示的批次處理動作結果的最大數目。預設值爲 200。

按一下 **[啓動]** 可以啓動作業，其將做爲背景作業執行。

第 5 章

配置與系統維護

本章提供使用管理員介面設定及維護 Identity Manager 物件與伺服器程序的資訊及程序。如需有關 Identity Manager 物件的更多資訊，請參閱簡介一章中的第 40 頁的「Identity Manager 物件」。

備註 如需有關爲服務提供者實作配置 Identity Manager 的資訊，請參閱第 17 章「服務提供者管理」。

本章包含以下主題：

配置 Identity Manager 策略

請閱讀本小節以取得有關配置使用者策略的資訊和程序。

什麼是策略？

藉由建立 Identity Manager 帳號 ID、登入和密碼特性的限制條件，Identity Manager 策略可設定 Identity Manager 使用者的限制。

備註 Identity Manager 還提供專門用於稽核使用者規範遵循的稽核策略。第 13 章「身份識別稽核：基本概念」中論述了稽核策略。

開啟策略頁面

您可以在 [策略] 頁面中建立並編輯 Identity Manager 使用者策略。

若要開啓 [策略] 頁面，請執行以下步驟：

1. 登入管理員介面。
2. 按一下 **[安全性]** 標籤，再按一下 **[策略]** 子標籤。

   [策略] 頁面會隨即開啓。

策略類型

使用 [策略] 頁面可編輯現有策略並建立新策略。

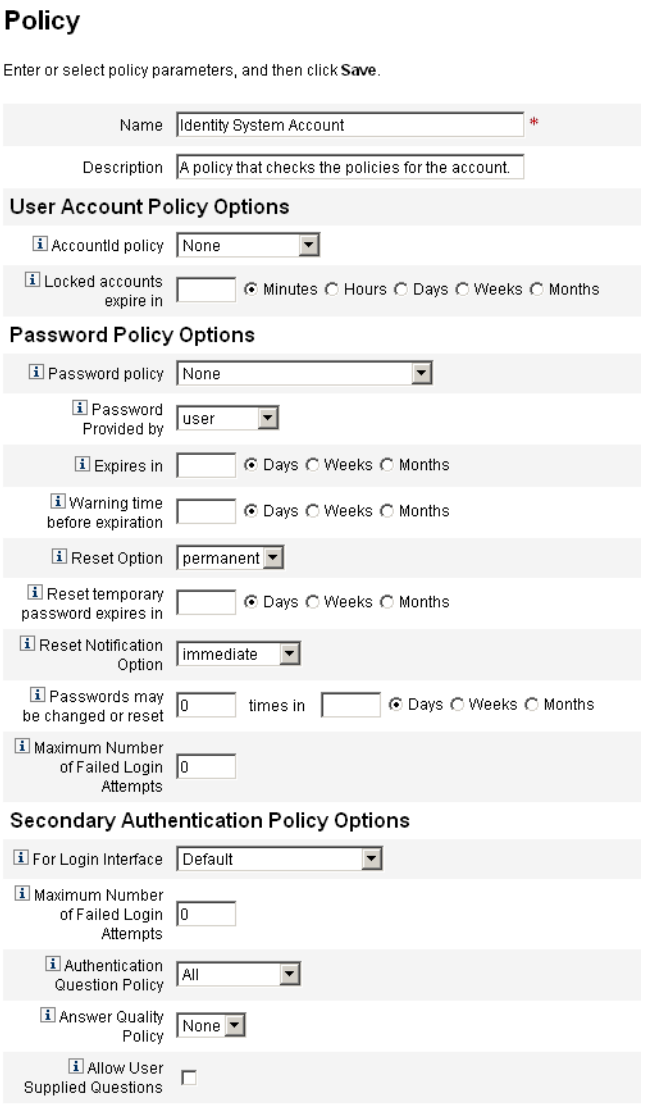
策略可分爲以下類型：

- **Identity 系統帳號策略** - 建立使用者、密碼和認證策略選項與限制。透過 [建立組織]、[編輯組織]、[建立使用者] 和 [編輯使用者] 等頁面，您可將識別系統帳號策略 (如圖 5-1 所示) 指定給組織或使用者。

  您可以設定或選取的選項包括：

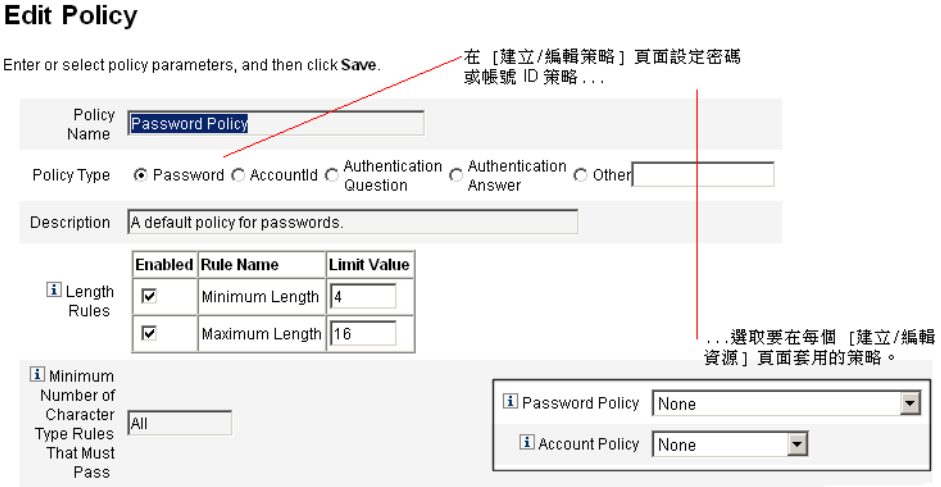
  - **使用者策略選項** - 指定使用者在無法正確回答認證問題時，Identity Manager 如何處理使用者帳號
  - **密碼策略選項** - 設定密碼過期、過期前的警告時間以及重設選項
  - **驗證策略選項** - 確定如何向使用者提出認證問題，使用者是否可以提供其自己的認證問題、是否在登入時強制執行認證以及建立可以向使用者顯示的問題庫。

圖 5-1 Identity Manager 策略



- **服務提供者系統帳號策略** - 此策略類型用於在服務提供者實作中，爲服務提供者使用者建立使用者、密碼和認證策略選項與限制。透過 [建立組織]、[編輯組織]、[建立服務提供者使用者] 和 [編輯服務提供者使用者] 等頁面，可將這些策略指定給組織或使用者。
- **字串品質策略** - 字串品質策略包括策略類型 (例如密碼、帳號 ID 和認證)，並可設定長度規則、字元類型規則和允許的文字與屬性值。此類型的策略繫結到每個 Identity Manager 資源，並在每個資源頁面中設定。圖 5-2 提供了一個範例。

圖 5-2　　建立/編輯密碼策略



您可以爲密碼和帳號 ID 設定的選項及規則包括：

- **長度規則** - 確定最小和最大長度。
- **字元類型規則** - 設定允許的字母、數字、大寫、小寫、重複及連續字元最小值和最大值。
- **密碼重複使用限制** - 指定一個數值，表示從目前的密碼往前有多少個密碼不可重複使用。當使用者試圖變更密碼時，將比對新密碼和密碼記錄以確保此爲專屬密碼。爲了安全起見，會儲存先前密碼的數位簽章，新的密碼會與此項進行比對。
- **禁止的文字和屬性值** - 指定 ID 或密碼中不能包含的文字和屬性。

策略中的「不得包含」屬性

您可以在 UserUIConfig 配置物件中，變更所允許的「不得包含」屬性集。UserUIConfig 中列出了這些屬性，如下所示：

- <PolicyPasswordAttributeNames> - 策略類型「密碼」
- <PolicyAccountAttributeNames> - 策略類型「帳號 ID」
- <PolicyOtherAttributeNames> - 策略類型「其他」

字典策略

字典策略可讓 Identity Manager 根據文字資料庫來檢查密碼，以確保它們不會遭受簡單的字典攻擊。Identity Manager 可搭配使用此策略與其他策略設定來強制限定密碼的長度及結構，讓攻擊者難以使用字典來猜測系統所產生或變更的密碼。

字典策略可擴充密碼排除清單，您可以使用策略來設定該清單 (您可使用 [管理員介面] 密碼 [編輯策略] 頁中的 [不包含文字] 選項來實作這份清單)。

配置字典策略

若要設定字典策略，您必須：

- 配置字典伺服器支援
- 載入字典

若要設定字典策略，請執行以下步驟：

1. 開啓 [策略] 頁面 (第 176 頁)。
2. 按一下 **[配置字典]** 顯示 [字典配置] 頁。
3. 選取並輸入資料庫資訊：
   - **資料庫類型** - 選取要用來儲存字典之資料庫的類型 (Oracle、DB2、SQLServer 或 MySQL)。
   - **主機** - 輸入要執行資料庫之主機的名稱。
   - **使用者** - 輸入在連線資料庫時使用的使用者名稱。
   - **密碼** - 輸入在連線資料庫時使用的密碼。
   - **連接埠** - 輸入資料庫偵聽的連接埠。

- **連線 URL** - 輸入在連線時使用的 URL。以下是可用的範本變數：
  - `%h` - 主機
  - `%p` - 連接埠
  - `%d` - 資料庫名稱
- **驅動程式類別** - 輸入與資料庫進行互動時要使用的 JDBC 驅動程式類別。
- **資料庫名稱** - 輸入要載入字典之資料庫的名稱。
- **字典檔案名稱** - 輸入在載入字典時使用的檔案名稱。

4. 按一下 **[測試]** 可測試資料庫連線。
5. 如果連線測試成功，請按一下 **[載入文字]** 載入字典。載入作業可能得花費幾分鐘才能完成。
6. 按一下 **[測試]** 確認字典已正確載入。

實作字典策略

若要實作字典策略，請執行以下步驟：

1. 開啓 [策略] 頁面 (第 176 頁)。
2. 按一下 **[密碼策略]** 連結可編輯密碼策略。
3. 在 [編輯策略] 頁面中，選取 **[根據字典文字檢查密碼]** 選項。
4. 按一下 **[儲存]** 儲存變更。

實作之後，將根據字典來檢查所有變更和產生的密碼。

自訂電子郵件範本

Identity Manager 使用電子郵件範本傳送動作的資訊和請求給使用者和核准人。系統包括以下各項的範本：

- **存取檢閱通知** - 當需要檢閱使用者的存取權限時，傳送通知。必須修正或緩解存取策略的違規時，系統會傳送此通知。.
- **帳號建立核准** - 將通知傳送給核准人，告知正等待其核准新帳號。只要將相關角色的「佈建通知選項」設成核准，系統就會傳送此通知。
- **帳號建立通知** - 傳送通知，告知已使用特定角色的指定建立帳號。在 [建立角色] 或 [編輯角色] 頁面的 [通知收信人] 欄位中選取一或多位管理員時，系統將傳送此通知。
- **帳號刪除核准** - 將通知傳送給核准人,告知正在等待其核准使用者帳號刪除動作。在 [建立角色] 或 [編輯角色] 頁面的 [通知收信人] 欄位中選取一或多位管理員時，系統將傳送此通知。
- **帳號刪除通知** - 傳送通知，告知已刪除帳號。
- **帳號更新通知** - 將通知傳送至指定的電子郵件地址或使用者帳號，告知已更新帳號。
- **密碼重設** - 傳送通知，告知 Identity Manager 密碼已重設。根據相關的 Identity Manager 策略所選的「重設通知選項」值，系統會立即通知重設密碼的管理員 (在 Web 瀏覽器中)，或以電子郵件通知其密碼已重設的使用者。
- **密碼同步通知** - 通知使用者已在所有資源上成功完成密碼變更。通知會列出已成功更新的資源，並指出密碼變更請求的來源。
- **密碼同步失敗通知** - 通知使用者沒有在所有資源上成功完成密碼變更。通知會提供錯誤清單並指出密碼變更請求的來源。
- **策略違規通知** - 傳送通知，告知發生了帳號策略違規。
- **調解帳號事件**、**調解資源事件**、**調解摘要** - 分別從 [通知調解回應]、[通知調解開始] 和 [通知調解結束] 預設工作流程進行呼叫。通知將依照每個工作流程中的配置傳送。
- **報告** - 將所產生報告傳送給指定的收件者清單中的收件者。
- **請求資源** -傳送通知給資源管理員，告知已請求資源。當管理員從 [資源] 區域中請求資源時，系統會傳送此通知。

- **重試通知** - 傳送通知給管理員，告知對資源嘗試進行特定作業失敗的次數已達指定的次數。
- **風險分析** - 傳送風險分析報告。將一或多名電子郵件收件者指定爲資源掃描的部分時，系統將傳送此報告。
- **臨時密碼重設** - 傳送通知給使用者或角色核准人，告知已爲帳號提供臨時密碼。根據相關的 Identity Manager 策略所選的「密碼重設通知選項」值，系統會立即向使用者顯示通知 (在 Web 瀏覽器中)、以電子郵件通知使用者，或以電子郵件通知角色核准人。
- **User ID Recovery** - 傳送回復的使用者 ID 至指定的電子郵件地址。

編輯電子郵件範本

您可以自訂電子郵件範本以便爲收件者提供特定的指導，告知其如何完成作業或如何查看結果。例如，您可能要自訂 [帳號建立核准] 範本，以透過增加以下訊息來將核准人導向至帳號核准頁面：

請至 `http://host.example.com:8080/idm/approval/approval.jsp`，以核准爲 `$(fullname)` 所建立的帳號。

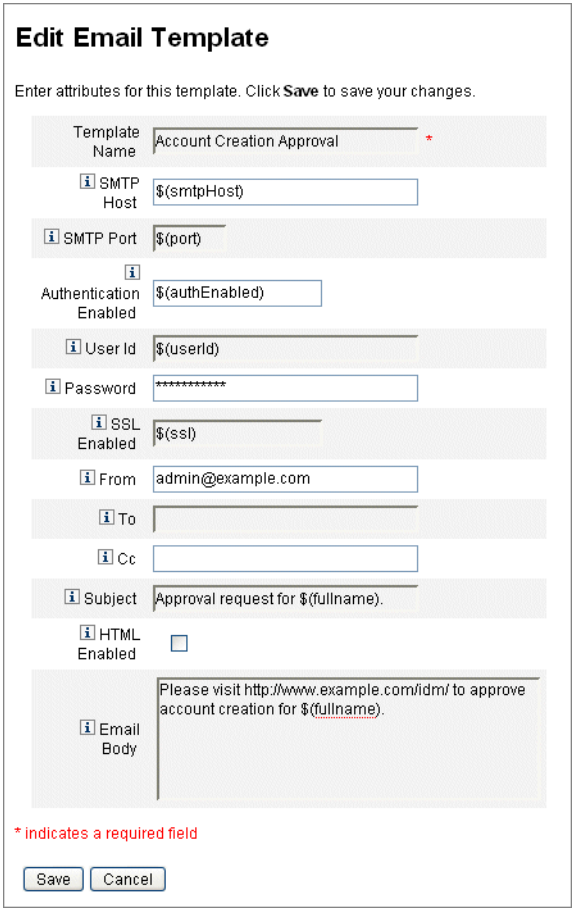
若要自訂電子郵件範本，請將 [帳號建立核准] 範本用做範例，並執行以下程序：

1. 在管理員介面中，按一下 **[配置]** 標籤，再按一下 **[電子郵件範本]** 子標籤。

   [電子郵件範本] 頁面會隨即開啓。

2. 按一下以選取 **[帳號建立核准]** 範本。

圖 5-3 編輯電子郵件範本



3. 輸入範本的詳細資訊：
   - 在 [SMTP 主機] 欄位中，輸入 SMTP 伺服器名稱，以便傳送電子郵件通知。
   - 在 [寄件者] 欄位中，自訂來源電子郵件地址。
   - 在 [收件者] 和 [副本] 欄位中，指定將會接收電子郵件通知的一個或多個電子郵件地址或 Identity Manager 帳號。
   - 在 [電子郵件內文] 欄位中，自訂內容以提供指向您的 Identity Manager 位置的指標。
4. 按一下 **[儲存]**。

您也可以使用 Identity Manager IDE 修改電子郵件範本。如需有關 IDE 的資訊，請參閱第 60 頁的 「Identity Manager IDE」。

電子郵件範本中的 HTML 和連結

您可以將 HTML 格式的內容插入電子郵件範本，以便在電子郵件訊息內文中顯示該內容。內容可包含文字、圖形和 Web 連結資訊。若要啓用 HTML 格式的內容，請選取 [啓用 HTML] 選項。

電子郵件內文中允許的變數

您也可以在電子郵件範本內文中包含變數參照，格式爲 $(*Name*)；例如：您的密碼 `$(password)` 已復原。

下表中定義每個範本所允許的變數。

表 5-1 電子郵件範本變數

範本	允許的變數
密碼重設	$(password) - 最新產生的密碼
更新核准	$(fullname) - 使用者的全名 $(role) - 使用者的角色
更新通知	$(fullname) - 使用者的全名 $(role) - 使用者的角色
報告	$(report) - 產生的報告 $(id) - 作業實例的編碼 ID $(timestamp) - 傳送電子郵件的時間
請求資源	$(fullname) - 使用者的全名 *$(resource) - 資源類型
風險分析	$(report) - 風險分析報告
臨時密碼重設	$(password) - 最新產生的密碼 $(expiry) - 密碼過期的日期

配置稽核群組和稽核事件

設定稽核配置群組可讓您記錄和報告您選取的系統事件。

稽核配置頁面

使用 [稽核配置] 頁面設定稽核群組。設定稽核群組可讓您稍後執行「稽核記錄」報告。

開啟稽核配置頁面

若要開啓 [稽核配置] 頁面，請執行以下步驟：

1. 開啓管理員介面。
2. 按一下 **[配置]** 標籤，然後再按一下 **[稽核]** 子標籤。

   [稽核配置] 頁面會隨即開啓。

配置稽核群組

配置稽核群組和事件需要 [配置稽核] 管理權能。

[稽核配置] 頁面若尚未開啓，請將其開啓 (請參閱上文步驟)。

[稽核配置] 頁面會顯示稽核群組清單，這些群組均可能包含一個或多個事件。您可以針對各個群組記錄成功事件、失敗事件或兩者均記錄。

按一下清單中的稽核群組以顯示 [編輯稽核配置群組] 頁面。此頁可讓您選取要在系統稽核記錄中當作稽核配置群組的一部份來記錄的稽核事件類型。

檢查是否已選取 **[啓用稽核]** 核取方塊。取消選取該核取方塊可停用稽核系統。

備註 如需有關稽核群組的更多資訊，請參閱 「稽核記錄」一章中的第 351 頁的 「稽核配置」。

編輯稽核配置群組中的事件

若要編輯群組中的事件，您可以新增或刪除某個物件類型的動作。若要執行此作業，請將該物件類型之 [動作] 欄中的項目從 **[可用]** 區域移至 **[已選取]** 區域，然後按一下 **[確定]**。

新增事件到稽核配置群組

若要將事件增加到群組，請按一下 **[新增]**。Identity Manager 會在頁面底部新增事件。從 **[物件類型]** 欄的清單中選取物件類型，然後將新物件類型之 **[動作]** 欄中的一個或多個項目，從 **[可用]** 區域移至 **[已選取]** 區域。按一下 **[確定]**，將事件增加到群組中。

Remedy 整合

您可以將 Identity Manager 與 Remedy 伺服器整合，使其根據指定的範本傳送 Remedy 票證。

在管理員介面的兩個區域中設定 Remedy 整合：

- **Remedy 伺服器設定** - 透過從 [資源] 區域建立 Remedy 資源來設定 Remedy 配置 (請參閱第 164 頁的「建立資源」)。在設定資源後，測試連線以確保啓用整合。
- **Remedy 範本** - 在設定 Remedy 資源後，定義 Remedy 範本。若要這麼做，請開啓管理員介面，按一下 **[配置]** 標籤，然後再按一下 **[Remedy 整合]**。然後您將選取 Remedy 模式和資源。

Remedy 票證的建立透過 Identity Manager 工作流程進行配置。根據您的喜好設定，可以在適當的時間進行呼叫，此呼叫將使用定義的範本開啓 Remedy 票證。如需有關配置工作流程的更多資訊，請參閱「Identity Manager Workflows, Forms, and Views」。

配置 Identity Manager 伺服器設定

您可以編輯伺服器特定設定，好讓 Identity Manager 伺服器只執行特定的作業。

若要配置伺服器專用的設定，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[配置]**，再按一下 **[伺服器]**。

   [配置伺服器] 頁面會隨即開啓。

2. 按一下 [配置伺服器] 頁面上清單內的伺服器，即可編輯個別伺服器的設定。

   Identity Manager 會顯示 [編輯伺服器設定] 頁面，在此您可以編輯調解器、排程程式、JMX 及其他設定。

調解器設定

調解器是執行調解的 Identity Manager 元件。若要瞭解調解，請參閱第 248 頁的「調解」。

若要配置調解器設定，請執行第 186 頁的「配置 Identity Manager 伺服器設定」中的步驟。選取 **[調解器]** 標籤。

依預設，調解器設定會顯示在 [編輯伺服器設定] 頁面中。您可以接受預設值，或取消選取 **[使用預設值]** 選項指定自訂的值。

備註 若要變更 Identity Manager 伺服器所使用的**預設**調解器設定，請參閱第 191 頁的「編輯預設伺服器設定」。

請使用下列設定配置調解器：

- **平行資源限制** - 指定調解器可以同時處理的最大資源執行緒數目。資源執行緒會將工作項目分配到工作者執行緒，所以，若增加額外的資源執行緒，可能也需要增加最大工作者執行緒數目。新安裝的預設值爲 **3**。
- **最小工作者執行緒** - 指定調解器會一直持續作用的處理中執行緒數目。新安裝的預設值爲 **2**。
- **最大工作者執行緒** - 指定調解器可以使用的處理中執行緒之最大數目。調解器僅會啓動工作負荷量所需的執行緒。如此會限制數目。工作者執行緒如閒置短時間，即會自動關閉。新安裝的預設值爲 **6**。

如需調校及疑難排解調解器的資訊，請參閱「Identity Manager 調校、疑難排解和錯誤訊息」。

檢視調解器狀態

若要檢視調解器狀態資訊，請開啓 [調解器狀態] 除錯頁面。

備註 您必須具備「除錯」權能，才能檢視 `/idm/debug/` 頁面。如需有關權能的資訊，請參閱第 217 頁的「指定權能」。

請將此 URL 鍵入瀏覽器，開啓 [調解器狀態] 除錯頁面：

```
http://<AppServerHost>:<Port>/idm/debug/Show_Reconciler.jsp
```

此處的 `AppServerHost` 是啓用調解器的主機。

請重新整理 [調解器狀態] 頁面，以檢視更新的調解器狀態資訊。如需有關此頁面的額外資訊，請按一下 **[說明]**。

排程程式設定

在 Identity Manager 中控制作業排程的是排程程式元件。

若要在特定的伺服器上配置排程程式設定，請執行第 186 頁的「配置 Identity Manager 伺服器設定」中的步驟。選取 **[排程程式]** 標籤。

您可以接受預設值，或取消選取 **[使用預設值]** 選項指定自訂的值。

- **排程程式啓動** - 選取排程程式在此伺服器上的啓動模式：
  - **自動** - 在伺服器啓動時即啓動。這是預設的啓動模式。
  - **手動** - 在伺服器啓動時啓動，但會保持暫停狀態，直到手動啓動。
  - **停用** - 在伺服器啓動時不要啓動。
- **啓用追蹤** - 選取此選項即可對此伺服器上的標準輸出啓動排程程式除錯追蹤。
- **最大同步運作作業數目** - 選取此選項即可指定排程程式在任何時間可執行的作業之最大數目 (而非預設值)。超過此限制的附加作業請求將會延遲或在其他伺服器上執行。
- **作業限制** - 指定可以在伺服器上執行的作業集。若要執行這個動作，請從可用作業清單中選取一項或多項作業。視您選取的選項而定，選取的作業清單可以是包含或排除清單。您可以選擇要允許清單中選取的作業以外的所有作業 (預設運作方式)，或只允許選取的作業。

按一下 **[儲存]** 以儲存伺服器設定的變更。

若要變更 Identity Manager 伺服器的預設排程程式設定，請參閱第 191 頁的「編輯預設伺服器設定」。

如需調校及疑難排解排程程式的資訊，請參閱 「Identity Manager 調校、疑難排解和錯誤訊息」。

電子郵件範本伺服器設定

若要配置 SMTP 伺服器設定，請執行第 186 頁的「配置 Identity Manager 伺服器設定」中的步驟。選取 **[電子郵件範本]** 標籤。

若不使用預設值，請清除 **[使用預設值]** 選項並輸入要使用的郵件伺服器，指定預設的電子郵件伺服器。您輸入的文字用於替代 [電子郵件範本] 中的 smtpHost 變數。

簡易郵件傳輸協定 (SMTP) 是在網際網路中傳輸電子郵件的標準。

若要變更 Identity Manager 伺服器的預設 SMTP 設定，請參閱第 191 頁的「編輯預設伺服器設定」。

JMX

Java 管理延伸 (JMX) 是一項 Java 技術，可讓您管理及 (或) 監視應用程式、系統物件、裝置及服務導向的網路。受管理/監視的實體以稱之爲 MBean 的物件表示 (意即「管理式 Bean」)。

本節說明如何在 Identity Manager 伺服器上配置 JMX，讓 JMX 用戶端得以監視系統的變化 (您也可以配置 Identity Manager 透過 JMX 提供稽核事件。如需相關資訊，請參閱第 375 頁)。

配置 JMX 輪詢設定

若要在個別伺服器上配置 JMX 輪詢設定，請執行以下步驟：

1. 請執行第 186 頁的「配置 Identity Manager 伺服器設定」中的步驟。選取 **[JMX]** 標籤。
2. 使用下列選項可啓用 JMX 叢集輪詢，並配置輪詢執行緒的間隔：
   - **啓用 JMX** - 使用此選項可啓用或停用 JMX 叢集 MBean 的輪詢執行緒。若要啓用 JMX，請清除預設選項 ([使用預設值 (false)])。因爲將系統資源用於輪詢循環，所以請僅在您要使用 JMX 時啓用此選項。
   - **輪詢間隔 (ms)** - 在啓用 JMX 後，使用此選項可變更伺服器輪詢儲存庫是否有變更的間隔時間。以毫秒爲單位指定間隔。

     預設論詢間隔爲 60000 毫秒。若要對其進行變更，請取消核取此選項的核取方塊，並在提供的輸入欄位中輸入新值。

3. 按一下 **[儲存]** 以儲存伺服器設定的變更。

備註 若要變更 Identity Manager 伺服器的**預設** JMX 輪詢設定，請參閱第 191 頁的「編輯預設伺服器設定」。

檢視 JMX 資料

使用 JMX 用戶端檢視 JMX 所收集的資料。包含在 JDK 1.5 的 JConsole 即爲此等用戶端。

在本機使用 JConsole

若要在伺服器執行所在的同一部機器上使用 JConsole，請設定下列特性：

- 設定 `JAVA_OPTS` 如下：
  - `-Dcom.sun.management.jmxremote`

JConsole 會使用正確的 PID 連線。

從遠端使用 JConsole

若要從遠端使用 JConsole，請設定下列特性：

- 設定 `JAVA_OPTS` 如下：
  - `-Dcom.sun.management.jmxremote.port=9004`
  - `-Dcom.sun.management.jmxremote.authenticate=false`
  - `-Dcom.sun.management.jmxremote.ssl=false`
- 在 `jre/lib/management` 目錄中，編輯 `jmxremote.access` 並確定下列兩行在檔案中未加註爲註釋：
  - `monitorRole readonly`
  - `controlRole readwrite`
- 若要查看 Identity Manager MBean，請使用與下列相似的 URL 連線至伺服器：

  `service:jmx:rmi:///jndi/rmi://localhost:9004/jmxrmi`

視環境之不同，也可能需要其他設定。如需更多資訊，請參閱 JConsole 文件。

備註 移至 Identity Manager 除錯頁面 (第 59 頁) 並按一下 **[顯示 MBean 資訊]**按鈕，亦可檢視 JMX 資料。

如需有關 JMX 的更多資訊，請瀏覽本網站：

http://java.sun.com/javase/technologies/core/mntr-mgmt/javamanagement/docs.jsp

編輯預設伺服器設定

預設伺服器設定功能可讓您爲所有的 Identity Manager 伺服器設定預設設定。除非您在個別伺服器設定頁中選取不同選項，否則伺服器會繼承這些設定。

若要編輯預設伺服器的設定，請執行以下步驟：

1. 在管理員介面中，按一下 **[配置] > [伺服器]**。

   [配置伺服器] 頁面會隨即開啓。

2. 按一下 **[編輯預設伺服器設定]**。

   [編輯預設伺服器設定] 頁面會隨即開啓。

[編輯預設伺服器設定] 頁面顯示與個別伺服器設定頁面一樣的選項。如需說明，請參閱文件中有關個別伺服器設定的各頁。

您對每個預設伺服器設定所做的變更會傳播至對應的個別伺服器設定，除非您取消選取該設定的使用預設選項。

按一下 **[儲存]** 以儲存伺服器設定的變更。

配置一般使用者介面

管理員只要修改管理員介面中的表單，即可配置特定方面的一般使用者介面。

若要設定在一般使用者介面中顯示資訊的選項，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[配置]**。
2. 按一下輔助功能表的 **[使用者介面]**。

   [使用者介面] 頁面會隨即開啓。
3. 完成並儲存表單的 **[一般使用者面板]** 部分。如需表單說明，請按一下 **[說明]**。

   如需完成表單的 **[匿名註冊]** 部分，請參閱第 113 頁的「匿名註冊」。

啟用一般使用者介面中的進程圖

進程圖係描述當一般使用者啓動請求或更新其設定檔時，Identity Manager 所遵循之工作流程。啓用時，在一般使用者送出表單之後，進程圖即會顯示在結果頁面中。

您必須先啓用管理員介面中的進程圖，才能啓用一般使用者介面中的進程圖。詳細資訊請參閱第 72 頁的「啓用進程圖」。

若要啓用一般使用者介面中的進程圖，請執行以下步驟：

1. 請依「配置一般使用者介面」中的步驟開啓 [使用者介面] 配置頁面。
2. 選取 **[啓用一般使用者進程圖]** 選項，其位於表單的 **[結果頁]** 區段中。

   若無法使用 **[啓用一般使用者進程圖]** 選項，則必須先啓用管理員介面中的進程圖。請參閱第 72 頁的「啓用進程圖」。
3. 按一下 **[儲存]**。

註冊 Identity Manager

竭誠歡迎管理員註冊 Identity Manager 安裝。

註冊需有 Sun Online 帳號及密碼。若無 Sun Online 帳號，請填寫下列位址的表單以註冊帳號：

https://reg.sun.com/register

從 [主控台] 或使用 [管理員] 介面皆可註冊 Identity Manager。

從 [主控台] 註冊還可讓您建立本機服務標籤，配合 Sun Service Tag 軟體使用可追蹤 Sun 系統、軟體及服務的資產管理。請務必先安裝服務標籤用戶端套裝軟體，再建立本機服務標籤。按一下以下位址的 [下載服務標籤] 按鈕，即可下載此套裝軟體：

http://inventory.sun.com/inventory

您應先使用可配置 Identity Manager 物件的管理員帳號登入，才能註冊 Identity Manager。此帳號應具備「產品註冊」權能。如需有關權能的資訊，請參閱第 217 頁的「指定權能」。

備註 您必須爲 Identity Manager 應用程式伺服器上的 Java 正確配置 SSL 功能，產品註冊功能才能發揮作用。`java.security` 檔案 (或等效檔案) 中所參照的所有 JAR 都必須出現。

從主控台註冊 Identity Manager

若要建立本機服務標籤，或透過網際網路向 Sun 註冊 Identity Manager，請執行以下步驟：

1. 在 Windows 上，於指令行鍵入下列內容，即可啓動 Identity Manager 主控台 (指令行) 介面：

   ```
   %WSHOME%\bin\lh
   ```

   在 Unix 上，於指令行中鍵入下列內容，即可啓動 Identity Manager 主控台 (指令行) 介面：

   ```
   $WSHOME/bin/lh
   ```

2. 請使用下列指令建立本機服務標籤：

   ```
   register -local
   ```

   請使用下列指令，透過網際網路向 Sun 註冊 Identity Manger：

   ```
   register -remote -u <userid> -p <password> -userSOA <soaUserid>
   -passSOA <soaPassword> -proxy <proxyHost> -port <proxyPortNumber>
   ```

   其中：

   - `userid` 是獲授權可執行註冊之 Identity Manager 管理員的 Identity Manager 使用者 ID
   - `password` 是獲授權可執行註冊之 Identity Manager 管理員的 Identity Manager 密碼
   - `soaUserid` 是用於註冊的 Sun Online 帳號之使用者 ID
   - `soaPassword` 是用於註冊的 Sun Online 帳號之密碼
   - `proxyHost` 是用於存取 Sun 線上註冊服務的網路代理伺服器。唯有當網路配置爲使用代理伺服器存取外部網際網路位址時才需要
   - `proxyPortNumber` 是用於存取 Sun 線上註冊服務之網路代理伺服器的連接埠。唯有當網路配置爲使用代理伺服器存取外部網際網路位址時才需要

register 指令

用法

```
register -local

register -remote [-u <userid> [-p <password>]] [-prompt] -userSOA <userid>
-passSOA <password> [-proxy <proxyHost> [-port <proxyPortNumber>]]
register [-help | -?]
```

選項

使用下列**選項**搭配 register 指令：

表 5-2 Syslog 指令選項

選項	描述
-local	在此主機上建立服務標籤。
-remote	透過網路直接向 Sun 註冊此 Identity Manager 安裝。
-u <userid>	獲授權可執行註冊之 Identity Manager 管理員的 Identity Manager 使用者 ID。
-p <password>	獲授權可執行註冊之 Identity Manager 管理員的 Identity Manager 密碼。
-prompt	缺少密碼時，以互動方式提示密碼。
-userSOA <userid>	要用於註冊的 Sun Online 帳號之使用者 ID。如使用 -remote 選項註冊即需要。
-passSOA <password>	要用於註冊的 Sun Online 帳號之密碼。如使用 -remote 選項註冊即需要。
-proxy <proxyHost>	用於存取 Sun 線上註冊服務的網路代理伺服器。唯有使用 -remote 選項註冊，以及當網路配置成使用代理伺服器存取外部網際網路位址時才需要。
-port <proxyPortNumber>	用於存取 Sun 線上註冊服務之網路代理伺服器的連接埠。唯有使用 -remote 選項註冊，以及當網路配置成使用代理伺服器存取外部網際網路位址時才需要。
-help | -?	將此指令的說明列示到主控台。

從管理員介面註冊 Identity Manager

若不需要建立本機服務標籤，請從管理員介面註冊 Identity Manager。

若要從管理員介面註冊 Identity Manager，請執行以下步驟：

1. 在管理員介面中，按一下 **[配置]**。
2. 按一下輔助功能表的 **[產品註冊]**。

   [產品註冊] 頁面會隨即開啓。
3. 填寫表單並按一下 **[立即註冊]**。按一下 [i-Helps] 以取得個別表單欄位的相關資訊。

備註 如果您的應用程式伺服器未配置成允許外寄 SSL 連線，可能會收到下列錯誤訊息：

由於無效的 Sun Online 帳號使用者/密碼而無法在 Sun Connection 伺服器上註冊。

若要解決此問題，請將適當的可信任根憑證增加至應用程式伺服器的金鑰庫。請參閱應用程式伺服器文件以取得詳細資訊。

備註 若舊版的 `xml-apis.jar` 及 `xercesImpl.jar` 出現在應用程式伺服器的類別路徑中，可能會收到下列錯誤訊息：

```
java.lang.NoSuchMethodError:org.w3c.dom.Node.getTextContent()L
java/lang/String;
```

若要解決此問題，請修改類別路徑，僅讓最新版的 `xml-apis.jar` 及 `xercesImpl.jar` 出現。

編輯 Identity Manager 配置物件

在管理 Identity Manager 的過程中，偶爾會需要您編輯 Identity Manager 系統配置物件 (亦稱之爲**系統配置檔案**) 或其他類似的物件。

若要使用管理員介面編輯物件，請執行以下步驟：

1. 請在瀏覽器中鍵入下列 URL，開啓 Identity Manager 的 [除錯] 頁面：

   `http://<AppServerHost>:<Port>/idm/debug/session.jsp`

   [系統設定] 頁面會隨即開啓。

備註 您必須具備 「除錯」權能，才能檢視 `/idm/debug/` 頁面。

2. 找到 **[列出物件]** 按鈕，然後從相鄰的 **[類型]** 下拉式清單中選取 **[配置]**。

   按一下 **[列出物件]** 按鈕。

   隨即會開啓 [列出物件類型：配置] 頁面。

3. 在物件清單中，找出所需物件，然後按一下 **[編輯]**。例如，若要編輯系統配置物件，請找到 **[系統配置]**，然後按一下 **[編輯]**。
4. 依指示編輯物件。
5. 按一下 **[儲存]**。
6. 若指示重新啓動伺服器，請遵照執行。

移除系統記錄檔中的記錄

系統記錄檔會擷取 Identity Manager 所產生的錯誤。系統記錄檔應定期截斷，以避免擴充得太大。請使用 [系統記錄檔維護作業] 移除系統記錄檔中的舊記錄。

若要排程作業以移除系統記錄檔中的舊記錄，請執行以下步驟：

1. 在管理員介面中，按一下 **[伺服器作業] > [管理排程]**。
2. 在 [可用於排程的作業] 區段中，按一下 **[系統記錄檔維護作業]**。

   [建立新的系統記錄檔維護作業作業排程] 頁面會隨即開啓。
3. 填寫表單並按一下 **[儲存]**。

第 6 章

管理

本章將提供有關在 Identity Manager 系統中執行一系列管理層級作業 (例如建立和管理 Identity Manager 管理員和組織) 的資訊與程序。還將提供有關如何在 Identity Manager 中使用角色、權能和管理角色的資訊。

這些資訊分別在以下主題中提供：

瞭解 Identity Manager 管理

Identity Manager 管理員是擁有許多 Identity Manager 權限的使用者。Identity Manager 管理員可管理：

- 使用者帳號
- 系統物件，例如角色與資源
- 組織

與使用者不同的是，Identity Manager 管理員可獲得指定的「權能」和「所控制的組織」。這些項目定義如下：

- **權能**。將存取權限授予 Identity Manager 使用者、組織、角色和資源的一系列權限。
- **所控制的組織**。指定管理員控制組織之後，管理員就可以管理該組織中的物件，以及該組織下層的所有組織。

託管

在大多數的公司中，執行管理作業的員工擁有特定責任。因此，這些管理員可以執行的帳號管理作業的範圍會有所限制。

例如，某管理員可能只負責建立 Identity Manager 使用者帳號。由於管理員的責任範圍有限，因此不大需要建立使用者帳號時所在資源的特定資訊，或關於系統內現有角色或組織的特定資訊。

Identity Manager 也可以限制管理員執行特定已定義範圍內之特定作業。

Identity Manager 如下支援權責區分與託管模型：

- 指定的**權能**會限制管理員只能執行特定的工作
- 指定的**所控制的組織**會限制管理員只能控制特定組織 (和那些組織內的物件)
- [建立使用者] 和 [編輯使用者] 頁面的篩選檢視，會讓管理員無法檢視與其工作責任無關的資訊。

當您設定新的使用者帳號或編輯使用者帳號時，可以從 [建立使用者] 頁面指定使用者的委派。

您也可以從 [工作項目] 標籤委託工作項目，例如要核准的請求。如需有關委派的更多資訊，請參閱第 230 頁的「委託工作項目」以取得詳細資訊。

建立管理員

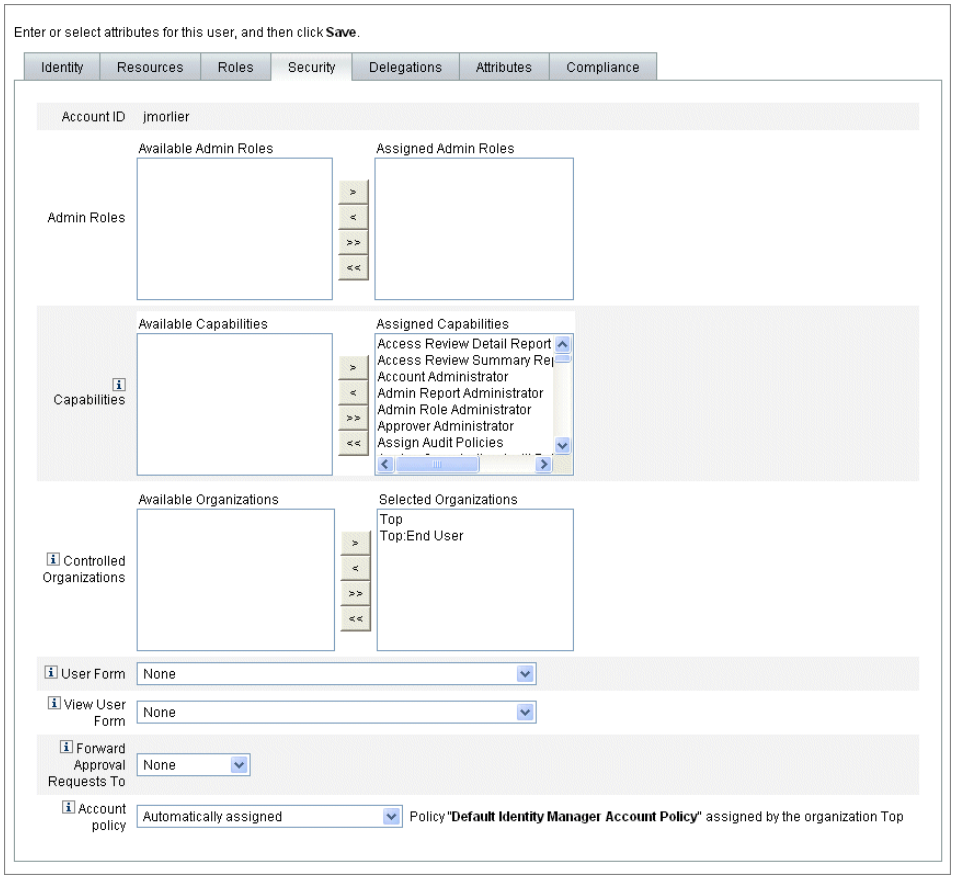
若要建立管理員，請將一個或多個權能指定給使用者，並指定要套用權能的組織。

若要建立管理員，請執行以下步驟：

1. 在管理員介面中，按一下功能表列的 **[帳號]**。[使用者清單] 頁面會隨即開啓。
2. 若要將管理權限授予現有使用者，請按一下使用者名稱 ([編輯使用者] 頁面會隨即開啓)，然後按一下 **[安全性]** 標籤。

   若需要建立新的使用者帳號，請參閱第 73 頁的「建立使用者」。
3. 依需要進行選擇，以建立管理控制：
   - **權能** - 選取一個或多個應該指定給此管理員的權能。此爲必要資訊。如需更多資訊，請參閱第 215 頁的「瞭解與管理權能」。
   - **所控制的組織** - 選取一個或多個應該指定給管理員的組織。管理員會控制所指定組織中的物件，以及階層中位於此組織以下之所有組織中的物件。此爲必要資訊。如需更多資訊，請參閱第 207 頁的「瞭解 Identity Manager 組織」。
   - **使用者表單** - 選取在建立和編輯 Identity Manager 使用者時，此管理員將使用的使用者表單 (若已指定該權能)。如果您不直接指定使用者表單，管理員將會沿用指定給他所屬組織的使用者表單。此處所選的表單會取代此管理員的組織內選定的任何表單。
   - **將核准請求轉寄給** - 選取一個使用者，以將目前擱置的所有核准請求轉寄給該使用者。此管理員設定也可以在 [核准] 頁面中設定。
   - **將工作項目委託給** - 如果可用，則使用此選項可指定使用者帳號的委派。您可以指定管理員的管理員、一個或多個選取的使用者，或使用委託核准人規則。

圖 6-1 [使用者帳號安全性] 頁面：指定管理員權限



篩選管理員檢視

藉由指定使用者表單給組織與管理員，您可以建立使用者資訊的特定管理員檢視。使用者資訊的存取權設定爲兩個層級：

- **組織** - 在建立組織時，您可以指定該組織中的所有管理員在建立與編輯 Identity Manager 使用者時，將使用的使用者表單。在管理員層級設定的任何表單將會覆寫此處設定的表單。若未替管理員或組織選取表單，Identity Manager 會繼承爲父組織選取的表單。若此處沒有設定表單，則 Identity Manager 會使用系統配置中設定的預設表單。
- **管理員** - 在指定使用者管理權能時，您可以直接將使用者表單指定給管理員。若您沒有指定表單，則管理員會繼承指定給其組織的表單 (或若沒有爲組織設定表單時，繼承系統配置中設定的預設表單)。

第 215 頁的「瞭解與管理權能」中說明您可以指定的內建 Identity Manager 權能。

變更管理員密碼

具有指定的管理員密碼變更權能的管理員或管理員所有者均可變更管理員密碼。

管理員可以使用下列表單，變更另一個管理員的密碼：

- **變更使用者密碼表單** - 開啓此表單的方式有兩種：
  - 按一下功能表中的 **[帳號]**。[使用者清單] 會隨即開啓。選取管理員，然後選取 **[使用者動作]** 清單中的 **[變更密碼]**。[變更使用者密碼] 頁面會隨即開啓。
  - 按一下功能表中的 **[密碼]** 。[變更使用者密碼] 頁面會隨即開啓。
- **標籤式使用者表單** - 按一下功能表中的 **[帳號]**。[使用者清單] 會隨即開啓。選取管理員，然後選取 **[使用者動作]** 功能表中的 **[編輯]**。[編輯使用者] 頁面 (標籤式使用者表單) 會隨即開啓。在 **[身份識別]** 表單標籤的 **[密碼]** 和 **[確認密碼]** 欄位中，鍵入新密碼。

管理員可以在 [密碼] 區域變更其自己的密碼。按一下功能表中的 **[密碼]**，然後按一下 **[變更我的密碼]**。

備註	套用到帳號的 Identity Manager 帳號策略會決定密碼限制，例如密碼到期時間、重設選項，與通知選擇。額外密碼限制可透過在管理員資源上所設定的密碼策略進行設定。

質疑管理員動作

您可配置讓 Identity Manager 在處理特定帳號變更之前，提示管理員輸入密碼。若認證失敗，則會取消帳號變更。

管理員可以使用三種表單來變更使用者密碼。這些表單是 [標籤式使用者] 表單、[變更使用者密碼] 表單和 [重設使用者密碼] 表單。若要確保在 Identity Manager 處理使用者帳號變更之前需要管理員輸入他們的密碼，請務必要更新此三個表單。

啟用標籤式使用者表單的詰問選項

若要在 [標籤式使用者] 表單上要求密碼詰問，請執行以下步驟。

1. 在管理員介面中，於瀏覽器內鍵入下列 URL，開啓 Identity Manager 除錯頁面 (第 59 頁) (您必須要有 [除錯] 權能才能開啓此頁面)。

   ```
   http://<AppServerHost>:<Port>/idm/debug/session.jsp
   ```

   [系統設定] 頁面 (Identity Manager 除錯頁面) 會隨即開啓。

2. 尋找 **[列出物件]** 按鈕，並從下拉式功能表選取 **[UserForm]**，然後按一下 **[ListObjects]** 按鈕。

   隨即會開啓 [列出物件類型：UserForm] 頁面。

3. 找到您在生產環境中使用的「標籤式使用者表單」副本，然後按一下 **[編輯]** (與 Identity Manager 一起發行的「標籤式使用者表單」是一種範本，而且不應該進行修改)。

4. 在 <Form> 元素內增加下列程式碼片段：

   ```
   <Properties>
     <Property name='RequiresChallenge'>
       <List>
         <String>password</String>
         <String>email</String>
         <String>fullname</String>
       </List>
     </Property>
   </Properties>
   ```

此特性的值，是可能包含下列一個或多個使用者檢視屬性名稱的清單：

- applications
- adminRoles
- assignedLhPolicy
- capabilities
- controlledOrganizations
- email
- firstname
- fullname
- lastname
- organization
- password
- resources
- roles

5. 儲存變更。

啟用 [變更使用者密碼] 和 [重設使用者密碼] 表單的詰問選項

若要在 [變更使用者密碼] 和 [重設使用者密碼] 表單上要求密碼詰問，請執行以下步驟：

1. 在管理員介面中，於瀏覽器內鍵入下列 URL，開啓 Identity Manager 除錯頁面 (第 59 頁) (您必須要有 [除錯] 權能才能開啓此頁面)。

   ```
   http://<AppServerHost>:<Port>/idm/debug/session.jsp
   ```

   [系統設定] 頁面 (Identity Manager 除錯頁面) 會隨即開啓。

2. 找到 **[列出物件]** 按鈕，並從下拉式功能表選取 **[UserForm]**，然後按一下 **[ListObjects]** 按鈕。

   隨即會開啓 [列出物件類型：UserForm] 頁面。

3. 找到您在生產環境中使用的「變更使用者密碼表單」副本，然後按一下 **[編輯]** (與 Identity Manager 一起發行的「變更使用者密碼表單」是一種範本，而且不應該進行修改)。

4. 找到 `<Form>` 元素，然後移至 `<Properties>` 元素。

5. 在 <Properties> 元素內增加下列一行，並儲存變更。

   ```
   <Property name='RequiresChallenge' value='true'/>
   ```

6. 重複步驟 3 - 5，但不要編輯您在生產環境中使用的「重設使用者密碼表單」副本。

變更認證問題的答案

使用 [密碼] 區域可變更您爲帳號身份驗證問題設定的答案。從功能表列中，選取 **[密碼]**，然後選取 **[變更我的答案]**。

如需有關認證的更多資訊，請參閱第 107 頁的 「使用者認證」。

在管理員介面中自訂管理員名稱顯示

在某些 Identity Manager 管理員介面頁面和區域中，可以依屬性 (例如電子郵件或完整名稱) 而非帳號 ID 顯示 Identity Manager 管理員，例如以下區域：

- 編輯使用者 (轉寄核准選項清單)
- 角色表格
- 建立/編輯角色
- 建立/編輯資源
- 建立/編輯組織/目錄結合
- 核准

若要將 Identity Manager 配置爲使用顯示名稱，請將以下內容增加到 UserUIConfig 物件中：

```
<AdminDisplayAttribute>
  <String>attribute_name</String>
</AdminDisplayAttribute>
```

例如，若要將電子郵件屬性作爲顯示名稱，請將以下屬性名稱增加到 UserUIconfig 中：

```
<AdminDisplayAttribute>
  <String>email</String>
</AdminDisplayAttribute>
```

瞭解 Identity Manager 組織

利用組織可執行以下動作：

- 有邏輯並安全地管理使用者帳號與管理員
- 限制對資源、應用程式、角色與其他 Identity Manager 物件的存取權

藉由建立組織並指定使用者至組織層級中的不同位置，您可以設定委託管理階段。包含一個或多個其他組織的組織稱爲父系組織。

所有 Identity Manager 使用者 (包括管理員) 皆靜態地指定給一個組織。使用者也可以被動態地指定給額外組織。

Identity Manager 管理員會額外指定，以控制組織。

建立組織

組織於 Identity Manager 帳號區域中建立。

若要建立組織，請執行以下步驟：

1. 在管理員介面中，按一下功能表列的 **[帳號]**。

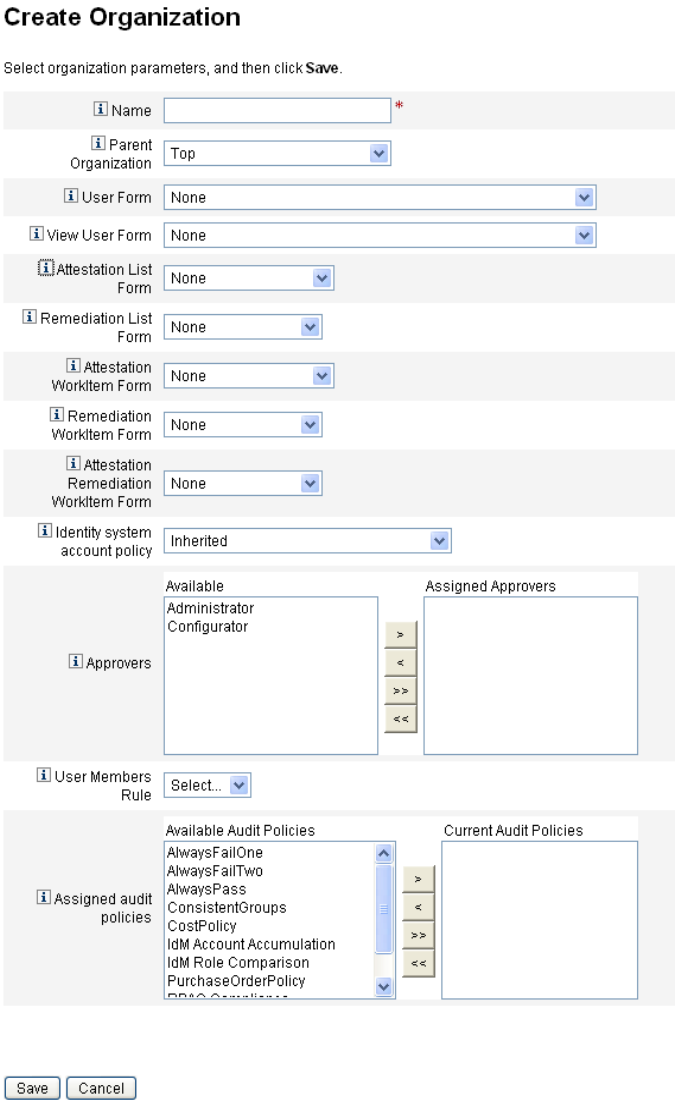
   [使用者清單] 頁面會隨即開啓。

2. 在 **[新動作]** 功能表中，選取 **[新組織]**。

提示 若要在組織階層的特定位置建立組織，請在清單中選取組織，然後選取 **[新動作]** 功能表中的 **[新組織]**。

圖 6-2 說明了 [建立組織] 頁面。

圖 6-2 [建立組織] 頁面



指定使用者給組織

每個使用者均爲一個組織的靜態成員，且可以是多個組織的動態成員。

組織成員身份定義如下：

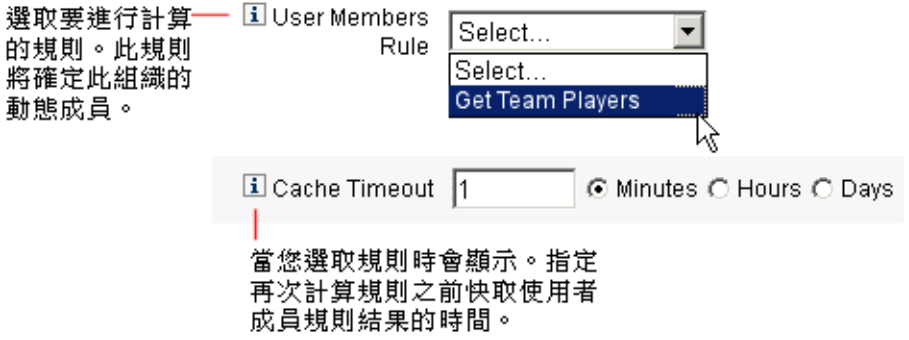
- **直接 (靜態) 指定** - 在 [建立使用者] 頁面或 [編輯使用者] 頁面中，直接將使用者指定給組織 (選取 **[身份]** 表單標籤可顯示 [組織] 欄位)。使用者必須直接指定給一個組織。
- **規則導向 (動態) 指定** - 透過指定給組織的 [使用者成員規則]，將使用者指定給組織。此規則在計算過後會傳回一組成員使用者。

  Identity Manager 會在下列情況計算 [使用者成員規則]：

  - 列出組織中的使用者時
  - 尋找使用者 (透過 [尋找使用者] 頁面)，包括搜尋位在具有使用者成員規則之組織中的使用者
  - 請求使用者存取權，但前提是目前的管理員會控制具有使用者成員規則的組織

從 [建立組織] 頁面的 **[使用者成員規則]** 欄位中選取使用者成員規則。圖 6-3 顯示使用者成員規則的範例。

圖 6-3　建立組織：使用者成員規則選取



使用者成員規則範例

以下範例顯示如何設定使用者成員規則，以動態控制組織的使用者成員身份。

備註 如需有關在 Identity Manager 中建立和使用規則的資訊，請參閱「Identity Manager Deployment Tools」。

金鑰定義與內含項

- 若要讓規則出現在 [使用者成員規則] 選項方塊中，其 `authType` 必須設爲 `authType='UserMembersRule'`。
- 上下文是目前驗證的 Identity Manager 使用者的階段作業。
- 定義的變數 (`defvar`) `Team players` 會爲作爲 Windows Active Directory 組織單位 (ou) `Pro Ball Team` 成員的每個使用者取得辨別名稱 (dn)。
- 對於找到的使用者，附加邏輯會將 `Pro Ball Team` ou 之每個成員使用者的 dn 與使用冒號前綴的 Identity Manager 資源名稱 (如 `:smith-AD`) 鏈結在一起。
- 傳回的結果將是與 Identity Manager 資源名稱鏈結的 dn 清單，格式爲 *dn*`:smith-AD`。

程式碼範例

下列程式碼範例說明使用者成員規則範例的語法。

編碼樣例 6-1 使用者成員規則範例

```
<Rule name='Get Team Players'
  authType='UserMembersRule'>
   <defvar name='Team players'>
      <block>
         <defvar name='player names'>
            <list/>
         </defvar>
   <dolist name='users'>
      <invoke class='com.waveset.ui.FormUtil'
     name='getResourceObjects'>
         <ref>context</ref>
         <s>User</s>
         <s>singleton-AD</s>
         <map>
            <s>searchContext</s>
            <s>OU=Pro Ball Team,DC=dev-ad,DC=waveset,DC=com</s>
            <s>searchScope</s>
            <s>subtree</s>
            <s>searchAttrsToGet</s>
            <list>
               <s>distinguishedName</s>
            </list>
         </map>
      </invoke>
      <append name='player names'>
      <concat>
         <get>
            <ref>users</ref>
            <s>distinguishedName</s>
         </get>
            <s>:sampson-AD</s>
      </concat>
      </append>
   </dolist>
      <ref>player names</ref>
   </block>
   </defvar>
      <ref>Team players</ref>
</Rule>
```

指定組織控制

從 [建立使用者] 或 [編輯使用者] 頁面中，指定一個或多個組織的管理控制。選取 **[安全性]** 表單標籤可顯示 [控制的組織] 欄位。

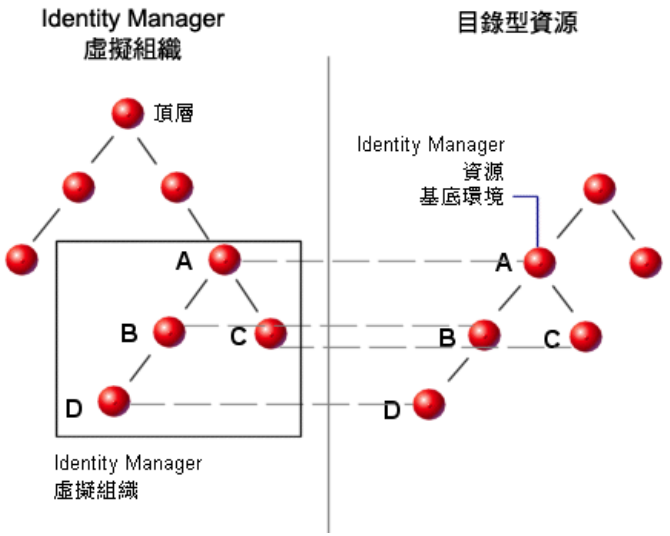
您也可以透過從 [管理員角色] 欄位指定一個或多個管理角色，來指定組織的管理控制。

瞭解目錄結合與虛擬組織

目錄結合是一組階層式的相關組織，對一個目錄資源中的一組實際階層式容器進行鏡像。目錄資源透過使用階層容器來使用階層名稱空間。目錄資源的範例有 LDAP 伺服器與 Windows Active Directory 資源。

目錄結合中的每個組織皆是**虛擬組織**。目錄結合中最頂層的虛擬組織是表示定義於資源中的基底環境的容器的鏡像。目錄結合中其餘的虛擬組織爲頂層虛擬組織的直接或間接子系組織，是所定義資源基底環境容器之子系目錄資源容器的鏡像。圖 6-4 說明了此結構。

圖 6-4　　Identity Manager 虛擬組織



可以在任一點將目錄結合連接至現有 Identity Manager 組織結構。然而，不能在現有目錄結合之內或之下連接目錄結合。

您將目錄結合增加至 Identity Manager 組織樹後，可以建立或刪除該目錄結合中上下文裡的虛擬組織。除此之外，您可以隨時重新整理內含目錄結合的虛擬組織集，來確保其與目錄資源容器保持同步。您無法在目錄結合中建立非虛擬組織。

您可以使用與 Identity Manager 組織相同的方式來建立虛擬組織的 Identity Manager 物件 (例如使用者、資源與角色) 成員，並可用於其中。

設定目錄結合

若要設定目錄結合，請執行以下步驟：

1. 在管理員介面中，選取功能表列的 **[帳號]**。

   [使用者清單] 頁面會隨即開啓。

2. 在 [帳號] 清單中選取 Identity Manager 組織。您選取的組織將成爲設定的虛擬組織的父系組織。

   然後，在 **[新動作]** 功能表中，選取 **[新目錄結合]**。

   Identity Manager 會開啓 [建立目錄結合] 頁面。

3. 選取設定虛擬組織的選項：

   - **父系組織** - 這個欄位包含您從 [帳號] 清單中選取的組織；不過，您也可以從清單中選取不同的父系組織。
   - **目錄資源** - 選取用於管理現有目錄的目錄資源，此目錄資源的結構會在虛擬組織中進行鏡像。
   - **使用者表單** - 選取要套用至這個組織中的管理員之使用者表單。
   - **Identity Manager 帳號策略** - 選取策略，或選取預設選項 (繼承) 以繼承父系組織的策略。
   - **核准人** - 選取可以對與這個組織相關的請求進行核准的管理員。

重新整理虛擬組織

此程序從選取的組織開始，向下重新整理虛擬組織並使之與相關目錄資源重新同步化。在清單中選取虛擬組織，然後在 [組織動作] 清單中，選取 [重新整理組織]。

刪除虛擬組織

刪除虛擬組織時，您可以從兩個刪除選項中選取：

- 僅刪除 Identity Manager 組織 - 僅刪除 Identity Manager 目錄結合。
- 刪除 Identity Manager 組織和資源容器 - 刪除 Identity Manager 目錄結合與本機資源上的對應組織。

選取一個選項，然後按一下 **[刪除]**。

瞭解與管理權能

權能爲 Identity Manager 系統中的多組權利。權能表示管理工作責任，例如重設密碼或管理使用者帳號。每個 Identity Manager 管理使用者均被指定了一項或多項權能，這會提供一組不會危及資料保護的權限。

您不需爲所有的 Identity Manager 使用者指定權能。只有透過 Identity Manager 執行一個或多個管理動作的使用者才需要權能。例如，使用者不需要指定的權能即可變更其密碼，但是若要變更其他使用者的密碼，則需有指定的權能。

爲您指定的權能會掌控您可存取 Identity Manager 管理介面的哪些區域。所有 Identity Manager 管理使用者可以存取特定的 Identity Manager 區域，包括：

- **[首頁]** 和 **[說明]** 標籤
- **[密碼]** 標籤 (僅限 **[變更我的密碼]** 和 **[變更我的答案]** 子標籤)
- **[報告]** (限於和管理員的特定責任相關的類型)

備註 第 619 頁的附錄 D「權能定義」含有 Identity Manager 的預設作業型和功能性權能清單 (含定義)。本附錄也會列出可利用各作業型權能存取的標籤及子標籤。

權能類別

Identity Manager 定義權能如下：

- 作業型。這些是位於最簡單作業層級上的權能。
- 功能性。功能性權能包含一個或多個其他功能性權能或作業型權能。

內建權能 (隨 Identity Manager 系統提供) 是受保護的，表示您無法對其進行編輯。但是您可以在建立的權能中使用它們。

受保護 (內建) 權能在清單中以紅色鑰匙 (或紅色鑰匙及資料夾) 圖示標示。您建立並可編輯的權能在權能清單中以綠色鑰匙 (或綠色鑰匙及資料夾) 圖示標示。

使用權能

本節說明如何建立、編輯、指定和重新命名權能。您必須以 [權能] 功能執行這些作業。

檢視權能頁面

[權能] 頁面位於 [安全性] 標籤下方。

若要開啓 [權能] 頁面，請執行以下步驟：

1. 在管理員介面中，按一下頂層功能表的 **[安全性]**。
2. 按一下輔助功能表的 **[權能]**。

   [權能] 頁面會隨即開啓，並顯示 Identity Manager 權能清單。

建立權能

使用下列程序可建立權能。若要複製權能，請參閱第 217 頁的「儲存並重新命名權能」。

若要建立權能，請執行以下步驟：

1. 在管理員介面中，按一下頂層功能表的 **[安全性]**。
2. 按一下輔助功能表的 **[權能]**。

   [權能] 頁面會隨即開啓，並顯示 Identity Manager 權能清單。
3. 按一下 **[新增]**。

   [建立權能] 頁面會隨即開啓。
4. 如下完成表單：
   a. 命名新的權能。
   b. 在 **[權能]** 區段中，使用箭號按鈕將應指定給使用者的權能移動至 **[指定的權能]** 方塊中。
   c. 在 **[指定者]** 方塊中，選取一或多位可將此權能指定給其他使用者的使用者。如果未選取任何使用者，則只有建立該權能的使用者能夠指定此權能。若建立權能的使用者並未指定「指定使用者權能」權能，則必須選取一或多位使用者，以確保至少有一位使用者能夠將權能指定給其他使用者。
   d. 在 **[組織]** 方塊中，選取一個或多個可以使用此權能的組織。
   e. 按一下 **[儲存]**。

備註 可供您選取指定者的使用者集，就是已具備 [指定權能] 權限的使用者。

編輯權能

您可以編輯「非保護的權能」。

若要編輯非保護的權能，請執行以下步驟：

1. 在管理員介面中，按一下頂層功能表的 **[安全性]**。
2. 按一下輔助功能表的 **[權能]**。

   [權能] 頁面會隨即開啓，並顯示 Identity Manager 權能清單。
3. 在清單中的權能上按一下滑鼠右鍵，然後選取 **[編輯]**。[編輯權能] 頁面會隨即開啓。
4. 進行變更，然後按一下 **[儲存]**。

您無法編輯內建權能。不過，您可以使用不同的名稱儲存它們，以建立您自己的權能。也可以在您建立的權能中使用內建權能。

儲存並重新命名權能

您可以使用新名稱儲存現有的權能，以建立新的權能。此程序稱爲複製權能。

若要複製權能，請執行以下步驟：

1. 在管理員介面中，按一下頂層功能表的 **[安全性]**。
2. 按一下輔助功能表的 **[權能]**。

   [權能] 頁面會隨即開啓，並顯示 Identity Manager 權能清單。
3. 在清單中的權能上按一下滑鼠右鍵，然後選取 **[另存新檔]**。

   隨即開啓一個對話方塊，要求您鍵入新權能的名稱。
4. 請鍵入名稱，然後按一下 **[確定]**。

現在即可編輯新的權能。

指定權能

使用 [建立使用者] 頁面 (第 73 頁) 或 [編輯使用者] 頁面 (第 78 頁)，將權能指定給使用者。您也可以透過指定管理員角色 (透過介面中的 [安全性] 區域設定) 將權能指定給使用者。詳細資訊請參閱第 218 頁的「瞭解與管理管理員角色」。

備註 第 619 頁的附錄 D「權能定義」含有 Identity Manager 的預設作業型和功能性權能清單 (含定義)。本附錄也會列出可利用各作業型權能存取的標籤及子標籤。

瞭解與管理管理員角色

管理員角色定義兩個項目，分別是一組權能以及控制範圍 (專有名詞**控制範圍**指的是一個或多個受管組織)。定義之後，就可以將管理員角色指定給一或多位管理員。

備註 請勿將角色與管理員角色混淆。角色是用來管理一般使用者對外部資源的存取權，而管理員角色主要是用以管理 Identity Manager 管理員對 Identity Manager 物件的存取權。

本節所呈現的資訊是針對管理員角色。如需有關角色的資訊，請參閱第 118 頁的「瞭解與管理角色」。

一個管理員可以有多個管理員角色。如此可讓管理員在某個控制範圍內擁有一組權能，而在另一個控制範圍內擁有另一組權能。例如，一個管理員角色可以針對在該管理員角色中所指定的控制組織，授予管理員建立和編輯使用者的權限。不過，第二個指定給相同管理員的管理員角色，可能只會獲得該管理員角色中所定義之不同控制組織集內的「變更使用者密碼」權限。

管理員角色可重複使用成對的權能和控制範圍。管理員角色也可簡化大量使用者的管理員權限之管理。管理員角色應用以授予管理員權限，而非直接將權能和所控制的組織指定給個別使用者。

您可以將權能及 (或) 組織**直接**或**動態** (間接) 指定給管理員角色：

- **直接** - 使用此方法，會將權能及/或所控制的組織明確指定給管理員角色。例如，您可以將「使用者報告管理員」權能和所控制的組織 *Top* 指定給管理員角色。
- **動態** (間接) - 此方法使用規則來指定權能和所控制的組織。已獲得管理員角色的管理員每次登入時，系統都會計算規則。而在認證管理員之後，規則會動態地判斷要指定哪一組權能及 (或) 所控制的組織。

  例如，當使用者登入時：

  - 若其 Active Directory (AD) 使用者職稱爲管理員，則權能規則可能會傳回**「帳號管理員」**作爲要指定的權能。
  - 若其 Active Directory (AD) 使用者部門爲行銷，則所控制的組織規則可能會傳回「行銷」作爲要指定之所控制的組織。

備註 您可以針對每個登入介面，啓用或停用將管理員角色動態指定給使用者的功能 (例如，[使用者] 介面或 [管理員] 介面)。若要執行此作業，請將下列系統配置屬性設爲 `true` 或 `false`：

`security.authz.checkDynamicallyAssignedAdminRolesAtLoginTo.logininterface`

所有介面的預設均爲 `false`。

如需有關編輯系統配置物件的說明，請參閱第 197 頁。

管理員角色規則

Identity Manager 提供可用以建立管理員角色規則的規則範例。您可以在 Identity Manager 安裝目錄的 `sample/adminRoleRules.xml` 中找到這些規則。

表 6-1 提供您必須指定給每個規則的規則名稱和 `authType`。

表 6-1 管理員角色規則範例

規則名稱	authType
所控制的組織規則	ControlledOrganizationsRule
權能規則	CapabilitiesRule
已為使用者指定管理員角色規則	UserIsAssignedAdminRoleRule

備註 如需有關爲服務提供者使用者管理員角色提供之規則範例的資訊，請參閱「服務提供者管理」一章中第 567 頁的「託管」。

使用者管理員角色

Identity Manager 包含內建管理員角色，稱爲「使用者管理員角色」。依預設，未向其指定權能或所控制的組織。您無法將其刪除。此管理員角色在登入時即已隱式指定給所有使用者 (一般使用者及管理員)，而與其登入的介面 (例如使用者、管理員、主控台或 IDE) 無關。

備註 如需有關爲服務提供者使用者建立管理員角色的資訊，請參閱「服務提供者管理」一章中第 567 頁的「託管」。

您可以透過管理員介面編輯使用者管理員角色 (選取 **[安全性]**，然後選取 **[管理員角色]**)。

由於透過此管理員角色靜態指定的任何權能或所控制的組織，會指定給所有的使用者，所以建議透過規則來指定權能與所控制的組織。這將使不同的使用者有不同的權能 (或沒有權能)，而且指定將根據某些因素 (例如他們的身分、所屬的部門或是否爲管理員) 來確定範圍，這些因素可以在規則的上下文中查詢。

使用者管理員角色不停用或替代工作流程中使用的 `authorized=true` 旗標。當使用者不應存取由工作流程存取的物件時，此旗標依然適用，除非工作流程正在執行。本質上來說，這會讓使用者進入以超級使用者身份執行模式。

不過，在部分情況下，使用者可能應該擁有工作流程以外 (也可能是以內) 之一個或多個物件的特定存取權。在這種情況下，如果使用的規則能動態指定權能和所控制的組織，可對這些物件進行細部授權。

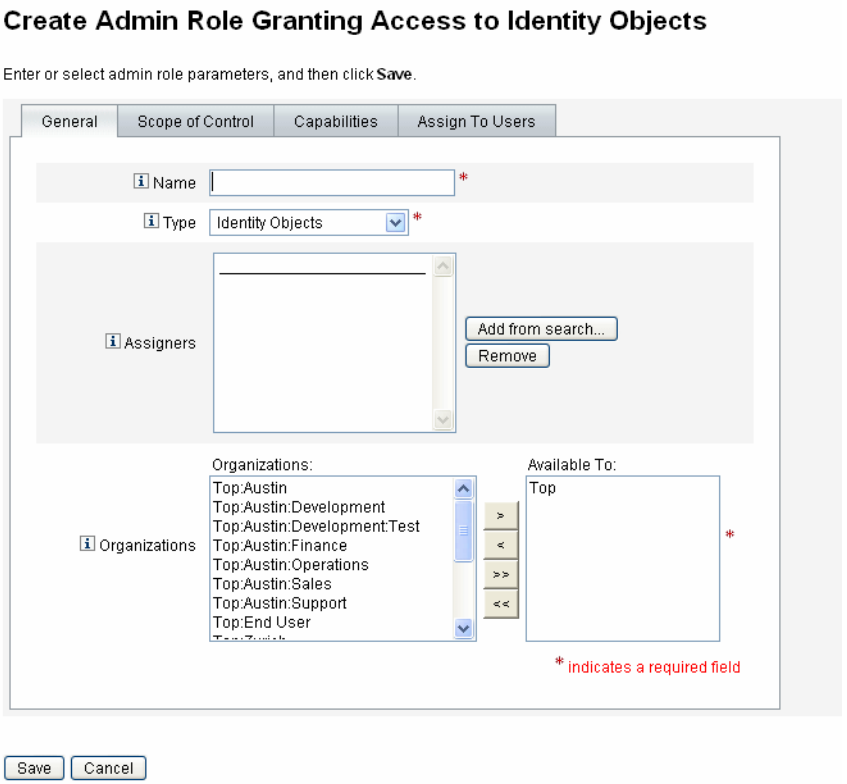
建立和編輯管理員角色

若要建立或編輯管理員角色，必須要爲您指定「管理員角色管理員」權能。

若要在管理員介面中存取管理員角色，請按一下 **[安全性]**，然後按一下 **[管理員角色]** 標籤。[管理員角色] 清單頁可讓您爲 Identity Manager 使用者和服務提供者使用者建立、編輯和刪除管理員角色。

若要編輯現有的管理員角色，請按一下清單中的名稱。按一下 **[新增]** 以建立管理員角色。Identity Manager 會顯示 [建立管理員角色] 選項 (如圖 6-5 所示)。[建立管理員角色] 檢視顯示四個標籤，您可以用來指定一般屬性、權能和新管理員角色的範圍，以及將角色指定給使用者。

圖 6-5　管理員角色建立頁面：[一般] 標籤



[一般] 標籤

可使用 [建立管理員角色] 或 [編輯管理員角色] 檢視的 [一般] 標籤來指定管理員角色的以下基本特徵：

- **名稱** - 此管理員角色的專屬名稱。

  例如，您可以爲對財務部門 (或組織) 中的使用者具有管理權能的使用者建立財務管理員角色

- **類型** - 選取 **[Identity 物件]** 或 **[服務提供者使用者]** 類型。這是必填欄位。

  如果您爲 Identity Manager 使用者 (或物件) 建立管理員角色，請選取 [Identity 物件]。如果您建立管理員角色是爲了將存取權限授予服務提供者使用者，請選取 [「服務提供者」使用者]。

備註 如需有關建立管理員角色以便將存取權限授予服務提供者使用者的資訊，請參閱「服務提供者管理」一章中第 567 頁的「託管」。

- **指定者** - 選取或搜尋可以將此管理員角色指定給其他使用者的使用者。可供您在其中進行選取的使用者集 (即已具備 [指定權能] 權限的使用者)。

  如果未選取任何使用者，則唯一能夠指定此管理員角色的使用者爲建立此管理員角色的使用者。如果建立該管理員角色的使用者並沒有指定 [指定使用者權能] 權能，請選取一個或多個使用者作爲 [指定者]，以確保至少有一位使用者能夠爲其他使用者指定管理員角色。

- **組織** - 選取可使用此管理員角色的一個或多個組織。這是必填欄位。

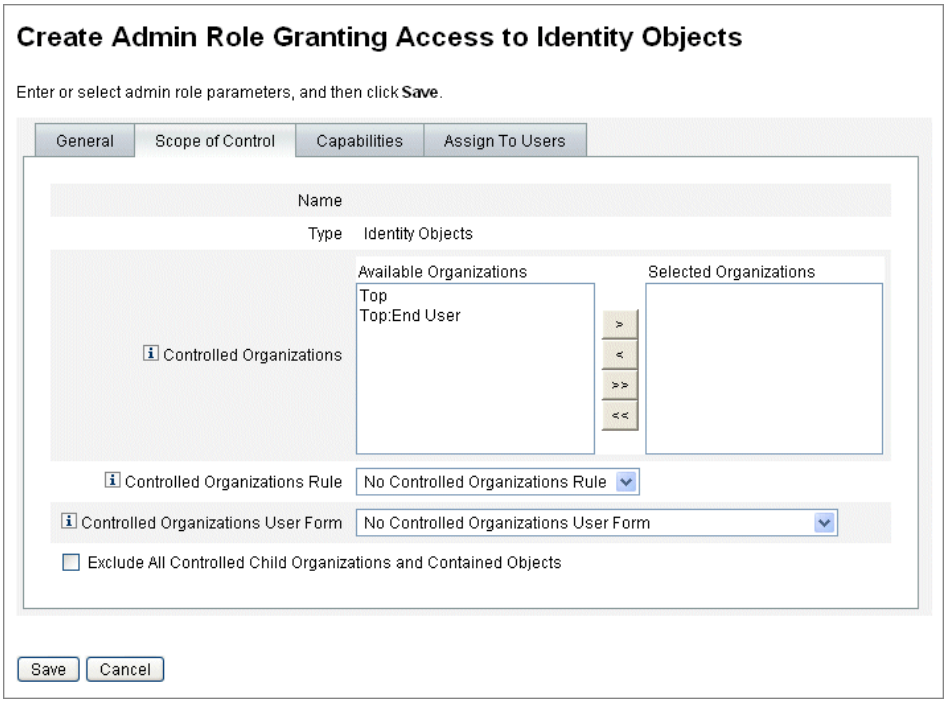
  管理員可管理階層中指定組織或指定組織下的任何組織中的物件。

控制範圍

Identity Manager 可讓您控制一般使用者之控制範圍內的使用者。

使用 [控制範圍] 標籤 (如圖 6-6 所示) 可指定此組織成員可管理的組織，或指定規則以確定管理員角色之使用者所要管理的組織，以及爲管理員角色選取使用者表單。

圖 6-6　　建立管理員角色：控制範圍



- **所控制的組織** - 從 [可用組織] 清單中選取此管理員角色有權管理的組織。
- **所控制的組織規則** - 選取規則，在使用者登入時會對該規則進行計算，以確定已具有此管理員角色的使用者所要控制的多個組織，或不控制任何組織。選取的規則必須具有 `ControlledOrganizationsRule` authType。依預設，不會選取任何所控制的組織規則。

備註 您可以使用 EndUserControlledOrganizations 規則根據組織需求定義所有必要的邏輯，以確保能委託給正確的一組使用者。

若要使用者的範圍清單與管理員的範圍清單相同，不論這些使用者登入管理員介面或一般使用者介面，皆必須如下變更 EndUserControlledOrganizations 規則：

將規則修改爲先檢查認證使用者是否爲管理員，然後再配置下列項目：

- 若使用者不是管理員，則會傳回應由一般使用者所控制的一組組織，例如使用者本身的組織 (例如 waveset.organization)。
- 如果使用者是管理員，則不傳回任何組織，如此使用者僅會控制指定的組織，因爲此使用者便是管理員。

例如：

```
<Rule protectedFromDelete='true'
      authType='EndUserControlledOrganizationsRule'
      id='#ID#End User Controlled Organizations'
      name='End User Controlled Organizations'>
  <Comments>
    如果登入的使用者不是 Idm 管理員，
    則傳回其所屬的組織。
    否則，會傳回空值。
  </Comments>
  <cond>
    <and>
      <isnull><ref>waveset.adminRoles</ref></isnull>
      <isnull><ref>waveset.capabilities</ref></isnull>
      <isnull><ref>waveset.controlledOrganizations</ref></isnull>
    </and>
    <ref>waveset.organization</ref>
  </cond>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Top' name='Top'/>
  </MemberObjectGroups>
</Rule>
```

- **所控制的組織使用者表單** - 選取使用者表單，已具有該管理員角色的使用者將在建立或編輯屬於此管理員角色之所控制的組織使用者時，使用該表單。依預設，不會選取任何所控制的組織使用者表單。

  透過管理員角色指定的使用者表單會置換從管理員所在組織繼承的任何使用者表單。不會置換直接指定給管理員的使用者表單。

指定權能

指定給管理員角色的權能決定已指定該管理員角色之使用者的權限。例如，此管理員角色可能被限制於僅爲其所控制的組織建立使用者。在這種情況下，您可以指定建立使用者權能。

在 [權能] 標籤上，可選取以下選項：

- **權能** - 這是一些特定的權能 (即管理權限)，管理員角色的使用者將具有這些權能以用於其所控制的組織。您可以從可用權能清單中選取一個或多個權能，並將它們移至 [指定的權能] 清單。
- **權能規則** - 選取規則，在使用者登入時會對該規則進行計算，以決定爲已具有該管理員角色之使用者授予一份包含多個權能的清單，或不授予任何權能。選取的規則必須具有 `CapabilitiesRule` authType。

將使用者表單指定給管理員角色

您可將使用者表單指定給管理員角色的成員。使用 [建立管理員角色] 或 [編輯管理員角色] 檢視中的 [指定給使用者] 標籤來指定此指定。

指定管理角色的管理員在建立或編輯使用者 (隸屬該管理角色所控制的組織) 時，將使用這個使用者表單。透過管理員角色指定的使用者表單會置換從管理員所在組織繼承的任何使用者表單。不會置換直接指定給管理員的使用者表單。

編輯使用者時將使用的使用者表單取決於以下優先順序：

- 如果直接將使用者表單指定給管理員，則會使用該表單。
- 如果沒有將使用者表單直接指定給管理員，但管理員已被指定可執行下列功能的管理員角色：
  - 控制正在建立或編輯的使用者爲其成員的組織，而且
  - 指定使用者表單

  則會使用該使用者表單。
- 如果沒有爲管理員直接指定或透過管理員角色間接指定任何使用者表單，則會使用指定給管理員之成員組織 (從管理員的成員組織開始，直到 `Top` 組織的下一層級) 的使用者表單。
- 如果沒有指定使用者表單給任何一個管理員成員組織，則會使用預設使用者表單。

如果管理員被指定多個管理員角色，這些角色控制相同的組織但指定了不同的使用者表單，則當其嘗試在該組織中建立或編輯使用者時會顯示錯誤。如果管理員嘗試指定兩個或兩個以上控制相同組織但指定了不同使用者表單的管理員角色，則會顯示錯誤。除非解決衝突，否則無法儲存變更。

一般使用者組織

「一般使用者」組織提供便利的方式，讓管理員製作一般使用者可以使用的特定物件 (例如資源和角色)。一般使用者可以使用一般使用者介面 (第 56 頁) 檢視指定的物件，也可能可以將指定的物件指定給他們自己 (擱置核准程序)。

備註

「一般使用者」組織在 Identity Manager 7.1.1 版時開始採用。

以前若要讓一般使用者存取 Identity Manager 配置物件 (例如 [角色]、[資源]、[作業] 等)，管理員必須編輯配置物件，並使用 [一般使用者作業]、[一般使用者資源] 和 [一般使用者 authType]。

現在，Sun 建議使用 「一般使用者」組織讓一般使用者存取 Identity Manager 配置物件。

「一般使用者」組織由所有使用者隱式控制，並讓使用者可檢視數種類型的物件 (包含作業、規則、角色和資源)。不過，組織在一開始時並沒有任何成員物件。

「一般使用者」組織是 Top 的成員，不得具有子組織。此外，「一般使用者」組織不會顯示在 [帳號] 頁面清單中。不過，在編輯物件 (例如 [角色]、[管理員角色]、[資源]、[策略]、[作業] 等) 時，您可以使用管理員使用者介面讓 「一般使用者」組織可以使用所有物件。

當一般使用者登入一般使用者介面時，會發生下列情況：

- 一般使用者已獲得 EndUser 組織的控制權 (ObjectGroup)
- Identity Manager 會計算內建「一般使用者所控制的組織」規則。此規則會自動讓使用者控制由規則所傳回的所有組織名稱。(此規則於 Identity Manager 7.1.1 版時加入。下節將予以說明)。
- 一般使用者已獲得 EndUser 權能中指定之物件類型的權限。

一般使用者所控制的組織規則

「一般使用者所控制的組織」規則的輸入引數，是認證使用者的檢視。Identity Manager 預期此規則會傳回的項目，是登入 [一般使用者] 介面的使用者將會控制的一個或多個組織。Identity Manager 預期此規則會傳回字串 (針對單一組織) 或清單 (針對多個組織)。

若要管理這些物件，使用者需要「一般使用者管理員」權能。已獲得「一般使用者管理員」權能的使用者，可檢視和修改「一般使用者所控制的組織」規則之內容。這些使用者也可檢視與修改 EndUser 權能中指定的物件類型。

「一般使用者管理員」權能預設會指定給「配置程式」使用者。而針對已登入的使用者，並不會動態反映任何清單變更或「一般使用者所控制的組織」規則評估後傳回的組織變更。這些使用者必須先登出再重新登入，才能察覺變更。

若「一般使用者所控制的組織」規則傳回無效的組織 (例如 Identity Manager 中不存在的組織)，則會在系統記錄檔中記錄此問題。若要更正此問題，請登入 [管理員] 使用者介面，並修正規則。

管理工作項目

由 Identity Manager 中作業產生的某些工作流程程序可建立動作項目或工作項目。這些工作項目可能是核准請求，或指定給 Identity Manager 帳號的某些其他動作請求。

Identity Manager 將所有工作項目聚集到介面的 [工作項目] 區域中，以使您可以從一個位置檢視和回應所有擱置請求。

工作項目類型

工作項目可以是以下任一類型：

- **核准** - 對新帳號或帳號變更進行核准的請求。
- **驗證作業** - 對使用者權限進行檢閱及核准的請求。
- **修正** - 對使用者帳號策略違規進行修正或緩解的請求。
- **其他** - 除以上標準類型之外的動作項目請求。即從自訂工作流程中產生的動作請求。

若要檢視每個工作項目類型的擱置工作項目，請按一下功能表的 **[工作項目]**。

備註 如果您是具有擱置工作項目 (或委託工作項目) 的工作項目所有者，則在您登入 Identity Manager 使用者介面時會顯示您的 [工作項目] 清單。

處理工作項目請求

若要回應工作項目請求，請按一下介面之 [工作項目] 區域中的一個工作項目類型。從請求清單中選取項目，然後按一下一個可用按鈕以指示您要執行的動作。工作項目選項因工作項目類型而異。

如需有關回應請求的更多資訊，請參閱以下主題：

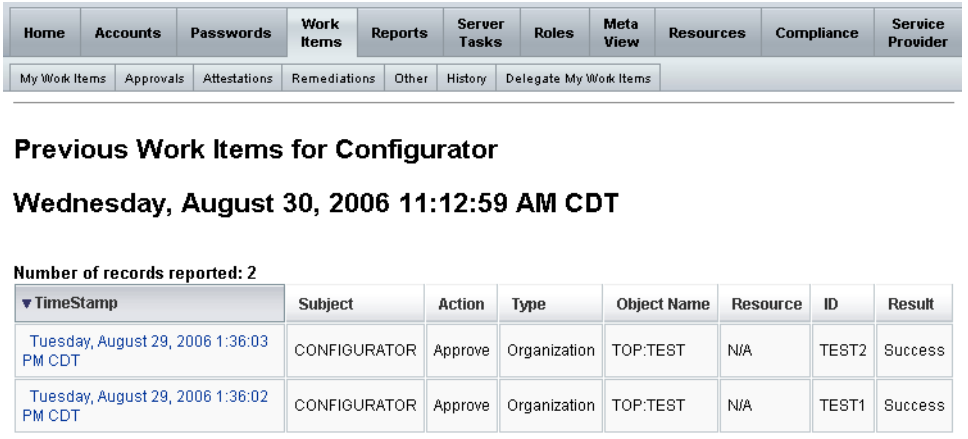
- 第 233 頁的「核准」
- 第 514 頁的「管理驗證責任」
- 第 489 頁的「修正與緩解規範遵循違規」

檢視工作項目歷程記錄

使用 [工作項目] 區域中的 [歷程記錄] 標籤，可檢視先前工作項目動作的結果。

圖 6-7 顯示工作項目歷程記錄的檢視範例。

圖 6-7　　工作項目歷程記錄檢視



委託工作項目

工作項目所有者可透過將工作項目委託給其他使用者達指定的時間長度，來管理工作負荷量。您可以使用主功能表的 **[工作項目] > [委託我的工作項目]** 頁面，將未來的工作項目 (例如核准請求) 委託給一或多位使用者 (受委託人)。使用者無需核准人權能即可擔任受委託人。

備註 委派功能僅適用於未來的工作項目。現有的項目 (即 [我的工作項目] 下列出的項目) 必須透過轉寄功能進行選擇性轉寄。

您也可以從其他頁面委託工作項目：

- 在管理員介面中，可以從 [建立使用者] 和 [編輯使用者] 頁面委託工作項目 (第 67 頁)。請按一下 **[委派]** 表單標籤。
- 在一般使用者 [使用者介面] 中 (第 54 頁)，使用者可以按一下 **[委派]** 功能表項目。

在有效委派期間，受委託人可代表工作項目所有者核准工作項目。受委託的工作項目包括委託名稱。

任何使用者都可以建立他們未來工作項目的一項或多項委派。可以編輯使用者的管理員，也可以代表該使用者建立委派。但是，管理員無法委託至使用者無法委託的對象 (管理員對委派的控制範圍，與所代表進行委派的原先使用者相同)。

稽核記錄項目

核准或拒絕委託的工作項目時，稽核記錄項目會列出委託人名稱。建立或修改使用者時，使用者的委託核准人資訊變更，會記錄在稽核記錄項目的詳細變更區段中。

檢視目前的委派

您可以在 [目前的委派] 頁面上檢視委派。

若要檢視目前的委派，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[工作項目]**。
2. 按一下輔助功能表的 **[委託我的工作項目]**。

   Identity Manager 顯示 [目前的委派] 頁面，您可以於此頁面中檢視與編輯目前有效的委派。

檢視先前的委派

您可以在 [先前的委派] 頁面上檢視先前的委派。

若要檢視先前的委派，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[工作項目]**。
2. 按一下輔助功能表的 **[委託我的工作項目]**。

   [目前的委派] 頁面會隨即開啓。
3. 按一下 **[前一個]**。

   [先前的委派] 頁面會隨即開啓。先前委託的工作項目可用以設定新的委派。

建立委派

您可以使用 [新委派] 頁面建立委派。

若要建立委派，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[工作項目]**。
2. 按一下 **[委託我的工作項目]**。

   [目前的委派] 頁面會隨即開啓。
3. 按一下 **[新增]**。

   [新委派] 頁面會隨即開啓。
4. 如下完成表單：

   a. 從 **[選取工作項目類型以進行委託]** 選項清單中，選取工作項目類型。若要委託所有工作項目，請選取 **[所有工作項目類型]**。

      若您是委託角色類型、組織或資源工作項目，請使用箭頭將選取項目從 **[可用]** 欄移動至 **[已選取]** 欄，以指定應定義此委派的特定角色、組織或資源。

   b. **將工作項目委託給** - 選取下列選項之一：

      - **已選取的使用者** - 選取此選項即可在您的控制範圍內，依名稱搜尋要擔任受委託人的使用者。若選取的任何受委託人也委託了他的工作項目，則您未來的工作項目請求即會委託給他的受委託人。
      - 在 [選取的使用者] 區域中選取一個或多個使用者。您也可以按一下 **[從搜尋中增加]**，以開啓搜尋功能並搜尋使用者。按一下 **[增加]**，將找到的使用者增加至清單中。若要從清單中移除受委託人，請選取該受委託人，然後按一下 **[移除]**。

- **我的管理員** - 選取此選項即可將工作項目委託給您的管理員 (若已指定)
- **DelegateWorkItemRule** - 選取規則即可傳回 Identity Manager 使用者名稱清單以供您委託所選取的工作項目類型。

c. **起始日期** - 選取委派工作項目開始的日期。依預設，所選日期開始於上午 12:01

d. **結束日期** - 選取委派工作項目結束的日期。依預設，所選日期結束於晚上 11:59

備註 工作項目如果只要委託一天，可以選取相同的開始日期和結束日期。

e. 按一下 **[確定]**，以儲存所選項目並返回待核准工作項目的清單。

備註 設定委派之後，任何在有效委派期間建立的工作項目，都會增加至委託清單。若結束委派或委派期限過期，則委託的工作項目就會傳回您的清單中。如此可能會在清單中產生重複的工作項目。但是，當您核准或拒絕其中一項，則重複項目便會自動從清單中移除。

委派給已刪除的使用者

當已刪除之使用者擁有任何擱置的工作項目時，Identity Manager 的運作如下：

- 若已委託擱置的工作項目，且尚未刪除委託人，則擱置的工作項目將會傳回委託人。
- 若尚未委託擱置的工作項目，或已委託擱置的工作項目且刪除了委託人，則在使用者的擱置工作項目獲得解決或轉寄給其他使用者之前，刪除嘗試會失敗。

結束委派

您可以從 [目前的委派] 頁面結束一個或多個委派。

若要結束一個或多個委派，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[工作項目]**。
2. 按一下輔助功能表的 **[委託我的工作項目]**。

   [目前的委派] 頁面會隨即開啓。
3. 選取一個或多個要結束的委派，然後按一下 **[結束]**。

   Identity Manager 會移除所選的委派配置，並將選定類型的所有委託工作項目都傳回至擱置工作項目的清單。

核准

將使用者增加至 Identity Manager 系統時，指定爲新帳號核准人的管理員必須驗證帳號的建立工作。

Identity Manager 支援三種核准種類：

- **組織** - 將使用者帳號增加至組織時所需的核准。
- **角色** - 將使用者帳號指定給角色時所需的核准。
- **資源** - 將存取資源的權限授予使用者帳號時所需的核准。

此外，若啓用了變更核准，而且已變更了角色，則會將變更核准工作項目傳送給指定的角色所有者。

Identity Manager 支援變更核准如下：

- **角色定義** - 若管理員變更角色定義，則需要來自指定的角色所有者之變更核准。角色所有者必須核准工作項目，才可進行變更。

備註 您可以將 Identity Manager 配置爲數字簽署的核准。如需說明，請參閱第 236 頁的 「配置數位簽署的核准與動作」。

備註 不熟悉 Identity Manager 的管理員，有時會混淆**核准**和聽來類似的**驗證**概念。雖然名稱聽起來十分類似，但是核准和驗證是在不同的環境中進行。

核准作業與驗證新使用者帳號相關。將使用者增加至 Identity Manager 時，可能需要一個或多個核准才可驗證新帳號已獲得授權。

而驗證作業則與驗證現有使用者是否只擁有適當資源的適當權限相關。在定期存取檢閱程序中，可能會呼叫 Identity Manager 使用者 (**驗證者**) 以確認其他使用者的帳號詳細資訊 (即使用者的指定資源) 是否有效且正確。此程序稱爲 「驗證作業」。

設定帳號核准人

爲組織、角色和資源核准人設定帳號核准人的動作不是必要作業，但建議進行此作業。對於已設定核准人的每個種類，帳號的建立至少需要進行一次核准。若一個核准人拒絕核准請求，則帳號不會建立。

您可以將多個核准人指定給每個種類。因爲種類中只需要一次核准，您可以設定多個核准人以協助確保工作流程不會延遲或終止。若某個核准人無法使用，則其他核准人可以處理請求。核准僅適用於帳號設定。依預設，帳號更新和刪除並不需要核准。不過，您可以自訂此程序，使其需要核准。

您可以自訂工作流程，方法是使用 Identity Manager IDE 變更核准流程、擷取帳號刪除，以及擷取更新。

如需有關 IDE 的資訊，請參閱第 60 頁的「Identity Manager IDE」。如需有關工作流程的資訊以及變更核准工作流程之圖示範例，請參閱「Identity Manager Workflows, Forms, and Views」。

Identity Manager 核准人既可核准也可拒絕核准請求。

管理員可以從 Identity Manager 介面的 [工作項目] 區域檢視和管理擱置核准。在 [工作項目] 頁面中，按一下 **[我的工作項目]** 以檢視擱置核准。按一下 **[核准]** 標籤以管理核准。

簽署核准

若要核准使用數位簽名的工作項目，必須先如第 236 頁的「配置數位簽署的核准與動作」所述設定數位簽名。

若要簽署核准，請執行以下步驟：

1. 在 Identity Manager 管理員介面中，選取 **[工作項目]**。
2. 按一下 **[核准]** 標籤。
3. 從清單中選取一個或多個核准。
4. 輸入核准的註釋，然後按一下 **[核准]**。

   Identity Manager 提示您並詢問是否信任該 Applet。
5. 按一下 **[始終]**。

   Identity Manager 將顯示一個註有日期的核准摘要。
6. 按 Enter 鍵或按一下 **[瀏覽]** 以找到金鑰庫的位置 (此位置在配置簽署的核准期間設定，如第 238 頁的「使用 PKCS12 之簽署核准的用戶端配置」程序中步驟 10m 所述)。
7. 輸入金鑰庫密碼 (此密碼在配置簽署的核准期間設定，如第 238 頁的「使用 PKCS12 之簽署核准的用戶端配置」程序中步驟 10l 所述)。
8. 按一下 **[簽名]** 以核准請求。

簽署後續核准

簽名核准後，後續的核准動作僅需要您輸入金鑰庫密碼，然後按一下 **[簽名]** (Identity Manager 應該會從上一次核准中記住金鑰庫位置)。

配置數位簽署的核准與動作

使用以下資訊與程序來設定數位簽署。您可以透過數位方式簽署：

- 核准 (包含變更核准)
- 存取檢閱動作
- 修正規範遵循違規事件

本小節討論的主題說明了將憑證和 CRL 增加至 Identity Manager 所需的伺服器端和用戶端簽署核准配置。

簽署的核准之伺服器端配置

若要啓用伺服器端配置，請執行以下步驟：

1. 開啓系統配置物件以進行編輯，並設定 `security.nonrepudiation.signedApprovals=true`

   如需有關編輯系統配置物件的說明，請參閱第 197 頁。

   若是使用 PKCS11，則也必須設定 `security.nonrepudiation.defaultKeystoreType=PKCS11`

   若是使用自訂 PKCS11 金鑰提供者，則也必須設定 `security.nonrepudiation.defaultPKCS11KeyProvider=`<提供者名稱>。

   備註 如需有關何時需要寫入自訂提供者的詳細資訊，請參閱 REF 工具組中的下列項目：

   `com.sun.idm.ui.web.applet.transactionsigner.DefaultPKCS11KeyProvider (Javadoc)`

   `REF/transactionsigner/SamplePKCS11KeyProvider`

   REF (資源擴充工具) 工具組隨附於產品 CD 的 `/REF` 目錄中，或隨附於安裝映像檔。

2. 將您的憑證機構 (CA) 之憑證增加爲可信任的憑證。若要如此，您必須首先取得憑證的副本。

   例如，如果您正在使用 Microsoft CA，請遵循如下類似步驟：

   a. 移至 `http://IPAddress/certsrv`，並以管理權限登入。

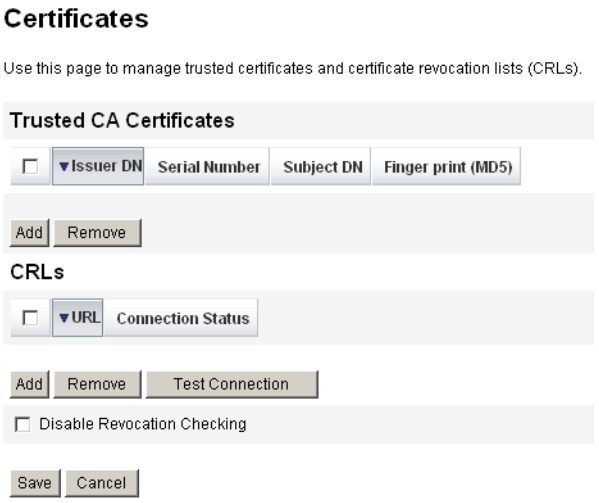
   b. 從清單中選取擷取 CA 憑證或憑證撤銷清單，然後按一下 **[下一頁]**。

   c. 下載並儲存 CA 憑證。

3. 將憑證增加至 Identity Manager 作爲可信任的憑證：

   a. 從管理員介面選取 **[安全性]**，然後選取 **[憑證]**。Identity Manager 會顯示 [憑證] 頁面。

圖 6-8 [憑證] 頁面



   b. 在 [可信任 CA 憑證] 區域中，按一下 **[增加]**。Identity Manager 將顯示 [匯入憑證] 頁面。

   c. 瀏覽至並選取可信任的憑證，然後按一下 **[匯入]**。

      現在憑證即顯示在可信任的憑證清單中。

4. 增加 CA 的憑證撤銷清單 (CRL)：

   a. 在 [憑證] 頁面的 [CRLs] 區域中，按一下 **[增加]**。

   b. 輸入 CA 之 CRL 的 URL。

備註

- 憑證撤銷清單 (CRL) 爲被撤銷或無效的憑證序列號之清單。
- CA 之 CRL 的 URL 可以爲 http 或 LDAP。
- 每個 CA 都有不同的 URL 來發行 CRL；您可以透過瀏覽 CA 憑證之 CRL 發行點的延伸來確定此位址。

5. 按一下 **[測試連線]** 以驗證該 URL。
6. 按一下 **[儲存]**。
7. 使用 jarsigner 簽署 applets/`ts2.jar`。

備註 請參閱 `http://java.sun.com/j2se/1.5.0/docs/tooldocs/windows/jarsigner.html`，以取得更多資訊。Identity Manager 隨附的 `ts2.jar` 檔案使用自我簽署憑證進行簽署，不應用於生產系統。在生產中，此檔案應該使用可信任憑證發出的編碼簽署憑證來重新簽署。

使用 PKCS12 之簽署核准的用戶端配置

下列配置資訊針對使用 PKCS12 的簽署核准。若要啓用用戶端配置，請執行以下步驟：

必要條件

現在至少需要 JRE 1.5。

程序

取得憑證和私密金鑰，然後將他們匯出至 PKCS#12 金鑰庫。

例如，如果您正在使用 Microsoft CA，請遵循如下類似步驟：

1. 使用 Internet Explorer，瀏覽至 `http://IPAddress/certsrv`，然後以管理權限登入。
2. 選取 [請求憑證]，然後按一下 **[下一頁]**。
3. 選取 [進階請求]，然後按一下 **[下一頁]**。
4. 按 **[下一步]**。
5. 選取憑證範本使用者。
6. 選取下列選項：
   a. Mark keys as exportable
   b. Enable strong key protection
   c. Use local machine store
7. 按一下 **[提交]**，然後按一下**[確定]**。
8. 按一下 **[安裝此憑證]]**。

9. 選取 **[執行] -> [mmc]** 以啓動 mmc。
10. 加入憑證快照：
    a. 選取 [主控台] -> [新增/移除嵌入式管理單元]。
    b. 按一下 **[增加...]**。
    c. 選取電腦帳號。
    d. 按 **[下一頁]**，然後按一下 **[完成]**。
    e. 按一下 **[關閉]**。
    f. 按一下 **[確定]**。
    g. 移至 **[憑證] -> [個人] -> [憑證]**。
    h. 在 **[管理員全部作業] 上按一下滑鼠右鍵 -> [匯出]** 。
    i. 按 **[下一步]**。
    j. 按 **[下一頁]** 來確認匯出私密金鑰。
    k. 按 **[下一步]**。
    l. 提供密碼，然後按 **[下一頁]**。
    m. 將 *CertificateLocation* 歸檔。
    n. 按 **[下一頁]**，然後按一下 **[完成]**。按一下 **[確定]** 來確認。

備註 請記下您在用戶端配置的步驟 10l (密碼) 和 10m (憑證位置) 中使用的資訊。您將需要該資訊來簽署核准。

使用 PKCS11 之簽署核准的用戶端配置

若使用 PKCS11 進行簽署核准，請參閱 REF 工具組中的下列資源，以取得配置資訊：

`com.sun.idm.ui.web.applet.transactionsigner.DefaultPKCS11KeyProvider (Javadoc)`

`REF/transactionsigner/SamplePKCS11KeyProvider`

REF (資源擴充工具) 工具組隨附於產品 CD 的 `/REF` 目錄中，或隨附於安裝映像檔。

檢視作業事件簽署

請執行以下步驟，以檢視 Identity Manager 稽核記錄報告中的作業事件簽名：

1. 從 Identity Manager 管理員介面，選取 **[報告]**。
2. 在 [執行報告] 頁面的 **[新增...]** 選項清單中，選取 **[稽核記錄報告]**。
3. 在 **[報告標題]** 欄位中，輸入標題 (例如「核准」)。
4. 在 **[組織]** 選取區域中，選取所有組織。
5. 選取 **[動作]** 選項，然後選取 **[核准]**。
6. 按一下 **[儲存]** 儲存報告，並返回至 [執行報告] 頁面。
7. 按一下 **[執行]** 執行該核准報告。
8. 按一下詳細資訊連結來查看作業事件簽署資訊，其中包括：
   - 核發者
   - 主旨
   - 憑證序列號
   - 簽署的訊息
   - 簽署
   - 簽署演算法

第 7 章

資料載入和同步化

本章提供使用 Identity Manager 資料載入與同步化功能的資訊與程序。您將瞭解如何使用 Identity Manager 資料同步化工具 (探索、調解和同步化) 將資料保持在最新狀態。

- 資料同步化工具：選哪一個好？
- 探索
- 調解
- Active Sync 介面

如需 Identity Manager 之資料載入與同步化運作方式的深入說明，請參閱「Identity Manager Deployment Overview」一書中的「Data Loading and Synchronization」一章。

資料同步化工具：選哪一個好？

Identity Manager 提供數種工具，可用以匯入及同步化帳號資料。如需爲指定作業選取正確工具的協助，請參閱表 7-1。

備註 如需 Identity Manager 之資料載入與同步化運作方式的深入說明，請參閱「Identity Manager Deployment Overview」一書中的「Data Loading and Synchronization」一章。

表 7-1 與資料同步化工具搭配使用的作業

您想要的是：	就請選擇此功能：
開始時將資源帳號拉進 Identity Manager，載入前不檢視	從資源載入
開始時將資源帳號拉進 Identity Manager，可以選擇性地在載入前檢視與編輯資料	擷取至檔案，從檔案載入
定期將資源帳號拉進 Identity Manager，根據配置的策略對每個帳號採取行動	調解資源
將資源帳號變更推或拉入 Identity Manager	使用 Active Sync 介面 (多重資源實作) 進行同步化

探索

Identity Manager 帳號探索功能有助於推進快速部署與加速帳號建立的作業。這些功能的說明如下：

- **擷取至檔案** - 將資源介面傳回的資源帳號擷取至檔案 (CSV 或 XML 格式)。在將資料匯入 Identity Manager 之前，您可以處理這個檔案。
- **從檔案載入** - 讀取檔案 (CSV 或 XML 格式) 中的帳號並將帳號載入 Identity Manager。
- **從資源載入** - 結合使用其他兩個探索功能，可從資源擷取帳號，並將這些帳號直接載入 Identity Manager。

您可以使用這些工具來建立新的 Identity Manager 使用者，或是將資源上的帳號與現有的 Identity Manager 使用者帳號關聯。

備註 本節各頁的重點在於如何使用 Identity Manager 的各項「探索」功能。若要深入瞭解資料載入及同步化，請參閱「Identity Manager Deployment Overview」一書中的「Data Loading and Synchronization」一章。

擷取至檔案

使用此功能將資源帳號從某資源擷取至 XML 或 CSV 文字檔。執行這個動作可以讓您在將資料匯入 Identity Manager 之前，先檢視並變更擷取的資料。

若要擷取帳號，請執行以下步驟：

1. 從功能表列中，選取 **[帳號]**，然後選取 **[擷取至檔案]**。
2. 選取從該處擷取帳號的資源。
3. 選取輸出帳號資訊的檔案格式。您可以擷取資料至 XML 檔案，或以逗號分隔值 (CSV) 格式排列帳號屬性的文字檔案。
4. 按一下 **[下載]**。Identity Manager 將顯示 [檔案下載] 對話方塊，您可在此對話方塊中選擇儲存或檢視擷取的檔案。

如果您選擇開啓檔案，則可能需要選取用於檢視檔案的程式。

從檔案載入

使用此功能將資源帳號 (可以是透過 Identity Manager 從資源擷取的帳號，或是從其他檔案來源擷取的帳號) 載入 Identity Manager。Identity Manager 擷取至檔案功能建立的檔案採用 XML 格式。如果載入的是新使用者的清單，資料檔案一般爲 CSV 格式。

關於 CSV 檔案格式

待載入的帳號通常在試算表中列出，並儲存爲逗號分隔值 (CSV) 格式，以便載入 Identity Manager 中。CSV 檔案內容必須遵循以下格式指導原則：

- **第 1 行** - 列出每個欄位的欄標題或模式屬性 (以逗號分隔)。
- **第 2 行到結尾** - 列出第 1 行所定義之每個屬性的值 (以逗號分隔)。若不存在欄位值的資料，則必須以相鄰逗號來代表該欄位。

  例如，檔案的前三行看起來可能像下圖中的檔案項目：

```
firstname,middleinitial,lastname,accountId,asciipassword,EmployeeID,Departm
ent,Phone
John,Q,Example,E1234,E1234,1234,Operations,555-222-1111
Jane,B,Doe,E1111,E1111,1111,,555-222-4444
```

圖 7-1 用於載入資料之正確格式化的 CSV 檔案範例

```
firstname,middleinitial,lastname,accountId,asciipassword,EmployeeID,Department,Ph
John,Q,Example,E1234,E1234,1234,Operations,555-222-1111
Jane,B,Doe,E1111,E1111,1111,,555-222-4444
```

在本範例中，第二位使用者 (Jane Doe) 不隸屬於任何部門。缺少的值以相鄰逗號 (,,) 表示。

若要載入帳號，請執行以下步驟：

1. 在管理員介面中，按一下功能表的 **[帳號]**，然後再按一下 **[從檔案載入]**。

   Identity Manager 即會顯示 [從檔案載入帳號] 頁面。

2. 在 [從檔案載入帳號] 頁面中指定下列載入選項：

   - **使用者表單** - 當載入作業建立 Identity Manager 使用者時，使用者表單會指定組織以及角色、資源和其他屬性。選取要套用至每個資源帳號的使用者表單。

- **帳號相互關聯規則** - 帳號相互關聯規則會選取可以擁有所有不屬於任何使用者之資源帳號的 Identity Manager 使用者。指定好未擁有之資源帳號的屬性之後，相互關聯規則會傳回一份名稱清單或是一份屬性條件清單，這些清單將用來選取可能的所有者。選取一項規則，用來尋找可能是各無主資源帳號所有者的 Identity Manager 使用者。
- **帳號確認規則** - 帳號確認規則會從相互關聯規則所選取之可能所有者的清單中，排除全部非所有者。指定 Identity Manager 使用者的完整資料以及未擁有之資源帳號的屬性之後，如果使用者擁有該帳號，則確認規則傳回 true，否則傳回 false。選取一個規則來測試資源帳號的各個可能所有者。如果您選取 **[無確認規則]**，則 Identity Manager 會接受所有可能的所有者而不進行確認。

備註 在您的環境中，如果相互關聯規則只會爲各個帳號選取最多一位所有者，則您不需使用確認規則。

- **僅載入相符帳號** - 選取此選項即僅將符合現有 Identity Manager 使用者的帳號載入 Identity Manager 中。如果您選取此選項，載入時會捨棄所有不相符的資源帳號。
- **更新屬性** - 選取此選項即可將目前的 Identity Manager 使用者屬性值，替代成所載入帳號的屬性值。
- **合併屬性** - 輸入一個或多個屬性名稱 (以逗號分隔)，這些屬性的值應進行合併 (會排除重複項目) 而非覆寫。此選項僅能用於清單類型的屬性，如群組和郵件收件人清單。您還必須選取 [更新屬性] 選項。
- **結果層級** - 選取一個臨界值，達到該臨界值時，載入程序便會爲每個帳號單獨記錄一個結果：
  - **僅在出錯時** - 只有在載入帳號時產生了錯誤訊息，才會爲該帳號單獨記錄一個結果。
  - **警告與出錯時** - 如果在載入帳號時產生警告或錯誤訊息，則會爲該帳號單獨記錄一個結果。
  - **參考性與其他** - 爲每個帳號單獨記錄一個結果。這樣會導致載入過程執行得更慢。

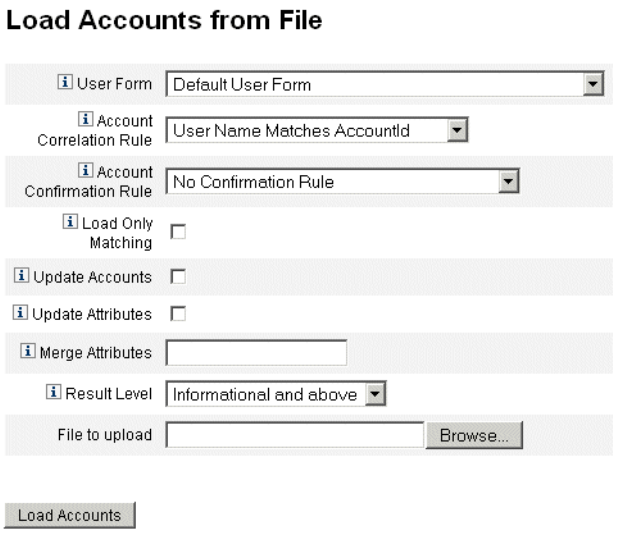
3. 在 [要上傳的檔案] 欄位中，指定要載入的檔案，然後按一下 **[載入帳號]**。

備註

- 如果輸入檔案不包含使用者欄，您必須爲載入作業選取確認規則以便順利執行。
- 與載入程序相關聯的作業實例名稱是以輸入檔案名稱爲基礎；因此，若您重新使用檔案名稱，則與最近一次載入程序相關聯的作業實例將會覆寫所有先前的作業實例。

圖 7-2 說明了 [從檔案載入] 螢幕中的欄位和選項。

圖 7-2 從檔案載入



如果帳號符合現有的使用者 (或與其相關聯)，載入程序會將帳號與使用者合併。該程序還會從沒有關聯的任何輸入帳號建立新的 Identity Manager 使用者 (除非已經指定「需要關聯」)。

`bulkAction.maxParseErrors` 配置變數設定會限制載入檔案時可以找到的錯誤數。預設的限制是 10 個錯誤。如果找到 `maxParseErrors` 錯誤數，則會停止剖析。

從資源載入

使用此功能可根據您指定的載入選項直接擷取帳號，並將其匯入 Identity Manager。

若要匯入帳號，請執行以下步驟：

1. 在管理員介面中，按一下功能表的 **[帳號]**，然後再按一下 **[從資源載入]**。

   [從資源載入帳號] 頁面會隨即開啓。

2. 在 [從資源載入帳號] 頁面中指定載入選項：

   本頁面上的載入選項與 [從檔案載入] 頁面上的選項相同 (第 244 頁)。

調解

使用調解功能定期比較 Identity Manager 中的資源帳號與實際出現在資源上的帳號。調解會使帳號資料產生相互的關聯，並凸顯其差異。

備註 本節各頁的重點在於如何使用管理員介面執行調解作業。若要深入瞭解調解，請參閱「Identity Manager Deployment Overview」一書中的「Data Loading and Synchronization」一章。

調解概念摘要

由於調解專用於進行中的比較，因此其具有以下特性：

- 能夠更明確地診斷出帳號情況，且所支援回應的範圍比探索程序更廣泛
- 能夠進行排程 (探索則不行)
- 能夠提供增量模式 (探索永遠爲完整模式)
- 可偵測原生變更 (探索則不行)

您也可以將調解配置爲在資源處理的下列各點啓動強制工作流程：

- 在調解任何帳號之前
- 在每個帳號中
- 在調解所有帳號之後

從 [資源] 區域存取 Identity Manager 調解功能。[資源] 清單會顯示每個資源上次調解的時間以及其目前的調解狀態。

備註 調解係由 Identity Manager 的調解器元件執行。如需有關調解器配置設定的資訊，請參閱第 187 頁的「調解器設定」。

關於調解策略

調解策略可讓您按照資源爲每一項調解作業建立一組回應。您可在策略中選取要執行調解的伺服器，確定執行調解的頻率以及時間，還可以針對調解時遭遇的各種狀況設定回應。您也可以配置調解，使其偵測出對帳號屬性進行的原生變更 (非透過 Identity Manager 進行的變更)。

編輯調解策略

若要編輯調解策略，請執行以下步驟：

1. 在管理員介面中，按一下功能表的 **[資源]**。
2. 在 **[資源清單]** 中選取資源。
3. 在 **[資源動作]** 清單中選取 **[編輯調解策略]**。

Identity Manager 顯示 [編輯調解策略] 頁面，您可以在其中選取如下策略：

- **調解伺服器** - 在叢集環境中，每部伺服器都可執行調解。指定哪個 Identity Manager 伺服器將會對策略中的資源執行調解。
- **調解模式** - 可在不同模式下執行調解，不同的模式會針對不同的品質進行最佳化處理：
  - **完整式調解** - 可進行完整的調解，但速度會變慢。
  - **漸進式調解** - 對速度進行最佳化處理，但調解不夠完整。

  選取 Identity Manager 應在哪個模式下對策略中的資源執行調解。選取 **[不調解]** 可停用對目標資源的調解。
- **完整式調解排程** - 如果啓用了完整式調解模式，則會按固定的排程自動執行完整式調解。指定應對策略中的資源執行完整式調解的頻率。
  - 選取 **[繼承預設策略]** 選項可繼承更高層級策略的指定排程。
  - 清除 **[繼承預設策略]** 選項可指定排程。使用提供的欄位建立循環排程，或使用 [作業排程重複] 規則建立調解排程的自訂調整。如需有關建立「作業排程重複」規則的資訊，請參閱第 257 頁的 「使用作業排程重複規則」。

- **漸進式調解排程** - 如果啓用了漸進式調解模式，則會按固定的排程自動執行漸進式調解。
  - 選取 **[繼承預設策略]** 選項可繼承更高層級策略的排程。
  - 清除 **[繼承預設策略]** 選項可指定排程。使用提供的欄位建立循環排程，或使用 [作業排程重複] 規則建立調解排程的自訂調整。如需有關建立「作業排程重複」規則的資訊，請參閱第 257 頁的「使用作業排程重複規則」。

備註 並非所有資源都支援漸進式調解。

- **屬性層級調解** - 可以配置調解，使其偵測在本機上對帳號屬性進行的變更 (亦即，不是透過 Identity Manager 進行的變更)。指定調解時是否要偵測對 **[調解後的帳號屬性]** 內所指定的屬性所做的原生變更。
- **帳號相互關聯規則** - 帳號相互關聯規則會選取可以擁有所有不屬於任何使用者之資源帳號的 Identity Manager 使用者。指定好未擁有之資源帳號的屬性之後，相互關聯規則會傳回一份名稱清單或是一份屬性條件清單，這些清單將用來選取可能的所有者。選取一項規則，用來尋找可能是各無主資源帳號所有者的 Identity Manager 使用者。
- **帳號確認規則** - 帳號確認規則會從相互關聯規則所選取之可能所有者的清單中，排除全部非所有者。指定好 Identity Manager 使用者的完整資料以及未擁有之資源帳號的屬性之後，如果使用者擁有該帳號，則確認規則傳回 true，否則傳回 false。選取一個規則來測試資源帳號的各個可能所有者。如果您選取 **[無確認規則]**，則 Identity Manager 會接受所有可能的所有者而不進行確認。

備註 在您的環境中，如果相互關聯規則只會爲各個帳號選取最多一位所有者，則您不需使用確認規則。

- **代理管理員** - 指定在執行調解回應時所要使用的管理員。調解只能執行允許指定代理管理員執行的動作。回應將會使用與此管理員相關的使用者表單 (如有必要)。

  您也可以選取 **[沒有代理管理員]** 選項。選取此選項後，調解結果可供檢視，但不會執行回應動作或工作流程。

- **狀況選項** (與 [回應]) - 調解可識別數種類型的狀況。下文說明各種狀況。在 **[回應]** 欄中指定調解應採取的任何動作。
  - **確認** - 預期的帳號已存在。

    若要標記爲「確認」，以下情況必須爲真：
    - Identity Manager **預期**帳號存在。
    - 資源中有該帳號。

- **刪除** - 預期的帳號不存在。

  若要標記爲「刪除」，以下情況必須爲真：

  - Identity Manager **預期**帳號存在。
  - 資源中**沒有**該帳號。

- **找到** - 調解程序在指定的資源中找到相符帳號。

  若要標記爲「找到」，以下情況必須爲真：

  - Identity Manager 預期帳號可能存在也可能不存在 (若資源已指定給使用者但尚未佈建，則資源中可能有也可能沒有帳號)。
  - 資源中有該帳號。

- **缺少** - 在指定給使用者的資源中找不到相符帳號。

  若要標記爲「缺少」，以下情況必須爲真：

  - Identity Manager 預期帳號可能存在也可能不存在 (若資源已指定給使用者但尚未佈建，則資源中可能有也可能沒有帳號)。
  - 資源中**沒有**該帳號。

- **衝突** - 將資源中的同一帳號指定給兩個或更多的 Identity Manager 使用者。

- **未指定** - 調解程序在未指定給使用者的資源中找到相符帳號。

  若要標記爲「未指定」，以下情況必須爲真：

  - Identity Manager **不預期**帳號存在 (若資源未指定給使用者，則 Identity Manager 不會預期帳號存在)。
  - 資源中有該帳號。

- **不相符** - 資源帳號與所有使用者均不相符。

- **爭議** - 資源帳號與多位使用者相符。

從這些回應選項中選取一個 (可用選項會因狀況不同而有所差異)：

- **根據資源帳號建立新的 Identity Manager 使用者** - 以資源帳號屬性執行使用者表單來建立新的使用者。資源帳號不會隨任何變更而更新。
- **建立 Identity Manager 使用者的資源帳號** - 透過使用者表單重新產生資源帳號屬性，重建缺少的資源帳號。
- **刪除資源帳號與停用資源帳號** - 刪除/停用資源上的帳號。

- **將資源帳號與 Identity Manager 使用者連結與取消資源帳號與 Identity Manager 使用者的連結** - 將資源帳號指定增加至使用者，或移除指定給使用者的資源帳號。這不會執行任何表單的處理。
- **不採取動作** - 若不希望調解執行修復作業，請選取此選項。

  您可手動修復調解所探索到的任何帳號狀況。按一下功能表的 **[資源] > [檢查帳號索引]**。您可在此處瀏覽所有已調解帳號的記錄狀況。在帳號上按一下滑鼠右鍵，即可看到有效修復選項的清單。詳細資訊請參閱第 256 頁的「檢查帳號索引」。

- **調解前工作流程** - 可以配置調解，使其在調解資源前先執行使用者專用的工作流程。指定調解應執行的工作流程。若不應執行任何工作流程，請選取 [不執行工作流程]。
- **視帳號而定的工作流程** - 可以配置調解，使其在回應資源帳號的狀況後，執行使用者專用的工作流程。指定調解應執行的工作流程。若不應執行任何工作流程，請選取 [不執行工作流程]。
- **調解後工作流程** - 可以配置調解，使其在完成資源調解後，執行使用者專用的工作流程。指定調解應執行的工作流程。若不應執行任何工作流程，請選取 **[不執行工作流程]**。
- **說明狀況** - 若啓用此選項，調解會記錄額外的資訊，說明它分類帳號狀況的方式。依照預設，此選項是停用的。若要將說明記錄下來，調解的執行過程將需要花更長的時間。
- **錯誤限制** - 若是啓用，則在處理過程中一旦發生指定的錯誤次數，調解即會自動終止。0 值表示不限制錯誤數。取消選取 [繼承] 預設策略會顯示 [最大] 錯誤允許欄位，並輸入值。
- **從本機移除的最大帳號數** - 此選項是一種防護機制，可計算資源上遺失的帳號數，並會在超過臨界值時，避免調解器取消帳號的連結。

  若要啓用此功能，請清除 **[繼承預設策略]** 核取方塊，並在 **[允許從本機移除的最大帳號數]** 欄位中指定百分比。此臨界值必須設定爲 0 與 100 之間的整數百分比 (0 表示關閉此功能)。

  若移除的帳號百分比超過此臨界值，調解會繼續處理與遺失帳號無關的所有作業，並在完成時產生錯誤。

按一下 **[儲存]** 儲存策略變更。

啟動調解

啓動調解作業時有兩個選項可以使用：

- **調解排程** - 在 [編輯調解策略] 頁面中設定調解排程，可按照固定間隔時間執行調解。

  請參閱第 249 頁的「編輯調解策略」，並依步驟開啓 [編輯調解策略] 頁面。

  調解將會根據您在策略中所設的參數來執行。

- **立即調解** - 若要立即執行調解，請執行以下步驟：

  a. 在管理員介面中，按一下功能表的 **[資源]**。

  b. 在 **[資源清單]** 中選取資源。

  c. 在 **[資源動作]** 清單中，選取以下一項作業：

     - 立即進行完整式調解
     - 立即進行漸進式調解

  調解將會根據您在策略中所設的參數來執行。如果該策略已經爲調解作業設定了定期的排程，調解作業就會繼續按照指定的時間來執行。

取消調解

若要取消調解，請執行以下步驟：

1. 在管理員介面中，按一下功能表的 **[資源]**。
2. 在 **[資源清單]** 中選取要取消調解的資源。
3. 找到 **[資源動作]** 清單，並選取 **[取消調解]**。

檢視調解狀態

有兩種主要方式可檢視調解狀態。若要檢視詳細的調解狀態，請開啓特定資源的 [調解摘要結果] 頁面。[資源清單] 中亦可直接取得有限的調解狀態。

檢視詳細的調解狀態

使用 [調解摘要結果] 頁面可檢視詳細的調解狀態。

若要檢視詳細的調解狀態，請執行以下步驟：

1. 在管理員介面中，按一下功能表的 **[資源]**。
2. 在 **[資源清單]** 中選取要檢視其調解狀態的資源。
3. 找到 **[資源動作]** 清單，並選取 **[檢視調解狀態]**。

   該資源的 [調解摘要結果] 頁面會隨即開啓。

檢視資源清單中的調解狀態

檢視 [資源清單] 亦可取得調解狀態 (若要顯示 [資源清單]，請開啓管理員介面並按一下功能表的 **[資源]**)。

[狀態] 欄會報告下列調解狀態的情況：

- **不明** - 狀態不明。最近一次調解作業的結果無法使用。
- **停用** - 已停用調解功能。
- **失敗** - 最近一次的調解無法完成。
- **成功** - 最近一次的調解順利完成。
- **完成時有錯誤發生** - 最近一次的調解已完成，但同時有錯誤發生。

備註 您必須重新整理本頁面才可檢視狀態的變更 (資訊不會自動重新整理)。

使用帳號索引

帳號索引會記錄 Identity Manager 已知之各資源帳號的上一已知狀態。帳號索引主要是由調解來維護，但其他 Identity Manager 功能也會視需要對其進行更新。

探索工具不會更新帳號索引。

搜尋帳號索引

搜尋帳號索引可檢視指定之資源帳號的最新已知狀態。

若要搜尋帳號索引，請執行以下步驟：

1. 在管理員介面中，按一下功能表的 **[資源]**。
2. 在 **[資源清單]** 中選取要搜尋其帳號索引的資源。
3. 找到 **[資源動作]** 清單，並選取 **[搜尋帳號索引]**。

   [搜尋帳號索引] 頁面會隨即開啓。
4. 選取搜尋類型，然後輸入或選取搜尋屬性。
   - **資源帳號名稱** - 選取此選項，再選取其中一個修飾鍵 ([開頭爲]、[包含] 或 [是])，然後輸入部分或完整的帳號名稱。
   - **資源爲下列一項** - 選取此選項，然後從清單中選取一個或多個資源，以便在指定資源中尋找已調解帳號。
   - **所有者** - 選取此選項，再選取其中一個修飾鍵 ([開頭爲]、[包含] 或 [是])，然後輸入部分或完整的所有者名稱。若要搜尋無主帳號，請搜尋處於「不相符」(UNMATCHED) 或「爭議」(DISPUTED) 狀況的帳號。
   - **狀況爲下列一項** - 選取此選項，然後從清單中選取一個或多個狀況，以在指定的狀況中尋找已調解的帳號。
5. 按一下 **[搜尋]** 來根據您的搜尋參數來搜尋帳號。若要限制搜尋結果，您可以選擇性地在 **[只返回]** 欄位中指定數目。預設限制爲前 1000 個找到的帳號。

   按一下 **[重設查詢]** 以清除頁面並選取新選項。

檢查帳號索引

還可以檢視所有 Identity Manager 使用者帳號，並可選擇爲每位使用者分別調解帳號。

若要檢查帳號索引，請執行以下步驟：

1. 在管理員介面中，按一下功能表的 **[資源]**。
2. 按一下輔助功能表的 **[檢查帳號索引]**。

   [檢查帳號索引] 頁面會隨即開啓。

本表顯示 Identity Manager 已知的所有資源帳號 (不論其是否爲 Identity Manager 使用者所擁有)。此資訊按資源或 Identity Manager 組織分組。若要變更此檢視，請從 **[變更索引檢視]** 清單中選取一個檢視。

使用帳號

若要使用資源中的帳號，請選取 **[按資源分組]** 索引檢視。Identity Manager 會顯示每種類型資源的資料夾。可以展開資料夾以導覽到特定資源。按一下資源旁的 **+** 或 **-** ，可顯示 Identity Manager 已知的所有資源帳號。

上次在該資源上調解之後直接新增至資源中的帳號將不會顯示。

您也許能夠執行幾種動作，但要視給定帳號目前的狀況而定。在帳號上按一下滑鼠右鍵，即可看到有效修復選項的清單。您也可以檢視帳號的詳細資訊或選擇調解某個帳號。

運用使用者

若要使用 Identity Manager 使用者，請選取 **[按使用者分組]** 索引檢視。在此檢視中，Identity Manager 使用者和組織會以與 [帳號清單] 頁面類似的階層顯示。若要察看目前指定給 Identity Manager 中的使用者的帳號，請瀏覽至該使用者，然後按一下使用者名稱旁邊的指示器。Identity Manager 已知的使用者帳號及這些帳號的目前狀態，會顯示在使用者名稱之下。

您也許能夠執行幾種動作，但要視給定帳號目前的狀況而定。您也可以檢視帳號的詳細資訊或選擇調解某個帳號。

使用作業排程重複規則

使用「作業排程重複規則」可以調整調解排程。例如，若要將排程於週六執行的調解推遲至下週一執行，請使用「作業排程重複規則」。

「作業排程重複規則」可用以調整完整及增量調解的排程。

如需有關如何選取「作業排程重複」規則的資訊，請參閱第 249 頁的「編輯調解策略」。

調解執行次數的排程方式

調解工作一旦完成，調解器元件即會檢查下次排定的執行時間。

首先，調解器會查看預設的排程，取得下次的執行時間。接著，調解器會執行所有適用的「作業排程重複規則」，瞭解是否需要調整排程。若需調整排程，規則的排程即會置換該調解的預設排程。

備註 「作業排程重複規則」無法置換預設排程。它們僅能逐一**置換**已排定工作的開始時間。

「接受全部日期」規則範例

本節說明名爲「接受全部日期」的內建規則範例。

若要檢視「接受全部日期」規則範例，請執行以下步驟：

1. 在文字編輯器中開啓 `ReconRules.xml`，其位於 Identity Manager 的 `sample` 目錄中。
2. 搜尋名爲 `SCHEDULING_RULE_ACCEPT_ALL_DATES` 的規則。

規則的 `subtype` 屬性必須設爲 `SUBTYPE_TASKSCHEDULE_REPETITION_RULE`，([編輯調解策略] 頁面的) [作業排程重複規則] 下拉式功能表才會列出該規則：

```
<Rule subtype='SUBTYPE_TASKSCHEDULE_REPETITION_RULE'
name='SCHEDULING_RULE_ACCEPT_ALL_DATES'>
```

如前文所述，「作業排程重複規則」可修改預設的調解排程。

變數 calculatedNextDate 可接受下個日期 (依預設方式計算) 或傳回其他日期。正如範例規則所列，calculatedNextDate 會無條件接受預設日期：

編碼樣例 7-1 SCHEDULING_RULE_ACCEPT_ALL_DATES 規則邏輯 (摘錄)

```
<RuleArgument name='calculatedNextDate'/>
<block>
  <ref>calculatedNextDate</ref>
</block>
```

若要建立自訂的排程，請置換 <block> 元素之間的規則邏輯。例如，若要將調解的開始時間變更至每週六上午 10:00，請將下列 JavaScript 加入 <block> 元素之間：

編碼樣例 7-2 作業排程重複規則邏輯範例

```
<block>
  <script>
     var calculatedNextDate = env.get('calculatedNextDate');

  // 請測試以查看此項作業是否排程於週六執行
  // (請注意，6 在 JavaScript 中表示週六)
  if(calculatedNextDate.getDay() == 6) {
   // 若是，請將時間設爲 10:00:00
       calculatedNextDate.setHours(10);
       calculatedNextDate.setMinutes(0);
       calculatedNextDate.setSeconds(0);
  }
  // 傳回修改的日期
    calculatedNextDate;
  </script>
</block>
```

在 編碼樣例 7-2 中，calculatedNextDate 最初設爲預設的排定時間。若下次排定的執行日期爲週六，則規則會排程調解於 10:00 開始。若下次排定的執行日期**不是**週六，編碼樣例 7-2 會傳回 calculatedNextDate 但不會調整任何時間，並使用預設的排程。

如需有關建立自訂規則以用於 Identity Manager 的更多資訊，請參閱「Identity Manager Deployment Tools」一書中的「Working with Rules」一章。

Active Sync 介面

Identity Manager Active Sync 功能可使儲存在授權外部資源 (如應用程式或資料庫) 中的資訊與 Identity Manager 使用者資料同步化。爲 Identity Manager 資源配置同步化可讓它偵聽或輪詢對授權資源所做的變更。

在 (適當目標物件類型的) 資源同步化策略中指定 [輸入表單]，可配置將資源屬性變更匯入 Identity Manager 的方法。

備註 本章各頁的重點在於如何使用管理員介面執行 Active Sync 作業。若要深入瞭解 Active Sync，請參閱「Identity Manager Deployment Overview」一書中的「Data Loading and Synchronization」一章。

配置同步化

Identity Manager 使用同步化策略啓用資源的同步化。

編輯同步化策略

每項資源都有其專屬的同步化策略。

若要編輯或配置同步化，請執行以下步驟：

1. 在管理員介面中，按一下功能表的 **[資源]**。
2. 在 **[資源清單]** 中選取要配置同步化的資源。
3. 找到 **[資源動作]** 清單，並選取 **[編輯同步化策略]**。

   該資源的 [編輯同步化策略] 頁面會隨即開啓。

在 [編輯同步化策略] 頁面中指定以下選項，以配置同步化：

- **目標物件類型** - 選取要套用策略的使用者類型，亦即 Identity Manager 使用者或服務提供者使用者。

  備註 在服務提供者實作中，必須將同步化策略 (物件類型已指定服務提供者使用者) 配置爲啓用此類使用者的資料同步化。如需有關服務提供者使用者的更多資訊，請參閱第 17 章「服務提供者管理」。

- **排程設定** - 使用此區段可指定啓動方法和輪詢排程。

  [啓動類型] 可以爲 [手動]、[自動]、[以容錯移轉方式自動啓動] 或 [停用]：

  - **自動或以容錯移轉方式自動啓動** - 在 Identity 系統啓動時即啓動授權來源
  - **手動** - 需要管理員啓動授權來源。
  - **停用** - 停用資源。

  使用 **[開始日期]** 和 **[啓動時間]** 選項來指定何時開始輪詢。透過選取間隔並輸入間隔值 (秒、分鐘、小時、天、週、月) 可指定輪詢週期。

  如果設定了在未來發生的輪詢起始日期與時間，則輪詢會在指定時間開始。如果設定了在過去發生的輪詢起始日期與時間，則 Identity Manager 會根據此資訊及輪詢間隔決定何時開始輪詢。例如：

  - 您將資源的即時同步配置在 2005 年 7 月 18 日 (星期二)
  - 您設定資源爲每週輪詢，輪詢開始日期爲 2005 年 7 月 4 日 (星期一)，開始時間爲上午 9:00。

  在此情況下，資源將在 2005 年 7 月 25 日 (下一個星期一) 開始輪詢。

  如果您未指定開始日期或時間，資源將立即開始輪詢。如果您採用此方法，則每次重新啓動應用程式伺服器時，所有爲使用中的同步化配置的資源均將立即開始輪詢。此典型方法用於設定起始日期和時間。

- **同步化伺服器** - 在叢集環境中，每個伺服器都可以執行同步化。選取一個選項以指定將用於執行資源同步化的伺服器。
  - 如果在任何伺服器上執行同步化皆可，則選取 **[使用任何可用伺服器]**。啓動同步化時，將從一組可用的伺服器中選擇一個伺服器。
  - 選取 **[使用 waveset.properties 中的設定]**，以使用該特性中所指定的伺服器執行同步化 (此功能已經停用)。
  - 選取 **[使用指定伺服器]**，再從 [同步化伺服器] 清單中選取一個或多個可用的伺服器，以選取特定伺服器執行同步化。
- **資源專用設定** - 使用此區段可指定同步化以何種方式確定要爲資源處理的資料。
- **共用設定** - 爲資料同步化作業指定以下一般設定：
  - **代理管理員** - 選取將處理更新的管理員。所有動作都將透過指定給此管理員的權能來授權。您應該利用空的使用者表單選取代理管理員。
  - **輸入表單** - 選取將處理資料更新的輸入表單。這個選擇性的配置項目允許在儲存帳號屬性前先轉換屬性。

- **規則 -** 您可以指定資料同步化程序期間要使用的規則：
  - **處理規則** - 選取此規則可指定要針對每個內送帳號執行的處理規則。選取此選項會置換其他所有選項。如果指定處理規則，則每一列都會執行此處理，不論此資源上的其他設定爲何。可以是程序名稱，也可以是評估程序名稱的規則。
  - **相互關聯規則** - 選取相互關聯規則，以置換資源調解策略中所指定的相互關聯規則。相互關聯規則會使資源帳號與 Identity 系統帳號相互關聯。
  - **確認規則** - 選取確認規則，以置換資源調解策略中所指定的確認規則。
  - **解決處理規則** - 選取此規則以指定當資料輸入的記錄有多個相符項時，所要執行的作業定義之名稱。此程序會提示管理員進行手動操作。可以是程序名稱，也可以是評估程序名稱的規則。
  - **刪除規則** - 選取規則，在針對每個內送使用者更新對該規則進行計算之後，該規則會傳回 true 或 false，以確定是否要執行刪除作業。

- **建立不相符的帳號** - 啓用此選項 (true) 後，介面將嘗試建立在 Identity Manager 系統中找不到的帳號。如果未啓用，介面將透過 [解決處理規則] 傳回的程序來執行帳號。
- **記錄設定** - 指定以下記錄選項的值：
  - **最多記錄封存數量** - 如果此值大於零，將保留最近的 N 個記錄檔。如果此值爲零，則會重複使用單個記錄檔案。如果此值爲 -1，則永不捨棄任何記錄檔案。
  - **最長記錄有效期間** - 超過此段期間之後，將歸檔現用的記錄。如果時間爲 0，則不會執行有時限的歸檔。如果 [最多記錄封存數量] 爲 0，則會在超過此時段後將現用記錄截斷，然後重複使用該記錄。此有效期間標準的計算與 [最大記錄檔案大小] 中所指定的標準無關。

    輸入一個數字，然後選取時間單位 (天、小時、分鐘、月、秒或週)。預設單位是日。
  - **記錄檔案路徑** - 輸入目錄路徑，將在該目錄中建立現用記錄檔案與封存記錄檔案。記錄檔案名稱的開頭將會是資源名稱。
  - **最大記錄檔案大小** - 以位元組爲單位，輸入現用記錄檔案大小的最大值。當現用記錄檔案達到所允許的最大限制時，就會被封存起來。如果 [最多記錄封存數量] 爲 0，則會在超過此時段後將現用記錄截斷，然後重複使用該記錄。此大小標準的計算與 [最長記錄有效期間] 中所指定的有效期間標準無關。

- **記錄層級** - 輸入記錄的層級：
  - 0 - 不記錄
  - 1 - 錯誤
  - 2 - 資訊
  - 3 - 詳細
  - 4 - 除錯

按一下 **[儲存]** 儲存資源的策略設定。

編輯 Active Sync 介面

編輯 Active Sync 介面之前，請停止同步化。

若要停止同步化，請執行以下步驟：

1. 開啓 [編輯同步化] 頁面 (如需說明，請參閱第 259 頁的「編輯同步化策略」)。
2. 找到 **[排程設定]** 下的 **[啓動類型]**，然後選取 **[停用]**。

   請針對服務提供者使用者取消選取 **[啓用同步化]** 選項。

   將出現一則警告訊息，指出已停用使用中的同步化。
3. 按一下 **[儲存]**。

   停用資源的同步化將導致儲存變更時停止同步化作業。

調校 Active Sync 介面效能

由於同步化是背景作業，所以 Active Sync 介面配置可能會影響伺服器效能。調校 Active Sync 介面效能必須進行下列作業：

- 變更輪詢間隔
- 指定將執行介面的主機
- 啓動與停止
- 介面記錄

透過資源清單管理 Active Sync 介面。選取 Active Sync 介面，然後從 [資源動作] 清單的 [同步化] 區段中存取啓動、停止與狀態重新整理控制動作。

變更輪詢間隔

輪詢間隔決定 Active Sync 介面開始處理新資訊的時間。應該根據正在執行的作業的類型來決定輪詢間隔。例如，如果介面會從資料庫讀取一長串使用者，且每次都會更新 Identity Manager 中的所有使用者，請考慮在每天早上幾小時內執行此程序。有些介面可以快速搜尋要處理的新項目，並可將它們設定爲每分鐘執行。

指定將執行介面的主機

若要指定將執行介面的主機，請編輯 `waveset.properties` 檔案。將 `sources.hosts` 特性編輯爲以下任一選項：

- 設定 `sources.hosts=`*hostname1,hostname2,hostname3*。這會列出要執行 Active Sync 介面之機器的主機名稱。介面將會在此欄位中列出的第一台可用主機上執行。

  備註 您輸入的 *hostname* 必須與 Identity Manager 伺服器清單中的某項目相符。從 [配置] 標籤檢視伺服器清單。

  或

- 設定 `sources.hosts=localhost`。透過此設定，介面將在第一台嘗試爲資源啓動 Active Sync 的 Identity Manager 伺服器上執行。

備註 在叢集環境中，如果您需要指定特定伺服器，便應使用第一個選項。

此特性設定僅適用於 Identity Manager 使用者同步化。服務提供者使用者同步化的主機配置將由同步化策略決定。

可以將需要更多記憶體與 CPU 週期的 Active Sync 介面配置爲在專屬伺服器上執行，這樣有助於系統的負載平衡。

啟動與停止

您可以停用、手動啓動或自動啓動 Active Sync 介面。若要啓動或停止 Active Sync 介面，您必須有適當的管理員權能來變更 Active Sync 資源。如需有關管理員權能的資訊，請參閱第 215 頁的 「權能類別」。

如果將介面設定爲自動，當應用程式伺服器重新啓動時，介面也會重新啓動。當您啓動介面時，它會立刻執行並在指定的輪詢間隔來臨時執行。如果您停止介面，下次介面在檢查到停止旗標時便會停止。

介面記錄

介面記錄擷取有關介面目前處理情況的資訊。記錄擷取資訊的詳細程度需視您設定的記錄的記錄層級而定。介面記錄在除錯問題與監視介面程序進度時非常有用。

每個介面各有其記錄檔案、路徑和記錄層級。您可以在 [同步化策略] 的 [記錄] 區段爲適當的使用者類型 (Identity Manager 或服務提供者) 指定這些值。

刪除介面記錄

僅當停止介面後，才能刪除介面記錄。多數情況下，請在刪除記錄前製作記錄副本作爲歸檔之用。

第 8 章

報告

Identity Manager 報告自動和手動系統作業。強大的報告功能組可讓您隨時擷取和檢視有關 Identity Manager 使用者的重要存取資訊和統計。

在本章中，您將瞭解 Identity Manager 報告類型、如何建立、執行和透過電子郵件傳送報告，以及如何下載報告資訊。

本章分爲以下小節：

使用報告

在 Identity Manager 中，將報告視爲一類特殊的作業。因此，可以在 Identity Manager 管理員介面的兩個區域中使用報告：

- **報告 (執行報告)** - 使用 [執行報告] 區域以定義、執行、刪除和下載報告。只有具有足夠權能的管理員，才可以定義、執行、刪除和下載報告。詳細資訊請參閱第 619頁的附錄 D「權能定義」。
- **伺服器作業** - 定義報告後，就可以移至 [已排程的作業] 區域 **([伺服器作業] > [管理排程])** 以排程和修改報告作業。TaskDefinition 物件必須包含 `visibility=schedule`，才能進行排程。請使用除錯頁面進行此變更。詳細資訊請參閱第 197 頁的「編輯 Identity Manager 配置物件」。

報告類型

報告分爲兩個種類：

- Identity Manager 報告 - 包含多種報告類型，包括即時、摘要、稽核記錄、系統記錄檔與使用情況報告。
- 稽核員報告 - 提供可協助您依據稽核策略中定義的條件，管理使用者規範遵循的資訊。

在這兩個種類裡，報告會進一步分成多種報告類型。報告類型在本章稍後會有更詳盡的討論。Identity Manager 報告從第 273 頁開始有相關討論，稽核員報告的相關討論則位於第 284 頁上。

如需有關如何檢視 Identity Manager 報告與稽核員報告的說明，請參閱第 268 頁的「檢視報告」。

執行報告

若要執行報告，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[報告]**。

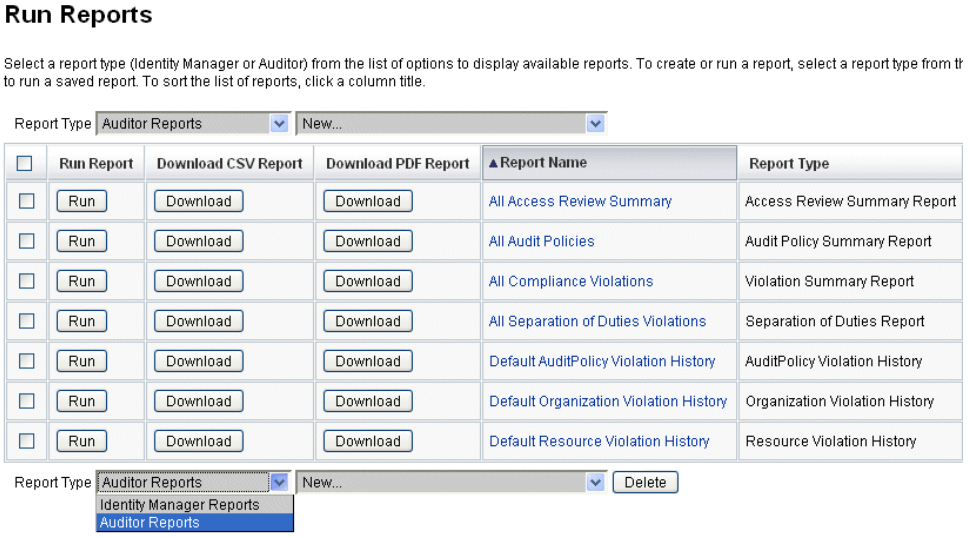
   [執行報告] 頁面會隨即開啓。

2. 若要檢視可用 Identity Manager 報告的清單，請在 **[報告類型]** 下拉式功能表中選取 **[Identity Manager 報告]** (預設會選取這個選項)。

   若要檢視可用稽核員報告的清單，請在 **[報告類型]** 下拉式功能表中選取 **[稽核員報告]**。詳細資訊請參閱第 485 頁的「使用 Auditor 報告」。

   圖 8-1 爲 [執行報告] 頁面的範例。[稽核員報告] 可從 **[報告類型]** 下拉式功能表中選取。

圖 8-1　　執行報告選取



3. 按一下 **[執行]** 以執行報告。

備註 若要讓同一份報告的多個實例同時執行，請編輯報告，並選取 **[是否允許報告同步執行]** 選項。啓用此選項可讓多名管理員同時執行同一份報告。

若同時執行同一份報告的兩個或更多實例，每份報告的報告名稱後會依序附加管理員 ID 與時間戳記。

檢視報告

從 [執行報告] 頁面執行報告後，您可以立即檢視輸出，或於稍後檢視。

若要檢視報告，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[報告]**。

   [執行報告] 頁面會隨即開啓。

2. 按一下 **[檢視報告]** 標籤。

   [檢視報告] 頁面會隨即開啓。

3. 按一下報告加以檢視。

建立報告

若要修改現有報告，並以新名稱加以儲存，請參閱下節中的「編輯及複製報告」。

若不以現有報告爲基礎，而建立新的 Identity Manager 報告或稽核員報告，請使用以下步驟：

1. 在管理員介面中，按一下主功能表的 **[報告]**。

   [執行報告] 頁面會隨即開啓。

2. 使用 **[報告類型]** 下拉式功能表選取報告種類。有兩種報告種類可供選擇：

   - **Identity Manager 報告**
   - **稽核員報告**

3. 使用下一個下拉式功能表，選取要建立的特定報告類型 (此功能表頂端顯示 **[新增...]**)。

Identity Manager 會顯示 [定義報告] 頁面，您可在其中選擇建立報告時要用的選項，並加以執行或儲存。

輸入並選取報告條件之後，您可以：

- 執行報告但不儲存 - 按一下 **[執行]** 以執行報告。Identity Manager 不儲存報告 (如果您定義了新的報告) 或變更的報告條件 (如果您編輯了現有的報告)。
- 儲存報告 - 按一下 **[儲存]** 以儲存報告。一旦儲存後，您就可以從 [執行報告] 頁面 (報告清單) 來執行此報告

如需有關執行報告的更多資訊，請參閱第 267 頁的「執行報告」。

編輯及複製報告

若要複製報告、修改現有報告並以新名稱儲存報告，

若要編輯或複製報告，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[報告]**。

   [執行報告] 頁面會隨即開啓。

2. 使用 **[報告類型]** 下拉式功能表選取報告種類。有兩種報告種類可供選擇：

   - **Identity Manager 報告**
   - **稽核員報告**

   報告的表格會顯示選定種類中的現有報告。

3. 按一下報告名稱加以編輯。

4. 若要編輯報告，請視需要調整報告參數，然後按一下 **[儲存]**。

   若要複製報告，請輸入新的報告名稱、視需要調整報告參數，然後按一下 **[儲存]** 以新名稱儲存此報告。

通過電子郵件傳送報告

建立或編輯報告時，您可選取某一選項，將報告結果傳送給一或多位電子郵件收件者。當您選取此選項時，頁面會重新整理並提示您輸入電子郵件收件者。輸入一或多位收件者，以逗號分隔郵件地址。

您也可選擇要附加到電子郵件中的報告格式：

- **附加 CSV 格式** – 附加使用逗號分隔值 (CSV) 格式的報告。
- **附加 PDF 格式** – 附加使用可攜式文件格式 (PDF) 的報告。

排定報告

您可以根據自己的意願，即是要立即執行報告或是將其排定爲以固定間隔執行，而做出不同的選擇：

- **[報告] > [執行報告]** - 可讓您立即執行所儲存的報告。在報告清單中，按一下 **[執行]**。Identity Manager 會執行報告，然後以摘要和明細形式顯示結果。
- **[伺服器作業] > [管理排程]** - 排程要執行的報告作業。選取報告作業後，您便可設定報告頻率及選項。您還可以調整特定的報告詳細資訊 (像在 [定義報告] 頁面的 [報告] 區域中那樣)。

  若要讓報告 TaskDefinition 顯示於此清單中，TaskDefinition 物件中的 `visibility` 屬性必須設爲 `schedule`。

下載報告資料

在 [執行報告] 頁面中，您可以下載用於其他應用程式 (如 Acrobat Reader 或 StarOffice) 的報告資訊。

開啓 [執行報告] 頁面，然後在下列其中一欄中按一下 **[下載]**：

- **下載 CSV 報告** -下載 CSV 格式的報告輸出。儲存之後，您可以使用其他應用程式 (例如 StarOffice) 開啓並使用報告。
- **下載 PDF 報告** -下載可攜式文件格式的報告輸出，這種格式可使用 Adobe Reader 檢視。

圖 8-2 下載報告

配置報告輸出

若要配置報告輸出，請按一下 **[報告]**，然後選取 **[配置報告]**。

[配置報告] 頁面上有下列可用選項：

- **PDF 報告選項**

  對於以可移植文件格式 (PDF) 產生的報告，您可以進行選取以決定要在報告中使用的字型。

  - **PDF 字型名稱** - 選取在產生 PDF 報告時要使用的字型。依預設，僅顯示可用於所有 PDF 檢視器的字型。然而，透過將字型定義檔案複製到產品的字型/目錄中並重新啓動伺服器，將其他字型 (例如支援亞洲語言所需的字型) 增加到系統。

    接受的字型定義格式包括 .ttf、.ttc、.otf 和 .afm。如果選取其中一種字型，則檢視報告的電腦系統上必須可以使用這種字型。或者選取 [PDF 文件中的內嵌式字型] 選項。

  - **PDF 文件中的內嵌式字型** - 選取此選項即可在所產生的 PDF 報告中使用內嵌的字型定義。如此即可在任意的 PDF 檢視器中檢視報告。

  備註 嵌入字型可能會使文件大小增大極多。

- **CSV 報告選項**

  - **字元集名稱** - 選取產生 CSV 報告時要使用的字元集。並非所有匯入 CSV 檔案的應用程式皆支援預設 UTF-8 編碼。視需要選取其他字元集。

- **追蹤的事件配置**

  - **啓用事件收集** - 此選項可用以配置系統監視的報告，但不適用於報告格式的自訂。如需更多資訊，請參閱第 296 頁的 「追蹤的事件配置」。

按一下 **[儲存]** 以儲存報告配置選項。

Identity Manager 報告

Identity Manager 報告類型可分成六種報告類型種類：

- 稽核記錄
- 個別使用者稽核記錄
- 即時
- 摘要
- 系統記錄檔
- 用法
- 工作流程

稽核記錄報告

稽核記錄報告會以系統稽核記錄中擷取的事件爲基礎。這些報告提供多項資訊，其中包括產生的帳號、核准的請求、失敗的存取嘗試、密碼變更與重設、自我佈建的作業、策略違規及服務提供者 (企業外部網路) 使用者等。

備註 在執行稽核記錄之前，您必須指定希望擷取的 Identity Manager 事件類型。若要執行此作業，請從功能表列中選取 **[配置]**，然後選取 **[稽核]**。選取一個或多個稽核群組名稱來記錄每個群組的成功與失敗事件。如需有關設定稽核配置群組的更多資訊，請參閱第 185 頁的「配置稽核群組和稽核事件」。

若要定義稽核記錄報告，請執行以下步驟：

1. 依照第 269 頁上用以建立報告的指示作業。

   從第一個 **[報告類型]** 功能表中選取 **[Identity Manager 報告]**，再從第二個功能表中選取 **[稽核記錄報告]**。

   [定義報告] 頁面會隨即開啓。

2. 填寫表單並按一下 **[儲存]**。

   對表單若有任何問題，請按一下 **[說明]**。

設定與儲存報告參數後，請立即從 [執行報告] 頁面執行報告。按一下 **[執行]** 可產生一個包含與已儲存條件相符之所有結果的報告。報告中包含事件發生日期、執行的動作及動作的結果。

個別使用者稽核記錄報告

「個別使用者稽核記錄報告」與「稽核記錄報告」相同，也是以擷取自系統稽核記錄的事件爲基礎。但此報告會提示您指定所要報告的使用者，並傳回對此使用者執行的作業清單。爲傳回最完整的結果，此報告會在稽核記錄的 [帳號 Id] 與 [ObjectDesc] 欄位中搜尋相符的使用者名稱。

您可以讓此報告傳回一組固定的欄，或選取一組自訂的欄。這些欄定義於 reporttasks.xml 與 defaultreports.xml 中。這兩個檔案皆位於 sample 目錄中 (位於您的 Identity Manager 安裝目錄中)。

若要定義個別使用者稽核記錄報告，請執行以下步驟：

1. 依照第 269 頁上用以建立報告的指示作業。

   從第一個 **[報告類型]** 功能表中選取 **[Identity Manager 報告]**，再從第二個功能表中選取 **[個別使用者稽核記錄報告]**。

   [定義報告] 頁面會隨即開啓。

2. 填寫表單並按一下 **[儲存]**。

   對表單若有任何問題，請按一下 **[說明]**。

即時報告

即時報告會直接輪詢資源以報告即時資訊。即時報告包括：

- **資源群組報告** - 摘要群組屬性，包括使用者成員身份。
- **資源狀態報告** - 透過對每個資源執行 testConnection 方法，測試一個或多個指定資源的連線狀態。
- **資源使用者報告** - 列出使用者資源的帳號和帳號屬性。

若要定義即時報告，請執行以下步驟：

1. 依照第 269 頁上用以建立報告的指示作業。

   從第一個 **[報告類型]** 功能表中選取 **[Identity Manager 報告]**，再從第二個功能表中選取 **[資源群組報告]**、**[資源狀態報告]** 或 **[資源使用者報告]**。

   [定義報告] 頁面會隨即開啓。

2. 填寫表單並按一下 **[儲存]**。

   對表單若有任何問題，請按一下 **[說明]**。

您設定與儲存報告參數後，請即從 [執行報告] 清單頁面中執行報告。按一下 **[執行]** 可產生一個包含與已儲存條件相符之所有結果的報告。

摘要報告

摘要報告類型包括 **[Identity Manager 報告]** 清單中的以下報告：

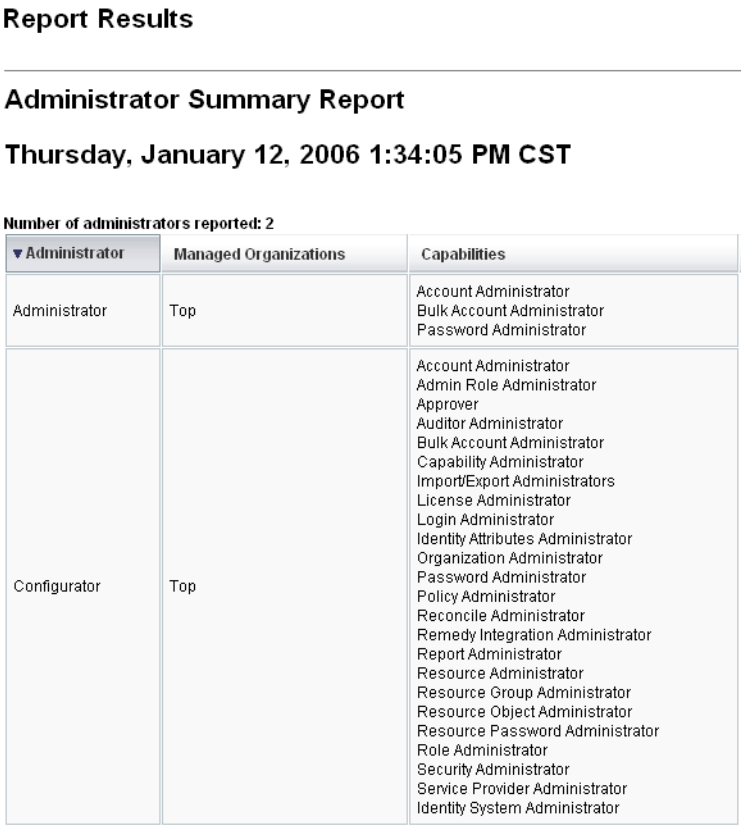
- **帳號索引報告** - 根據調解狀況來報告選取的資源帳號。
- **管理員報告** - 檢視 Identity Manager 管理員、管理員所管理的組織以及已指定的權能。定義管理員報告時，您可以依組織選取要包括的管理員。
- **管理員角色報告** - 列出已指定給管理員角色的使用者。
- **角色報告** - 報告角色與相關資源的各個層面。
- **作業報告** - 報告擱置的作業和已完成的作業。您可以透過從屬性清單中選取來決定要包括的資訊深度，例如核准者、說明、過期日期、所有者、起始日期與狀態。
- **使用者報告** - 檢視使用者、已指定給這些使用者哪些角色，以及他們可存取哪些資源。定義使用者報告時，您可以依名稱、指定的管理員、角色、組織或資源指定選取要包含的使用者。
- **使用者問題報告** - 可讓管理員尋找未回答最低數目的認證問題之使用者，此數目由使用者的帳號策略要求所指定。結果會指出使用者名稱、帳號策略、與策略相關的介面，以及最少需要回答的問題數目。

備註 依預設，以下報告在已登入管理員所控制的組織集上執行，除非選取了一個或多個組織 (針對其執行報告) 來置換該組織集。

- 管理員角色摘要
- 管理員摘要
- 角色摘要
- 使用者問題摘要
- 使用者摘要

如圖 8-3 所示，管理員報告列出了 Identity Manager 管理員、管理員管理的組織，及指定給他們的權能和管理員角色。

圖 8-3　管理員摘要報告



Report Results

Administrator Summary Report

Thursday, January 12, 2006 1:34:05 PM CST

Number of administrators reported: 2

▼Administrator	Managed Organizations	Capabilities
Administrator	Top	Account Administrator Bulk Account Administrator Password Administrator
Configurator	Top	Account Administrator Admin Role Administrator Approver Auditor Administrator Bulk Account Administrator Capability Administrator Import/Export Administrators License Administrator Login Administrator Identity Attributes Administrator Organization Administrator Password Administrator Policy Administrator Reconcile Administrator Remedy Integration Administrator Report Administrator Resource Administrator Resource Group Administrator Resource Object Administrator Resource Password Administrator Role Administrator Security Administrator Service Provider Administrator Identity System Administrator

若要定義 [摘要] 報告，請執行以下步驟：

1. 依照第 269 頁上用以建立報告的指示作業。

   從第二個功能表中，選取前述的其中一個 [摘要] 報告類型。

   [定義報告] 頁面會隨即開啓。

2. 填寫表單並按一下 **[儲存]**。

   對表單若有任何問題，請按一下 **[說明]**。

系統記錄檔報告

系統記錄檔報告會顯示儲存庫中記錄的系統訊息和錯誤。設定此報告時，可以指定要包含或排除下列項目：

- 系統元件 (例如佈建程式、排程程式或伺服器)
- 錯誤代碼
- 嚴重性層級 (錯誤、嚴重或警告)

您還可設定要顯示的最大記錄數 (預設爲 3000)，以及可用記錄超過指定的最大數時，要顯示最舊的記錄還是最新的記錄。

執行 [SystemLog 報告] 時，透過指定目標項目的 Syslog ID 可擷取特定的 Syslog 項目。例如，若要檢視 [最近的系統訊息] 報告中的特定項目，請編輯報告，並選取 **[事件]** 欄位。然後輸入必要的 syslog ID，再按一下 **[執行]**。

備註 您還可執行 `lh syslog` 指令以從系統記錄中擷取記錄。如需有關指令選項的詳細資訊，請閱讀附錄 A 「lh 參照」中的 「syslog 指令」。

若要定義 [系統記錄檔] 報告，請執行以下步驟：

1. 依照第 269 頁上用以建立報告的指示作業。

   從第一個 **[報告類型]** 功能表中選取 **[Identity Manager 報告]**，再從第二個功能表中選取 **[系統記錄檔報告]**。

   [定義報告] 頁面會隨即開啓。

2. 填寫表單並按一下 **[儲存]**。

   對表單若有任何問題，請按一下 **[說明]**。

您設定與儲存報告參數後，請即從 [執行報告] 清單頁面中執行報告。

使用情況報告

建立與執行使用情況報告，以檢視與 Identity Manager 物件 (如管理員、使用者、角色或資源) 有關之系統事件的圖形和 (或) 表格摘要。使用情況報告會以表格顯示資料，您也可以選擇以長條圖、圓餅圖或折線圖格式顯示資料。

若要定義使用情況報告，請執行以下步驟：

1. 依照第 269 頁上用以建立報告的指示作業。

   從第一個 **[報告類型]** 功能表中選取 **[Identity Manager 報告]**，再從第二個功能表中選取 **[使用情況報告]**。

   [定義報告] 頁面會隨即開啓。

2. 填寫表單並按一下 **[儲存]**。

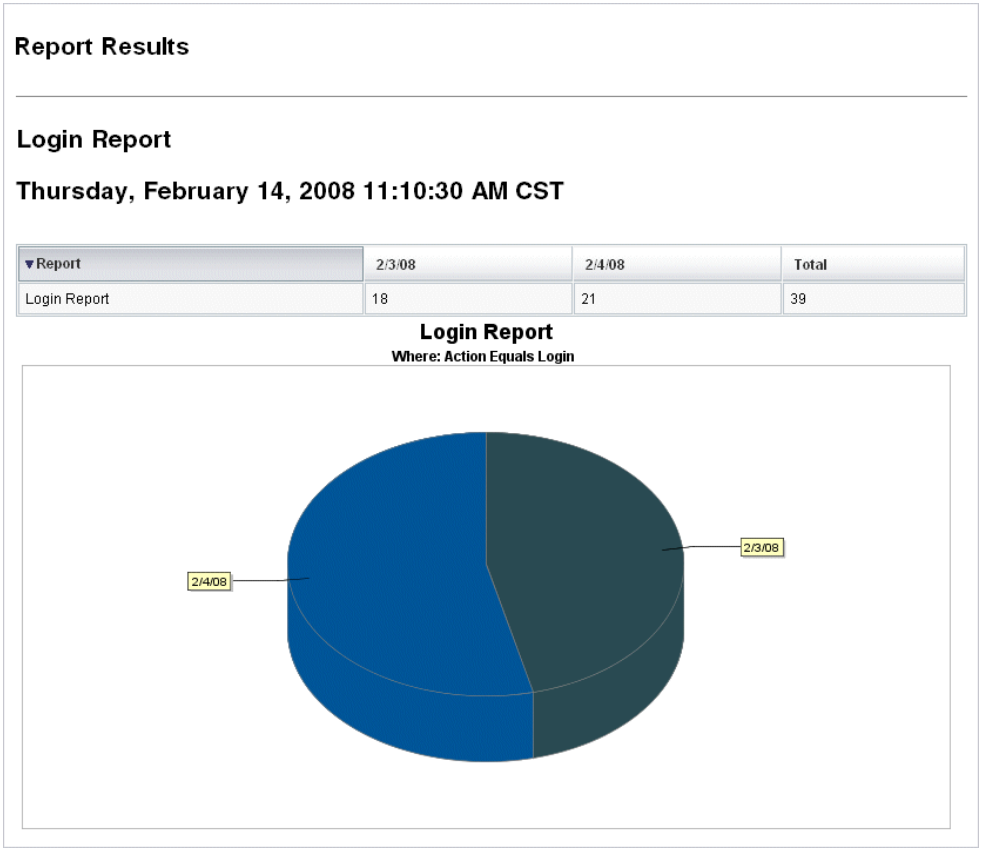
   對表單若有任何問題，請按一下 **[說明]**。

您設定與儲存報告參數後，請即從 [執行報告] 清單頁面中執行報告。

使用情況報告圖表

在圖 8-4 中，最上方的表格會顯示構成報告的事件，而下方的圖表會以圖形格式顯示相同資訊。

圖 8-4　使用情況報告 (產生的使用者帳號)



工作流程報告

此報告會依名稱列出工作流程，並提供以下資訊：

- 工作流程平均完成時間
- 請求工作流程的次數
- 已完成的工作流程請求數

此外，按一下工作流程名稱可開啓工作流程的詳細檢視，其中顯示工作流程中所提供的每個作業，及其平均完成時間。

在擷取效能度量以利驗證是否符合「服務等級協定」(SLA) 目標時，工作流程報告尤其有用。

您必須配置 Identity Manager 使其擷取工作流程時序度量，以做爲執行 「工作流程報告」的先決條件。詳細資訊請參閱下一節。

配置工作流程以擷取稽核時序事件

您必須先對要報告的各個工作流程類型開啓工作流程稽核功能，才能執行 「工作流程報告」。

備註 進行工作流程稽核時會降低效能。因此，只有要與 「工作流程報告」搭配使用的工作流程，始應啓用工作流程稽核。

開啓工作流程稽核，如下所示：

- 針對您可使用作業範本在管理員介面中配置的工作流程，在作業範本配置表單的 **[稽核]** 標籤上選取 **[稽核整個工作流程]** 核取方塊。請參閱第 329 頁的「配置 [稽核] 標籤」，以取得說明。
- 若爲沒有作業範本的工作流程，請參閱第 348 頁的「修改工作流程以記錄計時稽核事件」。

指定要為工作流程報告儲存的屬性

雖然定義屬性並非必要，但若要充分發揮「工作流程報告」的效能，則最好將您後續要用以篩選報告的屬性儲存起來。

若要定義您要爲每個工作流程類型儲存的屬性集，請使用管理員介面的標籤式作業範本配置表單。**[稽核]** 標籤包含 **[稽核屬性]** 區段，此區段位於 **[稽核整個工作流程]** 核取方塊下。請參閱第 329 頁的「配置 [稽核] 標籤」，以取得說明。

定義工作流程報告

若要定義「工作流程報告」，請執行以下步驟：

1. 依照第 269 頁上用以建立報告的指示作業。

   從第一個 **[報告類型]** 功能表中選取 **[Identity Manager 報告]**，再從第二個功能表中選取 **[工作流程報告]**。

   [定義報告] 頁面會隨即開啓。

2. 填寫表單並按一下 **[儲存]**。您可以定義時間參數，以及增加您選擇要稽核的任何屬性 (請參閱上一節中的「指定要爲工作流程報告儲存的屬性」)。

   若要縮小結果，請指定屬性名稱 (如 `user.global.state`)、選取條件，然後輸入屬性值。您可以視需要輸入屬性，數量不限。

   對表單若有任何問題，請按一下 **[說明]**。

設定與儲存報告參數後，請立即從 [執行報告] 頁面執行報告。按一下 **[執行]** 可產生一個包含與已儲存條件相符之所有結果的報告。

報告會依名稱傳回工作流程、平均完成時間、請求工作流程的次數，以及這些請求的完成數目。

按一下工作流程名稱可開啓工作流程的詳細檢視，其中顯示工作流程中所提供的每個作業。由於多個程序可具有相同的已命名作業，因此會依程序來限定作業範圍。

稽核員報告

稽核員報告提供有助於您依據稽核策略中定義的條件管理使用者規範遵循的資訊。

Identity Manager 提供以下稽核員報告：

- 存取檢閱範圍報告
- 存取檢閱詳細資訊報告
- 存取檢閱摘要報告
- 存取掃描使用者範圍報告
- 稽核策略摘要報告
- 已稽核的屬性報告
- 稽核策略違規歷程記錄
- 使用者存取報告
- 組織違規歷程記錄
- 資源違規歷程記錄
- 責任分離報告
- 違規摘要報告

若要定義稽核員報告，請執行第 269 頁的「建立報告」中的步驟。

如需有關稽核員報告的更多資訊，請參閱第 485 頁的「使用 Auditor 報告」。

使用圖形

您可以執行以下與圖形相關的作業：

- 檢視已定義的圖形
- 建立圖形
- 編輯圖形
- 刪除圖形

檢視已定義的圖形

Identity Manager 提供了一些範例圖形。有些使用範例資料，有些不使用。您可以建立適用於您的部署的其他圖形。

在將部署移至生產之前，您應移除範例圖形和範例面板。如果未收集可用的資料，則某些不使用範例資料的範例圖形可能顯示爲空白。

若要檢視已定義的圖形，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[報告]**。
2. 按一下輔助功能表中的 **[面板圖形]**。
3. 從 **[選取面板圖形類型]** 選項清單中，選取面板圖形的種類。

   所選取種類的所有圖形均會顯示在圖形清單中。
4. 按一下圖形名稱。
5. 如果需要，按一下 **[暫停重新整理]** 以暫停面板重新整理。按一下 **[繼續]** 以更新檢視。

備註	對於包含許多圖形的面板，有時暫停重新整理直到初始載入所有圖形是很有幫助的。

6. 如有需要，請按一下 **[立即重新整理]** 以強制執行立即重新整理。
7. 按一下 **[完成]** 以返回 [面板圖形] 清單頁面。

備註 若有圖形顯示錯誤訊息，請開啓要編輯的系統配置物件 (第 197 頁)，並設定 `dashboard.debug=true`。如果此特性已設定，請返回至產生錯誤的圖形，並使用 **[如果要回報問題，請包含此文字程序檔]** 連結擷取圖形程序檔。報告問題時應包含此圖形程序檔。

建立圖形

若要建立面板圖形，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[報告]**。
2. 按一下輔助功能表中的 **[面板圖形]**。
3. 從 [選取面板圖形類型] 選項清單中，選取面板圖形的種類。

   所選取種類的所有圖形均會顯示在圖形清單中。
4. 按一下 **[新增]** 以顯示 [建立面板圖形] 頁面。
5. 輸入 **[圖形名稱]**。增加圖形至面板時以名稱爲依據，因此請選擇唯一而有意義的名稱。
6. 選取 **[登錄]**：[IDM] 或 [SAMPLE]。

   範例資料選項是供您熟悉系統之用。由於並非所有追蹤的事件均具有範例資料，因此這個選項在示範和試驗各種圖形選項時最有用。移至生產環境之前請刪除範例資料。

備註 使用範例資料的追蹤事件集不同於實際追蹤的事件。

7. 從清單中選取所需類型的 **[追蹤的事件]**。

   事件爲系統特徵 (如記憶體使用率) 或事件彙集 (如資源作業)，會追蹤其之前的值並以圖形或圖表形式可視化顯示。

IDM 登錄的追蹤事件包括：

- **佈建程式執行計數** - 追蹤已發生的佈建程式作業數目 (依作業類型)。
- **執行佈建程式的持續時間** - 追蹤每個佈建程式作業的持續時間 (依作業類型)。
- **資源作業計數** - 追蹤資源作業的數目。
- **資源作業持續時間** - 追蹤資源作業的持續時間。
- **工作流程持續時間** - 追蹤執行工作流程所花費的時間。
- **工作流程執行計數** - 追蹤每個工作流程執行的次數。

8. 從清單中選取 **[時間範圍]**。

   此選項控制彙集資料的頻率 (例如一小時) 以及保留資料的頻率 (例如一個月)。系統可以儲存一段相當長的時間範圍內追蹤的事件資料，以獲得系統目前的詳細檢視並瞭解長期趨勢。

9. 從清單中選取 **[度量]**。已選取預設度量，是計數還是平均取決於所選取的追蹤事件。

   每個圖形顯示一種度量。可用的度量取決於所選取的追蹤事件。可使用的度量如下：

   - [計數] - 在該時間間隔內事件發生的總次數
   - [平均] - 在該時間間隔內事件值的算術平均值
   - [最大] - 在該時間間隔內的最大事件值
   - [最小] - 在該時間間隔內的最小事件值
   - [直方圖] - 在該時間間隔內各個事件值範圍的獨立計數

10. 從清單中選取 **[將計數顯示爲]**。

    圖形計數顯示爲原始總數或按不同時間比例進行劃分。

11. 從清單中選取 **[圖形類型]**。

    此選項控制追蹤事件資料的顯示方式。可用的圖形類型取決於所選取的追蹤事件，可以包含線形圖、長條圖及扇形圖。

12. **基本尺寸：**如有需要，請從清單中選取以下選項：

    - **[資源名稱]**。如果已選取，則所有尺寸值都會包含在圖形中。取消選取此選項來選擇要包含在圖形中的個別尺寸值。
    - **[伺服器實例]**。如果已選取，則所有尺寸值都會包含在圖形中。取消選取此選項來選擇要包含在圖形中的個別尺寸值。
    - **[作業類型]**。如果已選取，則所有尺寸值都會包含在圖形中。取消選取此選項來選擇要包含在圖形中的個別尺寸值。

    您選取尺寸後，頁面會重新整理以顯示圖形。

13. **圖形選項：**如有需要，請輸入 **[圖形子標題]**

    這會在圖形的主標題下產生一個子標題。

14. **進階圖形選項**：如有需要，選取 **[進階圖形選項]**。如果您想要設定以下內容，請選取此選項：

    - **網格線**
    - **字型**
    - **調色板**

15. 按一下 **[儲存]** 以建立圖形。

編輯圖形

若要編輯面板圖形，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[報告]**。
2. 按一下輔助功能表中的 **[面板圖形]**。

   [面板圖形] 頁面會隨即開啓。
3. 從 **[選取面板圖形類型]** 下拉式功能表中，選取種類。

   此時會開啓一個表格，列出面板圖形。
4. 按一下圖形名稱加以編輯。

   您可以編輯的圖形屬性因所選圖形而異。您可對以下一個或多個特性進行編輯：

   - **[圖形名稱]** - 圖形將依名稱增加至面板。
   - **登錄** - 指定在登錄中定義的追蹤事件描述。目前選項包括：SAMPLE、服務提供者與 IDM。
   - **[追蹤的事件]** - 系統特徵 (如記憶體使用率) 或事件彙集 (如資源作業)，其之前的值會以可檢視形或圖表追蹤和顯示。
   - **[時間範圍]** - 控制彙集資料的頻率以及保留資料的頻率。
   - **[度量]** - 每個圖形顯示一種度量。可用的度量取決於所選取的追蹤事件。對於所選的度量可能還提供有其他選項。
   - **[圖形類型]** - 控制追蹤事件資料的顯示方式 (例如，線形圖或長條圖)。
   - **包含的尺寸值** - 如果選取此選項，則所有尺寸值都會包含在圖形中。
   - **[圖形子標題]** - 如果需要，在圖形的主標題下輸入子標題。
   - **[進階圖形選項]** - 如果您想要設定以下內容，請選取此選項：
     - **網格線**
     - **字型**
     - **調色板**
5. 按一下 **[儲存]**。

刪除圖形

若要刪除已定義的圖形，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[報告]**。
2. 按一下輔助功能表中的 **[面板圖形]**。
3. 從 **[選取面板圖形類型]** 選項清單中，選取面板圖形的種類。

   所選取種類的所有圖形均會顯示在圖形清單中。
4. 使用核取方塊選取要刪除的圖形，然後按一下 **[刪除]**。

備註 包含圖形的所有面板會直接刪除圖形，而不會先行警告。

使用面板

面板是在單一頁面上檢視的相關圖形的集合。與圖形一樣，Identity Manager 提供了一組範例面板，管理員可根據自己的部署對其進行自訂。請參閱第 292 頁的「建立面板」，以取得說明。

若要檢視面板，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[報告]**。
2. 按一下輔助功能表中的 **[檢視面板]**，以檢視目前定義的面板。

   [面板] 頁面會隨即開啓。
3. 按一下您要檢視之面板旁的 **[顯示]**

備註 對於包含許多圖形的面板，有時暫停重新整理直到初始載入所有圖形是很有幫助的。

按一下 **[暫停]** 可暫停面板重新整理，而按一下 **[重新整理]** 可重新整理檢視。

以下小節提供了使用面板的程序：

- 建立面板
- 編輯面板
- 刪除面板

建立面板

若要建立面板，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[報告]**。
2. 按一下輔助功能表中的 **[檢視面板]**。
3. 按一下 **[新增]。**
4. 輸入新面板的名稱。
5. 輸入新面板摘要。
6. 從清單中選取重新整理率，以秒、分鐘或小時爲單位。

備註 將重新整理率設定爲少於 30 秒會導致包含數個圖形的面板發生問題。

7. 若要將圖形樣式關聯至面板，請從清單中選取適當的項目。

備註 一個圖形可用於多個面板。

8. 若要移除面板圖形，請從清單中選取適當的項目，然後按一下 **[移除圖形]**。
9. 按一下 **[儲存]**。

編輯面板

使用建立面板中說明的程序來編輯面板 (選取 [新增] 除外)，選取要修改的面板並編輯以下屬性：

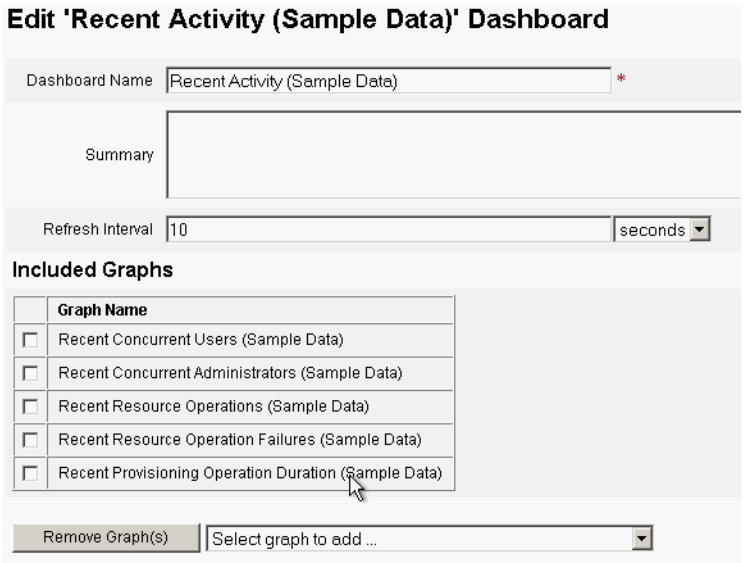
- 面板的名稱。
- 新面板摘要。
- 清單中的重新整理率，以秒、分鐘或小時爲單位。
- 增加或移除與面板關聯的圖形。

備註 從面板上移除某個圖形並不會將其刪除。該圖形仍可與其他面板配合使用。

一個圖形可用於多個面板。

圖 8-5 說明了範例面板編輯頁面。

圖 8-5 編輯面板



刪除面板

若要刪除 [服務提供者] 面板，請從 [服務提供者] 區域按一下 **[管理面板]**，然後選取需要的面板並按一下 **[刪除]**。

備註 使用此程序並不會移除面板中包含的圖形。請使用 [管理面板圖形] 頁面刪除圖形 (請參閱 「刪除圖形」)。

系統監視

您可以將 Identity Manager 設定爲即時追蹤事件，並可透過在面板圖形中檢視它們來監視事件。面板可讓您快速評估系統資源和找出異常，以瞭解之前的效能趨勢 (根據一天中的某時間、一週中的某天等)，並且在查看稽核記錄前以互動的方式鎖定問題。它們不提供與稽核記錄同樣詳細的資料，但其爲您提供在記錄中何處尋找問題的提示。

您可以建立圖形面板顯示，以在更高層級追蹤自動作業和手動作業。Identity Manager 提供了範例資源作業面板圖形。資源作業面板圖形可讓您快速監視系統資源，以將服務保持在可接受的層級。

您可以在資源作業面板中檢視這些圖形的範例資料。如需有關使用面板的更多資訊，請參閱第 291 頁的「使用面板」。

根據您的指定，系統會在各個層級收集並彙集統計資料，以顯示即時檢視。

追蹤的事件配置

在 [配置報告] 頁面的 [追蹤事件的配置] 區域，您可以確定目前是否已啓用追蹤事件的統計集合，並可將其啓用。按一下 **[啓用事件收集]** 可以啓用追蹤事件配置。

可爲事件集合指定以下選項：

- **時區** - 此選項可設定在記錄追蹤的事件時要使用的時區。其主要決定日期的劃分。

  或者，您也可以將時區設定爲伺服器上設定的預設時區。

- **要收集的時間範圍** - 此選項可指定彙集資料的時間間隔 (也就是收集和保存資料的頻率)。例如，如果選取一分鐘間隔，則資料將每分鐘收集並保存一次。

系統可儲存長時間的追蹤事件資料，不但能檢視系統目前的詳細資訊，也能瞭解長期趨勢。

可用的時間範圍如下。依預設全部選取。請取消選取不需要的收集間隔。

- 10 秒間隔
- 1 分鐘間隔
- 1 小時間隔
- 1 天間隔
- 1 週間隔
- 1 個月間隔

配置追蹤事件後，請使用面板來監視追蹤事件。請視需要使用滑動軸放大圖表的選取部分。

風險分析

您可以利用 Identity Manager 的風險分析功能報告其設定檔超出了某些安全性限制的使用者帳號。風險分析報告會掃描實體資源來收集資料，並依資源顯示有關停用帳號、已鎖定的帳號及無所有者帳號的詳細資訊。它們還會提供有關過期密碼的詳細資訊。報告詳細資訊會隨資源類型的變化而有所不同。

備註 可提供 AIX、HP、Solaris、NetWare NDS 和 Windows Active Directory 資源的標準報告。

風險分析頁面由表單控制，並可針對您的特定環境進行配置。您可以在 idm\debug 頁面的 RiskReportTask 物件下找到一份表單清單 (第 59 頁)，並可使用 Identity Manager IDE 對其進行修改 (第 60 頁)。如需有關配置 Identity Manager 表單的更多資訊，請參閱 「Identity Manager Workflows, Forms, and Views」。

建立風險分析報告

若要建立風險分析報告，請使用以下步驟：

1. 在管理員介面中，按一下主功能表的 **[報告]**。
2. 按一下輔助功能表的 **[執行風險分析]**。
3. 在 **[新增...]** 下拉式功能表中，選取要建立的報告。

   [風險分析報告設定] 頁面會隨即開啓。
4. 填寫表單。

   您可以將報告限制爲只掃描選取的資源，且您可以根據資源類型，掃描符合下列條件的帳號：

   - 已停用、過期、非使用中或已鎖定的帳號
   - 從未使用過的帳號
   - 沒有完整名稱或密碼的帳號
   - 不需要密碼的帳號
   - 密碼已到期或密碼在指定天數內未變更的帳號
5. 按一下 **[儲存]**。

排程風險分析報告

定義後，您就可以將風險分析報告排程爲以指定間隔執行。

若要排程風險分析報告，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[伺服器作業]**。
2. 按一下輔助功能表的 **[管理排程]**。

   [已排程的作業] 頁面會隨即開啓。
3. 選取要排程的風險分析報告。

   [建立新的風險分析作業排程] 頁面會隨即開啓。
4. 輸入名稱與排程資訊，然後選擇性調整其他風險分析選擇。
5. 按一下 **[儲存]** 以儲存排程。

第 9 章

作業範本

Identity Manager 的**作業範本**可讓您使用管理員介面，配置某些工作流程運作方式，作爲編寫自訂工作流程的一種替代方法。

本章分爲以下各節：

- 啓用作業範本 - 說明如何在系統中提供作業範本
- 配置作業範本 - 說明如何使用作業範本配置工作流程的運作方式

啟用作業範本

Identity Manager 提供了以下您可配置的作業範本：

- **建立使用者範本** - 配置用於建立使用者作業的特性。
- **刪除使用者範本** - 配置用於刪除使用者作業的特性。
- **更新使用者範本** - 配置用於更新使用者作業的特性。

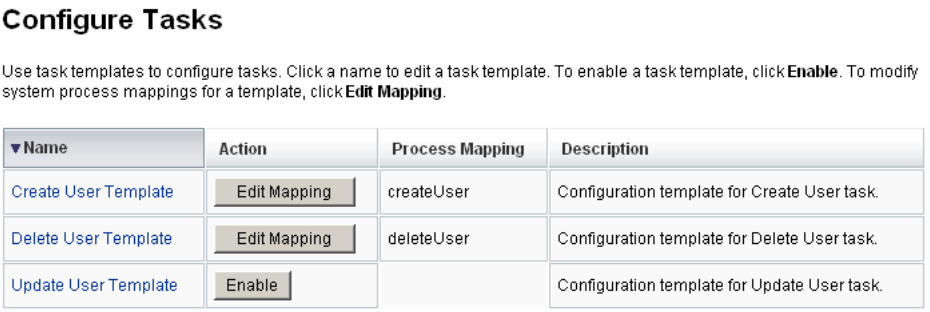
在使用作業範本之前，必須對映作業範本的程序。

若要對映程序類型，請執行以下步驟：

1. 在管理員介面中，從功能表選取 **[伺服器作業]**，然後選取 **[配置作業]**。

   圖 9-1 說明 [配置作業] 頁面。

圖 9-1 配置作業



[配置作業] 頁面包含一個表格，其中具有以下欄：

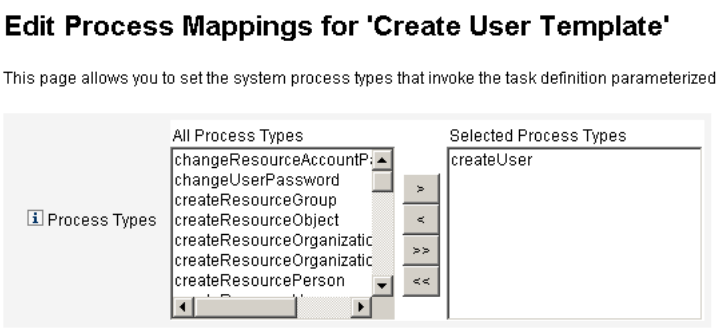
- **名稱** - 提供 [建立使用者範本]、[刪除使用者範本] 和 [更新使用者範本] 的連結。
- **動作** - 包含以下按鈕之一：
  - **啓用** - 如果您尚未啓用範本，則顯示此按鈕。
  - **編輯對映** - 啓用範本之後會顯示此按鈕。

  啓用和編輯程序對映的程序是一樣的。
- **程序對映** - 列出與每個範本對映的程序類型。
- **描述** - 提供每個範本的簡短描述。

2. 按一下 **[啓用]** 以開啓範本的 [編輯程序對映] 頁面。

   例如，對於 [建立使用者範本]，會顯示以下頁面 (圖 9-2)：

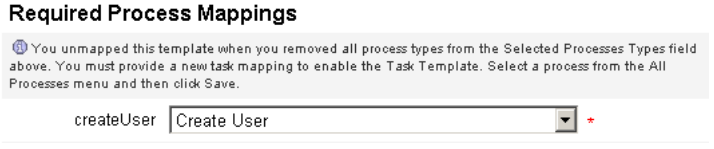
圖 9-2 [編輯程序對映] 頁面



備註 預設程序類型 (在此情況下，爲 createUser) 會自動顯示在 [已選取的程序類型] 清單中。如有必要，您可以從該功能表中選取其他程序類型。

- 通常，請勿爲每個範本對映多個程序類型。
- 如果從 [已選取的程序類型] 清單中移除程序類型，但未選取替代的程序類型，則將顯示 [必要的程序對映] 區段，指示您選取一個新的作業對映。

圖 9-3 必要的程序對映區段



3. 按一下 **[儲存]** 可對映選取的程序類型並返回到 [配置作業] 頁面。

備註 重新顯示 [配置作業] 頁面後，**[編輯對映]** 按鈕將替代 **[啓用]** 按鈕，而且程序名稱將列在 [程序對映] 欄中。

圖 9-4 更新的 [配置作業] 表

▼Name	Action	Process Mapping	Description
Create User Template	Edit Mapping	createUser	Configuration template for Create User task.
Delete User Template	Enable		Configuration template for Delete User task.
Update User Template	Enable		Configuration template for Update User task.

4. 爲剩餘的每個範本重複該對映程序。

備註

- 您可以選取 **[配置] > [表單與程序對映]**，以驗證對映。顯示 [配置表單與程序對映] 頁面後，向下捲動到 [程序對映] 表，並驗證以下程序類型已對映到該表中顯示的 [與下列項目對映的處理程序名稱] 項目。

程序類型	程序名稱對映至
createUser	建立使用者範本
deleteUser	Delete User Template
updateUser	更新使用者範本

  如果成功啓用範本，則 [與下列項目對映的處理程序名稱] 項目應該均包含文字 Template。

- 如果在 **[與下列項目對映的處理程序名稱]** 欄中鍵入**範本** (如表中所示)，則您還可以直接從 [表單與程序對映] 頁面對映這些程序類型。

配置作業範本

對映範本程序類型後 (第 300 頁)，即可配置作業範本。

若要配置作業範本，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[伺服器作業]**，再按一下 **[配置作業]**。

   [配置作業] 頁面會隨即開啓。

2. 選取 **[名稱]** 欄中的連結。將顯示以下頁面之一：

   - **編輯作業範本「建立使用者範本」** - 開啓此頁面可編輯用以建立新使用者帳號的範本。
   - **編輯作業範本「刪除使用者範本」** - 開啓此頁面可編輯用於刪除或取消佈建使用者帳號的範本。
   - **編輯作業範本「更新使用者範本」** - 開啓此頁面可編輯用於更新現有使用者資訊的範本。

   每個 [編輯作業範本] 頁面包含一組標籤，代表使用者工作流程的主要配置區域。

   下表說明了每個標籤、其用途以及哪些範本使用該標籤。

表 9-1 作業範本標籤

標籤名稱	用途	範本
一般 (預設標籤)	使您可以定義作業名稱在 [首頁] 和 [帳號] 頁面上的作業列中以及 [作業] 頁面的作業實例表中如何顯示。	僅 [建立使用者作業範本] 和 [更新使用者作業範本]
	讓您可以指定如何刪除/取消佈建使用者帳號	僅 [刪除使用者範本]
Notification	讓您可以配置在 Identity Manager 呼叫程序時傳送給管理員和使用者的電子郵件通知。	所有範本
核准	讓您可以按類型啟用或停用核准、定義其他核准人、在 Identity Manager 執行某些作業之前指定帳號資料的屬性。	所有範本
Audit	讓您可以啟用和配置工作流程的稽核。使用此標籤可配置工作流程，為 「工作流程報告」擷取資訊。	所有範本
佈建	讓您可以在背景執行作業並允許 Identity Manager 在作業失敗後重試該作業。	僅 [建立使用者作業範本] 和 [更新使用者作業範本]
生效和失效	讓您暫停建立作業直到指定的日期/時間 (生效)，或暫停刪除作業直到指定的日期/時間 (失效)。	建立使用者作業範本
資料轉換	讓您可以配置在佈建期間如何變換使用者資料。	僅 [建立使用者作業範本] 和 [更新使用者作業範本]

3. 選取其中一個標籤來配置範本的工作流程功能。

   以下章節提供了配置這些標籤的說明：

   - 第 305 頁的「配置 [一般] 標籤」
   - 第 308 頁的「配置 [通知] 標籤」
   - 第 314 頁的「配置 [核准] 標籤」
   - 第 329 頁的「配置 [稽核] 標籤」
   - 第 331 頁的「配置 [佈建] 標籤」
   - 第 332 頁的「配置 [生效和失效] 標籤」
   - 第 338 頁的「配置 [資料轉換] 標籤」

4. 您配置完這些範本後，請按一下 **[儲存]** 按鈕以儲存您的變更。

配置 [一般] 標籤

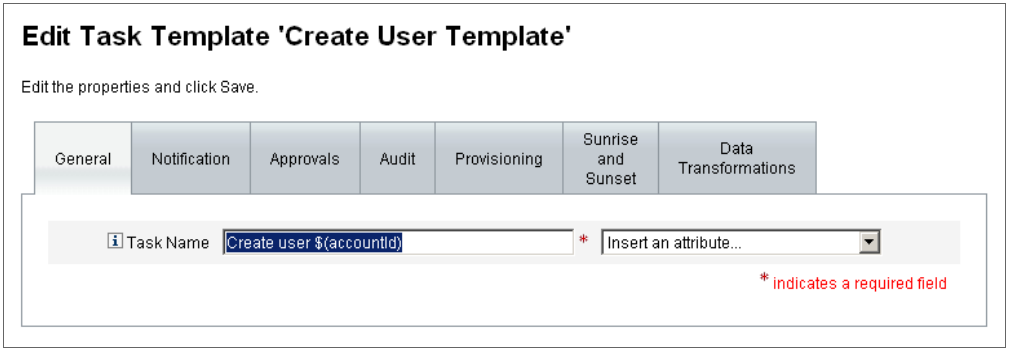
本節提供配置 **[一般]** 標籤的說明，此爲作業範本配置程序的一部份。如需如何啓動配置程序的說明，請參閱第 303 頁。

備註 在管理員介面中，用於編輯 [建立使用者範本] 及 [更新使用者範本] 的頁面是相同的，所以在同一節中說明配置。

對於 [建立使用者範本] 或 [更新使用者範本]

當您開啓 [編輯作業範本「建立使用者範本」] 表單或 [編輯作業範本「更新使用者範本」] 表單時，預設會顯示 **[一般]** 標籤頁。此頁面由 **[作業名稱]** 文字欄位及 **[插入屬性]** 功能表所組成，如圖 9-5 所示。如需如何啓動配置程序的說明，請參閱第 303 頁。

圖 9-5 [一般] 標籤：建立使用者範本



作業名稱可以包含字元和/ 或可在作業執行期間解析的屬性參照。

若要變更預設的作業名稱，請執行以下步驟：

1. 在 **[作業名稱]** 欄位鍵入名稱。

   您可以編輯或完全替代預設的作業名稱。

2. **[作業名稱]** 功能表會提供目前爲與此範本配置的作業相關聯的檢視而定義的屬性清單。從功能表中選取一個屬性 (**選擇性**)。

   Identity Manager 會將該屬性名稱附加到 [作業名稱] 欄位中的項目。例如：

   ```
   Create user $(accountId) $(user.global.email)
   ```

3. 完成後，您可以
   - 選取其他標籤繼續編輯該範本。
   - 按一下 **[儲存]** ，以儲存變更並返回到 [配置作業] 頁面。
   - 新的作業名稱會顯示在 Identity Manager 作業列中，位於 **[首頁]** 及 **[帳號]** 標籤的底部。
   - 按一下 **[取消]**，以放棄變更並返回到 [配置作業] 頁面。

對於 [刪除使用者範本]

當您開啓 [編輯作業範本「刪除使用者範本」] 頁面時，預設會顯示 **[一般]** 標籤頁 (如需如何啓動配置程序的說明，請參閱第 303 頁)。

若要指定如何刪除/取消佈建使用者帳號，請執行以下步驟：

1. 使用 **[刪除 Identity Manager 帳號]** 按鈕可以指定 Identity Manager 帳號是否可以在刪除作業期間被刪除，如下所示：
   - **永不** - 選取此項目可防止帳號遭刪除。
   - **僅當使用者在取消佈建後沒有連結的帳號時** - 選取此項目，會在僅當取消佈建後沒有連結的資源帳號時，才可以刪除使用者帳號。
   - **一律** - 選取此項目，則無論何種情況都允許刪除使用者帳號，即使仍有已指定的資源帳號。
2. 使用 **[取消佈建資源帳號]** 方塊可控制**所有**資源帳號的取消佈建作業，如下所示：
   - **全部刪除** - 啓用此方塊可以刪除所有指定資源中代表該使用者的所有帳號。
   - **全部取消指定** - 啓用此方塊可以取消指定給該使用者的所有資源帳號。無法刪除資源帳號。
   - **全部取消連結** - 啓用此方塊，可以中斷 Identity Manager 系統與資源帳號的全部連結。擁有指定但未連結帳號的使用者顯示時會帶有標記，以表示需要更新。

備註 這些控制項會置換 [取消佈建個別資源帳號] 表中的運作方式。

3. 使用 **[取消佈建個別資源帳號]** 方塊，可以對使用者取消佈建進行更細致的操作 (與 [取消佈建資源帳號] 相比)，如下所述：

   - **刪除** - 啓用此方塊，可以刪除此資源中代表該使用者的帳號。
   - **取消指定** - 啓用此方塊，則不再將該使用者直接指定到此資源。無法刪除資源帳號。
   - **取消連結** - 啓用此方塊，可以中斷 Identity Manager 系統與資源帳號的連結。擁有指定但未連結帳號的使用者顯示時會帶有標記，以表示需要更新。

備註 如果您要爲不同的資源指定不同的取消佈建策略，則 **[取消佈建個別資源帳號]** 選項將很有用。例如，大部分客戶不想刪除 Active Directory 使用者，因爲每個使用者具有一個全域識別碼，刪除後便無法重新建立。

但是，在增加新資源的環境中，您可能不需要使用此選項，因爲每次增加新資源時都必須更新取消佈建配置。

配置 [通知] 標籤

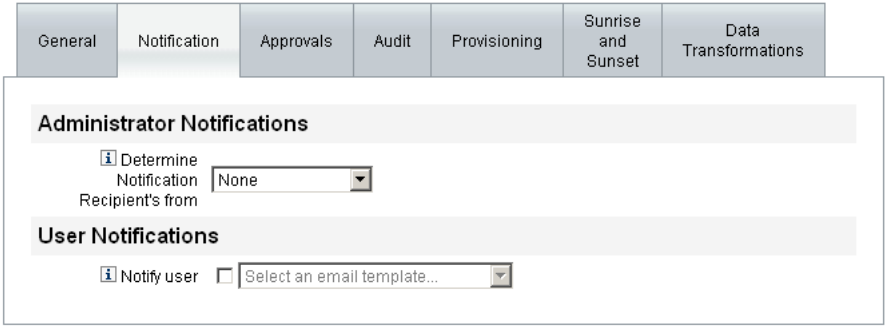
本節提供配置 **[通知]** 標籤的說明，此爲作業範本配置程序的一部份。如需如何啓動配置程序的說明，請參閱第 303 頁。

所有作業範本都支援在 Identity Manager 呼叫程序後 (通常在該程序完成後)，向管理員和使用者傳送電子郵件通知。您可以使用 [通知] 標籤來配置這些通知。

備註 Identity Manager 使用電子郵件範本，向管理員、核准人和使用者傳送資訊和動作請求。如需有關 Identity Manager 電子郵件範本的更多資訊，請參閱本指南中標題爲 「瞭解電子郵箱範本」的小節。

圖 9-6 顯示 [建立使用者範本] 的 **[通知]** 頁面。

圖 9-6 [通知] 標籤：建立使用者範本



配置使用者通知

指定要通知的使用者時，您還必須指定要用於產生通知電子郵件的電子郵件範本名稱。

若要通知已建立、更新或遭刪除的使用者，請啓用 **[通知使用者]** 核取方塊 (如圖 9-7 所示)，然後從清單中選取電子郵件範本。

圖 9-7　指定電子郵件範本

配置管理員通知

若要指定 Identity Manager 如何決定管理員通知收件者，請選取 **[確定通知收件者取得來源]** 功能表的選項。

可用的選項如下：

- **無** (預設值) - 不通知任何管理員。
- **屬性** - 選取此選項，可從使用者檢視中指定的屬性導出通知收件者的帳號 ID。如需更多資訊，請參閱第 310 頁的「依屬性指定管理員通知收件者」。
- **規則** - 選取此選項，可透過評估指定的規則以導出通知收件者的帳號 ID。如需更多資訊，請參閱第 311 頁的「依規則指定管理員通知收件者」。
- **查詢** - 選取此選項，可透過查詢特定資源以導出通知收件者的帳號 ID。如需更多資訊，請參閱第 312 頁的「依查詢指定管理員通知收件者」。
- **管理員清單** - 選取此選項，可從清單中明確選擇通知收件者。如需更多資訊，請參閱第 313 頁的「從管理員清單指定管理員通知收件者」。

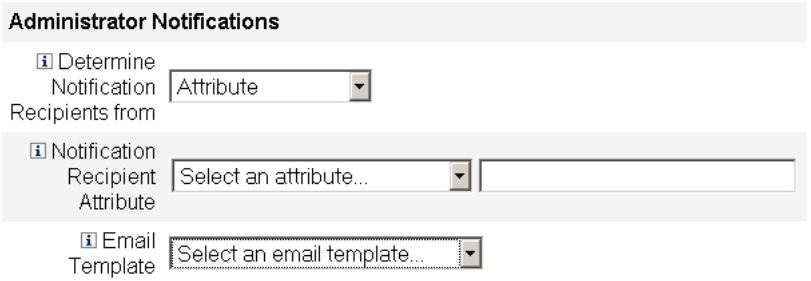
依屬性指定管理員通知收件者

若要從指定的屬性導出通知收件者的帳號 ID，請執行以下步驟：

備註 此屬性必須解析爲可表示單一帳號 ID 的字串或解析爲帳號 ID 的清單。

1. 從 **[確定通知收信人取得來源]** 功能表中選取 **[屬性]**，將顯示以下新選項：

圖 9-8 管理員通知：屬性



   - **通知收件者屬性** - 提供用於確定收件者帳號 ID 的屬性清單，其中的屬性是目前爲檢視所定義的屬性，該檢視與此範本所配置的作業相關聯。
   - **電子郵件範本** - 提供電子郵件範本的清單。

2. 從 **[通知收信人屬性]** 功能表中選取屬性。

   屬性名稱會顯示在功能表旁邊的文字欄位中。

3. 從 **[電子郵件範本]** 功能表中選取範本，以指定管理員通知電子郵件的格式。

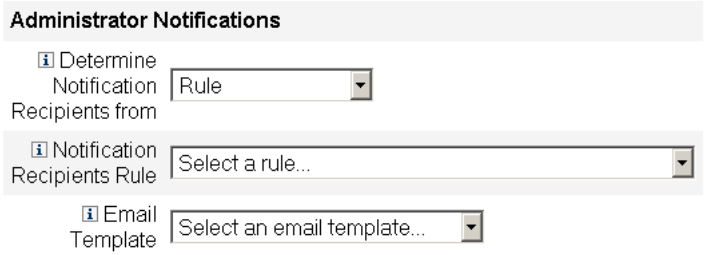
依規則指定管理員通知收件者

若要從指定的規則導出通知收件者的帳號 ID，請執行以下步驟：

備註 計算之後，此規則必須傳回代表單一帳號 ID 的字串或其元素爲帳號 ID 的清單。

1. 從 **[確定通知收信人取得來源]** 功能表中選取 **[規則]**，將會在 [通知] 表單中顯示以下新選項：

   圖 9-9 管理員通知：規則

   - **通知收件者規則** - 提供目前爲系統所定義之規則的清單，這些規則經過計算後，會傳回收件者的帳號 ID。
   - **電子郵件範本** - 提供電子郵件範本的清單。

2. 從 **[通知收信人規則]** 功能表中選取規則。
3. 從 **[電子郵件範本]** 功能表中選取範本，以指定管理員通知電子郵件的格式。

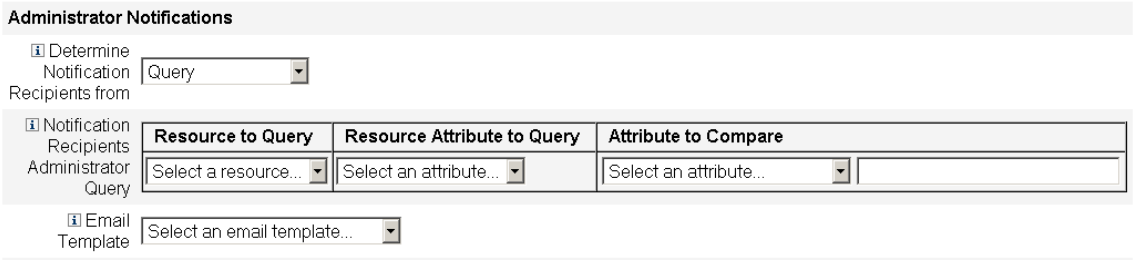
依查詢指定管理員通知收件者

若要查詢指定的資源，以導出通知收件者的帳號 ID，請執行以下步驟：

備註 目前僅支援 LDAP 和 Active Directory 資源查詢。

1. 從 **[確定通知收信人取得來源]** 功能表中選取 **[查詢]**，將會在 [通知] 表單中顯示以下新選項，如圖 9-10 中所示：

圖 9-10 管理員通知：查詢



通知收件者的管理員查詢 - 提供由下列功能表組成的表格，可用來建構查詢：

- **要查詢的資源** - 提供目前爲系統所定義之資源的清單。
- **要查詢的資源屬性** - 提供目前爲系統所定義之資源屬性的清單。
- **要比較的屬性** - 提供目前爲系統所定義之屬性的清單。
- **電子郵件範本** - 提供電子郵件範本的清單。

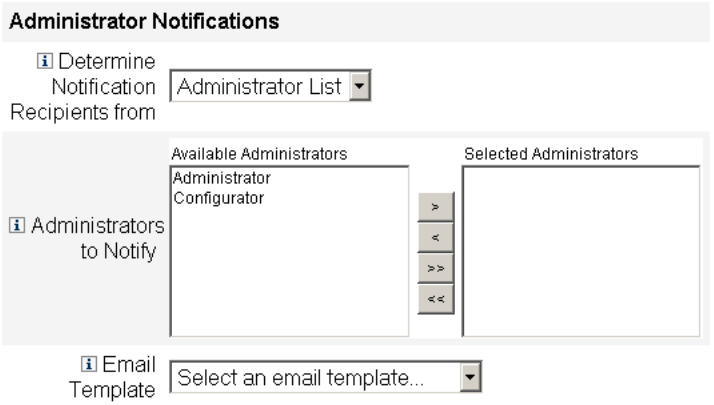
2. 從這些功能表中選取資源、資源屬性和要比較的屬性以建構查詢。
3. 從 **[電子郵件範本]** 功能表中選取範本，以指定管理員通知電子郵件的格式。

從管理員清單指定管理員通知收件者

若要從管理員清單指定管理員通知收件者，請執行以下步驟：

1. 從 **[確定通知收件者取得來源]** 功能表中選取 **[管理員清單]**，[通知] 表單即會顯示下列新選項：

圖 9-11 管理員通知：管理員清單



- **要通知的管理員** - 提供選取工具和可用管理員的清單。
- **電子郵件範本** - 提供電子郵件範本的清單。

2. 從 [可用管理員] 清單中選取一個或多個管理員，並將其移至 [選取的管理員] 清單中。
3. 從 **[電子郵件範本]** 功能表中選取範本，以指定管理員通知電子郵件的格式。

配置 [核准] 標籤

本節提供配置 **[核准]** 標籤的說明，此爲作業範本配置程序的一部份。如需如何啓動配置程序的說明，請參閱第 303 頁。

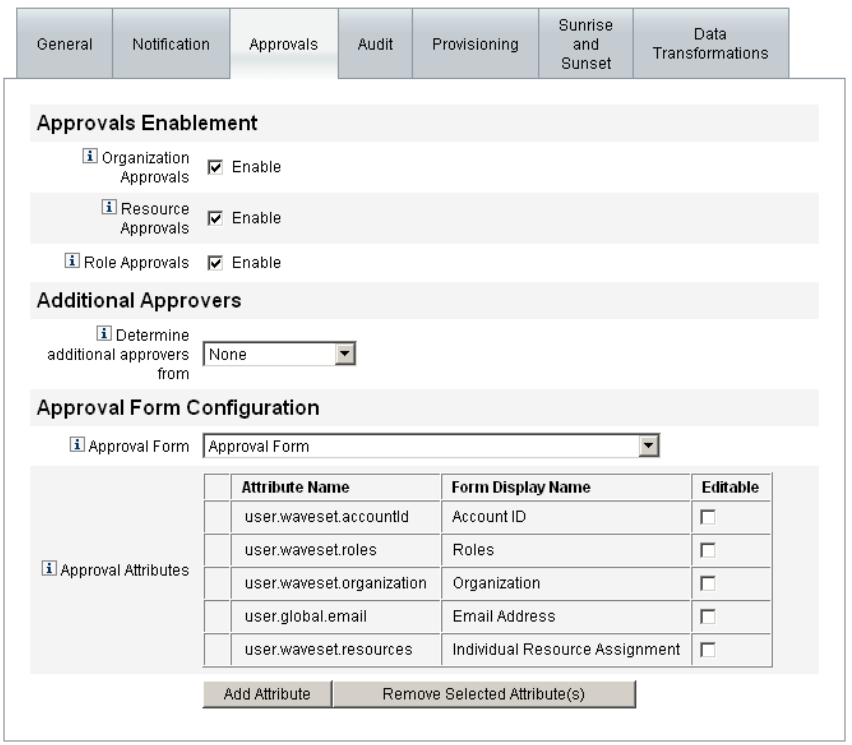
您可以使用 [核准] 標籤指定附加核准人，並在 Identity Manager 執行建立、刪除或更新使用者作業之前指定作業核准表單的屬性。

傳統的方式爲，在執行某些作業之前，需要與特定組織、資源或角色相關聯的管理員對作業進行核准。Identity Manager 也可讓您指定其他核准人，即需要對作業進行核准的其他管理員。

備註 如果您爲工作流程配置其他核准人，則需要取得原有核准人和範本中指定的任何其他核准人的核准。

圖 9-12 說明初始 [核准] 頁面的管理員使用者介面。

圖 9-12 [核准] 標籤：建立使用者範本



若要配置核准，請使用以下步驟：

1. 完成 [核准的軟體權利文件] 區段 (請參閱第 315 頁的 「啓用核准 ([核准啓用] 區段的 [核准] 標籤)」)。
2. 完成 [其他核准人] 區段 (請參閱第 316 頁的 「指定其他核准人 ([其他核准人] 區段的 [核准] 標籤)」)。
3. 完成 [核准表單配置] 區段 (僅 [建立使用者範本] 和 [更新使用者範本]) (請參閱第 325 頁的 「配置核准表單 ([核准表單配置] 區段的 [核准] 標籤)」)。
4. 您配置完 [核准] 標籤後，可以
   - 選取其他標籤繼續編輯該範本。
   - 按一下 **[儲存]** ，以儲存變更並返回到 [配置作業] 頁面。
   - 按一下 **[取消]**，以放棄變更並返回到 [配置作業] 頁面。

啟用核准 ([核准啟用] 區段的 [核准] 標籤)

使用以下 **[核准的軟體權利文件]** 核取方塊可以在建立使用者、刪除使用者或更新使用者作業進行之前要求核准。

備註 依預設，[建立使用者範本] 和 [更新使用者範本] 會啓用這些核取方塊，但 [刪除使用者範本] 則會**停用**。

- **組織核准** - 啓用此核取方塊可以請求所有已配置的組織核准人進行核准。
- **資源核准** - 啓用此核取方塊可以請求所有已配置的資源核准人進行核准。
- **角色核准** - 啓用此核取方塊可以請求所有已配置的角色核准人進行核准。

指定其他核准人 ([其他核准人] 區段的 [核准] 標籤)

使用 **[確定其他核准人取得來源]** 功能表，可以指定 Identity Manager 將如何爲建立使用者、刪除使用者或更新使用者作業確定其他核准人。

本功能表的選項會列在表 9-2 中。

表 9-2 [確定其他核准人取得來源] 功能表選項

選項	說明
None (預設)	**執行作業不需要其他核准人。**
屬性	**從使用者檢視中指定的屬性內導出核准人的帳號 ID。**
Rule	**透過評估指定的規則以導出核准人的帳號 ID。**
查詢	**透過查詢特定資源以導出核准人的帳號 ID。**
Administrator List	**從清單明確選擇核准人。**

若選取這些選項中的任何一個 (除了 **[無]** 以外)，則管理員使用者介面中都將顯示其他選項。

使用以下各章節提供的說明來指定確定其他核准人的方法。

- 透過屬性 (第 317 頁)
- 透過規則 (第 318 頁)
- 透過查詢 (第 319 頁)
- 透過管理員清單 (第 320 頁)

從屬性確定其他核准人

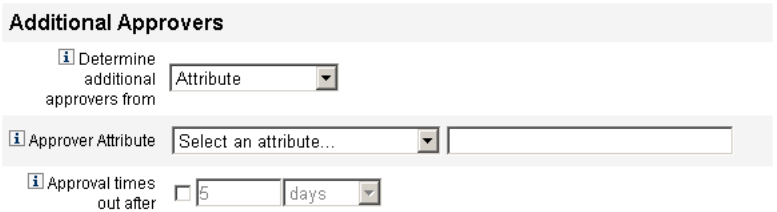
若要從屬性確定其他核准人，請執行以下步驟。

1. 從 **[確定其他核准人取得來源]** 功能表選取 **[屬性]**。

備註 此屬性必須解析爲可表示單一帳號 ID 的字串或解析爲帳號 ID 的清單。

將顯示以下新選項：

圖 9-13 其他核准人：屬性



- **核准人屬性** - 提供用於確定核准人帳號 ID 的屬性清單，其中的屬性是目前爲檢視所定義的屬性，該檢視與此範本所配置的作業相關聯。
- **核准逾時期限** - 提供用於指定核准何時逾時的方法。

備註 **[核准逾時期限]** 設定會影響初始核准和上報的核准。

2. 使用 **[核准人屬性]** 功能表來選取屬性。

   選取的屬性將顯示在旁邊的文字欄位中。

3. 決定您是否要在指定的時間期間之後核准逾時請求。
   - 如果您要指定逾時期間，則請繼續閱讀第 321 頁的「配置核准逾時 ([核准逾時期限] 區段)」，以取得說明。
   - 如果您不想指定逾時期間，則可以繼續執行第 325 頁的「配置核准表單 ([核准表單配置] 區段的 [核准] 標籤)」，或儲存變更並繼續配置其他標籤。

從規則確定其他核准人

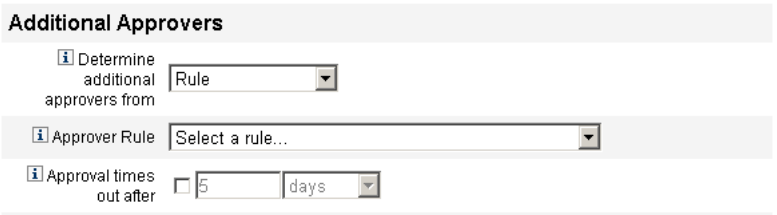
若要從指定的規則導出核准人的帳號 ID，請執行以下步驟：

1. 從 **[確定其他核准人取得來源]** 功能表選取 **[規則]**。

備註 計算之後，此規則必須傳回代表單一帳號 ID 的字串或其元素爲帳號 ID 的清單。

將顯示以下新選項。

圖 9-14 其他核准人：規則



- **核准人規則** - 提供目前爲系統所定義之規則的清單，這些規則經過計算後，會傳回收件者的帳號 ID。
- **核准逾時期限** - 提供用於指定核准何時逾時的方法。

備註 **[核准逾時期限]** 設定會影響初始核准和上報的核准。

2. 從 **[核准人規則]** 功能表中選取規則。
3. 決定您是否要在指定的時間期間之後核准逾時請求。
   - 如果您要指定逾時期間，則請繼續閱讀第 321 頁的「配置核准逾時 ([核准逾時期限] 區段)」，以取得說明。
   - 如果您不想指定逾時期間，則可以繼續執行第 325 頁的「配置核准表單 ([核准表單配置] 區段的 [核准] 標籤)」，或儲存變更並繼續配置其他標籤。

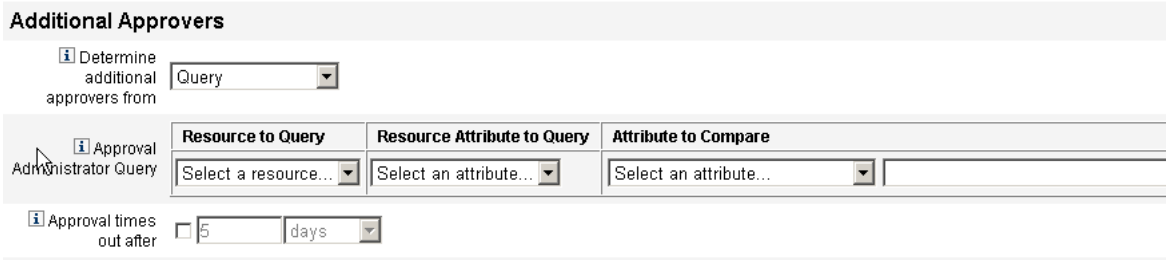
從查詢確定其他核准人

備註 目前僅支援 LDAP 和 Active Directory 資源查詢。

若要查詢指定的資源，以導出核准人的帳號 ID，請執行以下步驟：

1. 從 **[確定其他核准人取得來源]** 功能表中選取 **[查詢]**，將會顯示以下新選項：

圖 9-15 其他核准人：查詢



- **核准管理員查詢** - 提供由下列功能表組成的表格，可用來建構查詢：
  - **要查詢的資源** - 提供目前爲系統所定義之資源的清單。
  - **要查詢的資源屬性** - 提供目前爲系統所定義之資源屬性的清單。
  - **要比較的屬性** - 提供目前爲系統所定義之屬性的清單。
- **核准逾時期限** - 提供用於指定核准何時逾時的方法。

備註 **[核准逾時期限]** 設定會影響初始核准和上報的核准。

2. 如下所示，建構一個查詢：
   a. 從 **[要查詢的資源]** 功能表中選取資源。
   b. 從 **[要查詢的資源屬性]** 和 **[要比較的屬性]** 功能表中選取屬性。
3. 決定您是否要在指定的時間期間之後核准逾時請求。
   - 如果您要指定逾時期間，則請繼續閱讀第 321 頁的「配置核准逾時 ([核准逾時期限] 區段)」，以取得說明。

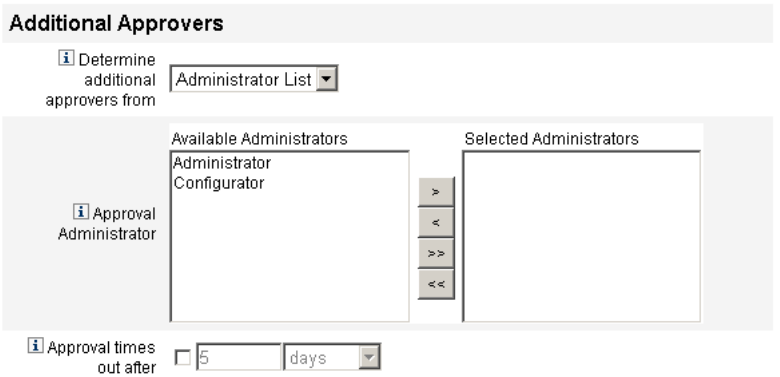
- 如果您不想指定逾時期間，則可以繼續執行第 325 頁的「配置核准表單 ([核准表單配置] 區段的 [核准] 標籤)」，或儲存變更並繼續配置其他標籤。

從管理員清單確定其他核准人

若要從 [管理員清單] 明確選擇其他核准人，請執行以下步驟：

1. 從 **[確定其他核准人取得來源]** 功能表中選取 **[管理員清單]** ，即會顯示下列新選項：

圖 9-16 其他核准人：管理員清單



- **要通知的管理員** - 提供選取工具和可用管理員的清單。
- **核准表單** - 提供其他核准人可用於核准或拒絕核准請求的使用者表單之清單。
- **核准逾時期限** - 提供用於指定核准何時逾時的方法。

備註 **[核准逾時期限]** 設定會影響初始核准和上報的核准。

2. 從 [可用管理員] 清單中選取一個或多個管理員，並將選取的名稱移至 [選取的管理員] 清單中。
3. 決定您是否要在指定的時間期間之後核准逾時請求。
   - 如果您要指定逾時期間，則請繼續閱讀第 321 頁的「配置核准逾時 ([核准逾時期限] 區段)」，以取得說明。
   - 若不要指定逾時期間，請繼續進入第 325 頁的「配置核准表單 ([核准表單配置] 區段的 [核准] 標籤)」。

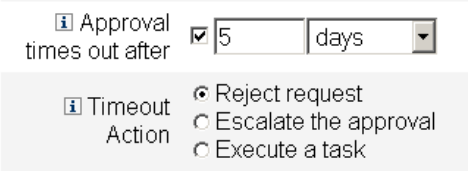
配置核准逾時 ([核准逾時期限] 區段)

若要配置核准逾時，請執行以下步驟：

1. 選取 **[核准逾時期限]** 核取方塊。

   相鄰的文字欄位和功能表會變爲可使用狀態，並顯示 **[逾時動作]** 選項，如下圖中所示。

   圖 9-17 [核准逾時] 選項

2. 使用 **[核准逾時期限]** 文字欄位和功能表可以指定逾時期間，如下所示：

   a. 請從功能表選取 **[秒]**、**[分鐘]**、**[小時]** 或 **[天]**。

   b. 在文字欄位中輸入數字，表示您要爲逾時指定多少秒、分鐘、小時或天。

備註 **[核准逾時期限]** 設定會影響初始核准和上報的核准。

3. 選取以下 **[逾時動作]** 按鈕之一，指定核准請求逾時後應執行的作業：

   - **拒絕請求** - 如果在指定的逾時期間之前未核准請求，Identity Manager 將自動拒絕該請求。
   - **上報核准** - 如果在指定的逾時期間之前未核准請求，Identity Manager 會自動將該請求上報至其他核准人。

     啓用此按鈕後，將顯示新的選項，因爲您必須指定 Identity Manager 將如何爲上報核准確定核准人。繼續進入第 322 頁的「配置 [確定上報核准人取得來源] 區段」，以取得說明。
   - **執行作業** - 如果核准請求在指定的逾時期間之前未經核准，Identity Manager 將自動執行替代作業。

     啓用此按鈕，並顯示 **[核准逾時作業]** 功能表後，您可以指定在核准請求逾時後要執行的作業。繼續進入第 324 頁的「配置 [核准逾時作業] 區段」，以取得說明。

配置 [確定上報核准人取得來源] 區段

在 **[逾時動作]** 區段 (第 321 頁) 中選取 **[上報核准]** 時，**[確定上報核准人取得來源]** 功能表即會出現 (圖 9-18)：

圖 9-18 確定上報核准人取得來源功能表

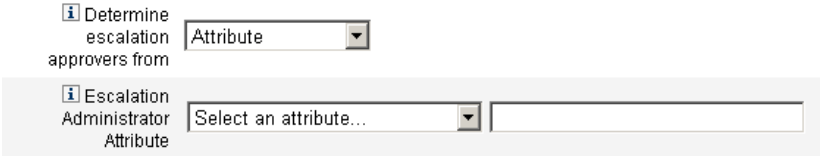
從此功能表中選取以下選項之一來指定如何爲上報核准確定核准人。

- **屬性** - 從新使用者檢視中所指定的屬性內確定核准人的帳號 ID。

備註 此屬性必須解析爲可表示單一帳號 ID 的字串或解析爲帳號 ID 的清單。

當 **[上報管理員屬性]** 功能表出現時 (圖 9-19)，請從清單中選取屬性。選取的屬性將顯示在旁邊的文字欄位中。

圖 9-19 上報管理員屬性功能表

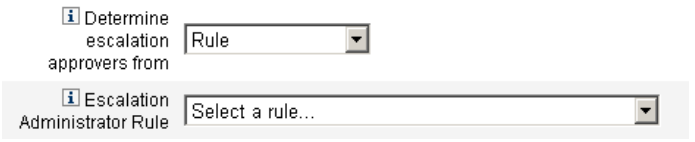


- **規則** - 透過評估指定的規則以確定核准人的帳號 ID。

  備註 計算之後，此規則必須傳回代表單一帳號 ID 的字串或其元素爲帳號 ID 的清單。

  當 **[上報管理員規則]** 功能表出現時 (圖 9-20)，請從清單中選取規則。

  圖 9-20 上報管理員規則功能表



- **查詢** - 透過查詢特定的資源以確定核准人的帳號 ID。

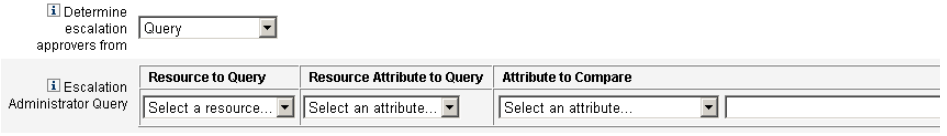
  當 **[上報管理員查詢]** 功能表出現時 (圖 9-21)，請依下列步驟建立查詢：

  a. 從 **[要查詢的資源]** 功能表中選取資源。

  b. 從 **[要查詢的資源屬性]** 功能表中選取屬性。

  c. 從 **[要比較的屬性]** 功能表中選取屬性。

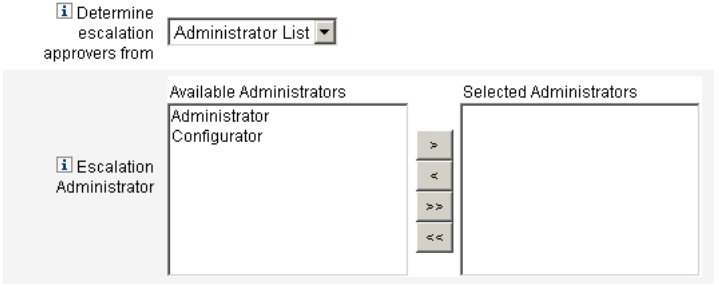
  圖 9-21 上報管理員查詢功能表



- **管理員清單** (預設值) - 從清單中明確選擇核准人。

  當 **[上報管理員]** 選取工具出現時 (圖 9-22)，請依下列步驟選取核准人：

  圖 9-22　　上報管理員選取工具



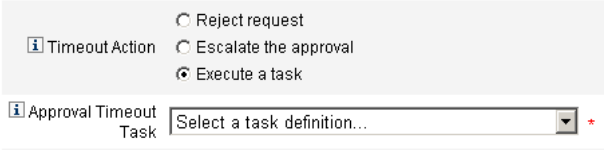
  a. 從 **[可用管理員]** 清單中，選取一個或多個管理員名稱。

  b. 將選取的名稱移至 **[選取的管理員]** 清單中。

配置 [核准逾時作業] 區段

在 **[逾時動作]** 區段中 (第 321 頁) 選取 **[執行作業]** 選項時，**[核准逾時作業]** 功能表即會出現 (圖 9-23)：

圖 9-23　　核准逾時作業功能表



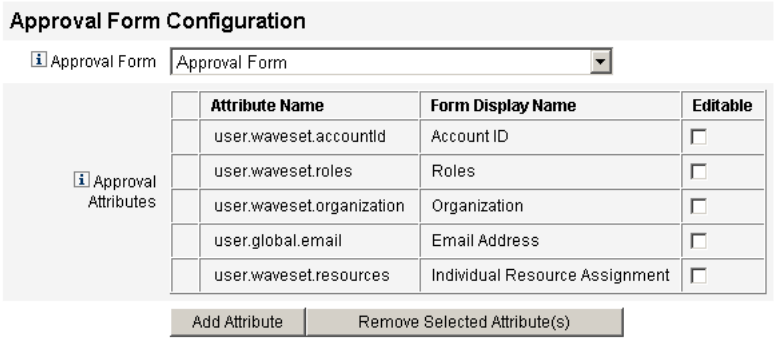
指定核准請求逾時後要執行的作業。例如，您可以允許請求者向管理員傳送說明請求或傳送報告。

配置核准表單 ([核准表單配置] 區段的 [核准] 標籤)

備註 [刪除使用者範本] 不包含 [核准表單配置] 區段。您僅可以爲 [建立使用者範本] 和 [更新使用者範本] 配置此區段。

您可以使用 [核准表單配置] 區段中的功能來選取核准表單，並將屬性增加到核准表單 (或從表單中移除屬性)。

圖 9-24 核准表單配置



依預設，[核准屬性] 表格包含以下標準屬性：

- `user.waveset.accountId`
- `user.waveset.roles`
- `user.waveset.organization`
- `user.global.email`
- `user.waveset.resources`

備註 預設核准表單配置爲可以顯示核准屬性。如果您使用的核准表單不是預設表單，則必須配置您的表單以顯示在 [核准屬性] 表格中指定的表單屬性。

若要配置其他核准人的核准表單，請執行以下步驟：

1. 從 **[核准表單]** 功能表中選取表單。

   核准人將使用此表單來核准或拒絕核准請求。

2. 啓用 **[核准屬性]** 表格的 **[可編輯]** 欄中的核取方塊，以使核准人可以編輯屬性值。

   例如，如果您啓用 `[user.waveset.accountId]` 核取方塊，則核准人可以變更使用者的帳號 ID。

備註 如果您修改了核准表單中任何帳號專用的屬性，則在實際佈建使用者時，也會置換所有相同名稱的全域屬性值。

例如，如果在系統中存在資源 `R1`，其具有 `description` 模式屬性，而您將 `user.accounts[R1].description` 屬性作爲可編輯的屬性增加到核准表單中，則任何對核准表單中 `description` 屬性值的變更均會置換僅從資源 `R1` 的 `global.description` 取得的值。

---

3. 按一下 **[增加屬性] 或 [移除選取的屬性]** 按鈕，從新使用者的帳號資料中指定要在核准表單中顯示的屬性。
   - 若要將屬性增加至表單，請參閱第 327 頁的 「增加屬性」。
   - 若要從表單移除屬性，請參閱第 328 頁的 「移除屬性」。

   備註 除非修改 XML 檔案，否則不能從核准表單中移除預設屬性。

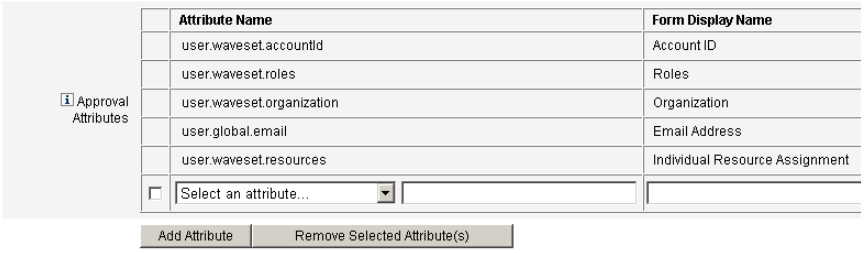
增加屬性

若要將屬性增加到核准表單，請執行以下步驟：

1. 按一下 [核准屬性] 表格下的 **[增加屬性]** 按鈕。

   在 [核准屬性] 表格中，**[屬性名稱]** 功能表將變爲可使用狀態，如下圖中所示：

   圖 9-25 增加核准屬性



2. 從功能表中選取屬性。

   選取的屬性名稱將顯示在旁邊的文字欄位中，同時該屬性的預設顯示名稱將顯示在 [表單顯示名稱] 欄中。

   例如，如果您選取 `user.waveset.organization` 屬性，則該表格將包含以下資訊：

   - 如有必要，您可以透過在相應的文字欄位中鍵入新名稱，來變更預設屬性名稱或預設表單顯示名稱。
   - 若要讓核准人可以變更屬性值，請啓用 **[可編輯]** 核取方塊。

     例如，核准人可能要置換資訊，如使用者的電子郵件地址。

3. 重複這些步驟以指定附加屬性。

移除屬性

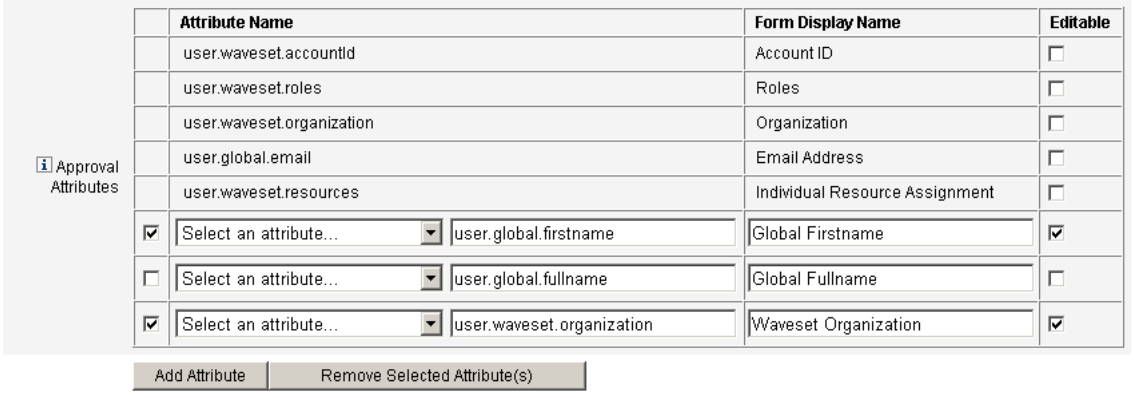
備註 除非修改 XML 檔案，否則不能從核准表單中移除預設屬性。

若要從核准表單移除屬性，請執行以下步驟：

1. 啓用 **[核准屬性]** 表格最左欄的一個或多個核取方塊。
2. 按一下 **[移除選取的屬性]** 按鈕，即可立即從 **[核准屬性]** 表格中移除選取的屬性。

   例如，當您按一下 **[移除選取的屬性]** 按鈕後，即會自下表中移除 `user.global.firstname` 及 `user.waveset.organization`。

圖 9-26 移除核准屬性

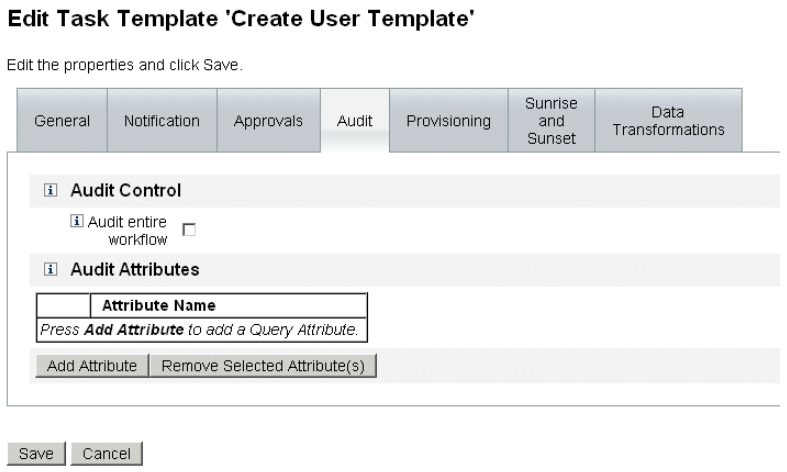


配置 [稽核] 標籤

本節提供配置 **[稽核]** 標籤的說明，此爲作業範本配置程序的一部份。如需如何啓動配置程序的說明，請參閱第 303 頁。

所有可配置的作業範本均支援配置工作流程稽核某些作業。尤其，您可以配置 [稽核] 標籤以控制是否稽核工作流程事件，並指定儲存哪些屬性以用於報告。

圖 9-27　稽核建立使用者範本



若要從使用者範本的 [稽核] 標籤配置稽核，請執行以下步驟：

1. 選取 **[稽核整個工作流程]** 核取方塊，以啓動工作流程稽核功能。如需有關工作流程稽核的資訊，請參閱第 343 頁的「透過工作流程建立稽核事件」。請注意，稽核工作流程會降低效能。
2. 按一下 **[增加屬性]** 按鈕 (位在 **[稽核屬性]** 區段中)，選取要稽核的屬性以執行報告。
3. 當 **[稽核屬性]** 表格中顯示 **[選取屬性...]** 功能表後，請從清單中選取屬性。

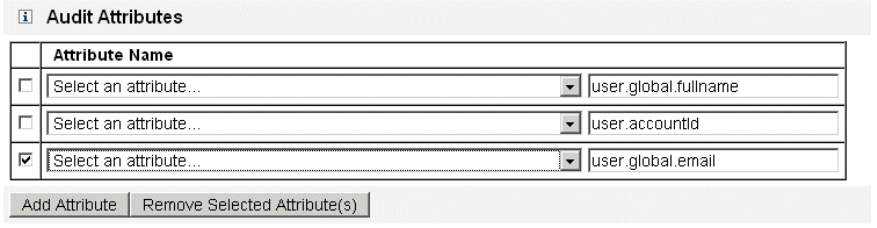
   選取的屬性名稱會顯示在相鄰的文字欄位中。

圖 9-28 增加屬性

若要從 [稽核屬性] 表中移除屬性，請執行以下步驟：

1. 啓用您想移除之屬性旁的核取方塊。

圖 9-29 移除 `user.global.email` 屬性



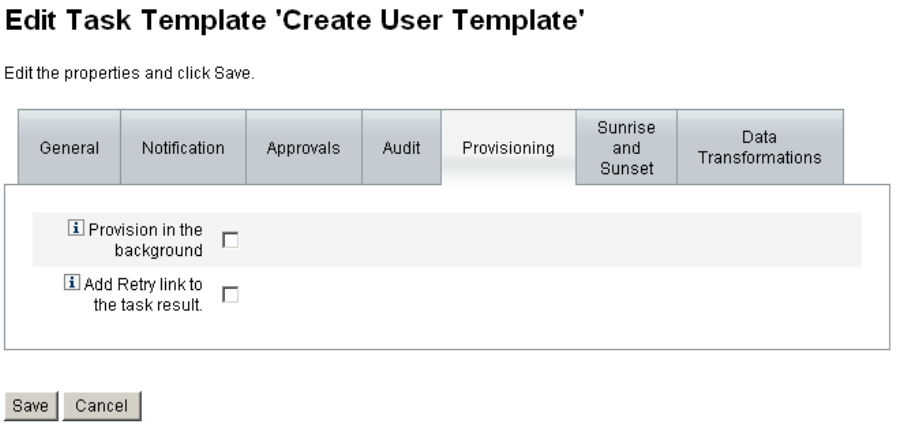
2. 按一下 **[移除選取的屬性]** 按鈕。

配置 [佈建] 標籤

本節提供配置 **[佈建]** 標籤的說明，此爲作業範本配置程序的一部份。如需如何啓動配置程序的說明，請參閱第 303 頁。

備註 此標籤僅對 [建立使用者範本] 和 [更新使用者範本] 可用。

圖 9-30 [佈建] 標籤：建立使用者範本



您可以使用 [佈建] 標籤來配置與佈建相關的以下選項：

- **在背景佈建** - 啓用此核取方塊可以在背景執行建立、刪除或更新作業，而非以同步方式執行作業。

  在背景中佈建可讓您在執行作業時繼續在 Identity Manager 中工作。

- **將「重試」連結增加至作業結果** - 若在執行作業時產生佈建錯誤，則啓用此核取方塊可以將 **[重試]** 連結增加至使用者介面。**[重試]** 連結可讓使用者在第一次嘗試失敗後再次嘗試執行該作業。

配置 [生效和失效] 標籤

本節提供配置 **[生效和失效]** 標籤的說明，此爲作業範本配置程序的一部份。如需如何啓動配置程序的說明，請參閱第 303 頁。

備註 僅有建立使用者作業範本提供此標籤。

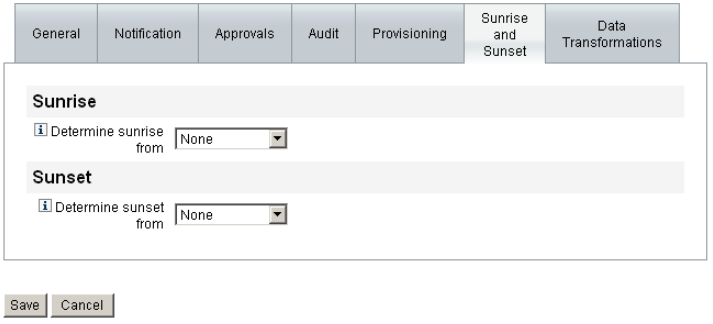
您可以使用 [生效和失效] 標籤，來選取確定以下動作之發生時間和日期的方法。

- 爲新使用者進行佈建 (**生效**)。
- 爲新使用者取消佈建 (**失效**)。

例如，您可以爲六個月後合同到期的臨時工指定失效日期。

圖 9-31 說明了 [生效和失效] 標籤上的設定。

圖 9-31 [生效和失效] 標籤：建立使用者範本



下面的主題提供了配置 [生效和失效] 標籤的說明。

配置生效

配置生效設定可指定將對新使用者進行佈建的時間和日期，以及指定將擁有生效工作項目的使用者。

若要讓配置生效，請執行以下步驟：

1. 從 **[確定生效取得來源]** 功能表選取以下選項之一，以指定 Identity Manager 將如何確定佈建的時間和日期。

   - **指定時間** - 將佈建延遲到指定的未來時間。繼續進入第 334 頁，以取得說明。
   - **指定日期** - 將佈建延遲到指定的未來行事曆日期。繼續進入第 334 頁，以取得說明。
   - **指定屬性** - 根據使用者檢視中的屬性值，將佈建延遲到指定的日期和時間。屬性必須包含日期/時間字串。指定屬性包含日期/時間字串後，您可以指定資料將遵循的日期格式。

     繼續進入第 335 頁，以取得說明。
   - **指定規則** - 根據規則延遲佈建，該規則在經過計算後會產生日期/時間字串。同指定屬性時一樣，您可以指定資料將遵循的日期格式。

     繼續進入第 336 頁，以取得說明。

備註 **[確定生效取得來源]** 功能表預設爲 **[無]** 選項，允許立即進行佈建。

2. 從 **[工作項目所有者]** 功能表選取使用者，以指定擁有生效工作項目的使用者。

備註 生效工作項目在 [核准] 標籤中可用。

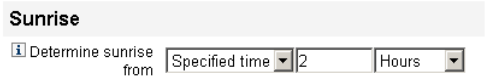
指定時間

若要將佈建延遲到指定的時間，請執行以下步驟：

1. 從 **[確定生效取得來源]** 功能表選取 **[指定的時間]**。
2. 當新的文字欄位和功能表顯示在 **[確定生效取得來源]** 功能表右側後，將空白的文字欄位中鍵入數字，並從該功能表選取時間單位。

   例如，如果您要在兩小時後佈建一個新使用者，則如下指定：

   圖 9-32 在兩個小時後佈建一個新使用者



指定日期

若要將佈建延遲到指定的行事曆日期，請執行以下步驟：

1. 從 **[確定生效取得來源]** 功能表選取 **[指定的天]**。
2. 使用顯示的功能表選項來指定在哪個月哪一週的哪一天進行佈建。

   例如，如果您要在九月的第二個星期一佈建新使用者，則如下指定：

   圖 9-33 透過日期佈建新使用者

指定屬性

若要根據使用者帳號資料中的屬性值，確定佈建的日期和時間，請執行以下步驟：

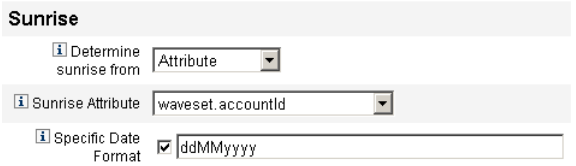
1. 從 **[確定生效取得來源]** 功能表中選取 **[屬性]**，以下選項將變爲可使用狀態：
   - **生效屬性** 功能表 - 提供目前爲與此範本所配置的作業相關聯之檢視而定義的屬性清單。
   - **指定的日期格式** 核取方塊和功能表 - 讓您可以指定屬性值的日期格式字串 (如有必要)。

備註	若未啓用 **[指定的日期格式]** 核取方塊，則日期字串必須遵循 `FormUtil` 方法 `convertDateToString` 可接受的格式。請參閱產品說明文件，以取得支援的日期格式的完整清單。

2. 從 **[生效屬性]** 功能表中選取屬性。
3. 如有必要，啓用 **[指定的日期格式]** 核取方塊，並在 **[指定的日期格式]** 欄位可使用後，輸入日期格式字串。

   例如，若要根據 `waveset.accountId` 屬性值，使用日、月和年格式佈建新使用者，請指定以下屬性：

圖 9-34 透過屬性佈建新使用者



指定規則

要計算指定的規則，以確定佈建的日期和時間，請執行以下步驟：

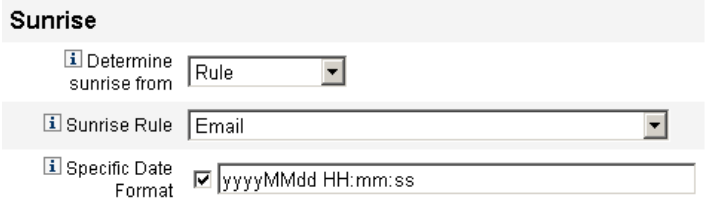
1. 從 **[確定生效取得來源]** 功能表中選取 **[規則]** ，以下選項將變爲可使用狀態：
   - **生效規則** 功能表 - 提供目前爲系統所定義之規則的清單。
   - **指定的日期格式** 核取方塊和功能表 - 讓您可以指定規則所傳回值的日期格式字串 (如有必要)。

備註 若未啓用 **[指定的日期格式]** 核取方塊，則日期字串必須遵循 `FormUtil` 方法 `convertDateToString` 可接受的格式。請參閱產品說明文件，以取得支援的日期格式的完整清單。

2. 從 **[生效規則]** 功能表中選取規則。
3. 如有必要，啓用 **[指定的日期格式]** 核取方塊，並在 **[指定的日期格式]** 欄位可使用後，輸入日期格式字串。

例如，若要根據電子郵箱規則，使用年、月、日、小時、分鐘和秒格式佈建新使用者，請指定以下屬性：

圖 9-35 透過規則佈建新使用者



配置失效

配置失效 (取消佈建) 的選項和程序與 「配置生效」小節提供的選項和程序相同。

唯一的不同是失效區段還提供了 **[失效作業]** 功能表，因爲您必須指定作業才能在指定日期和時間取消佈建使用者。

若要配置失效，請執行以下步驟：

1. 使用 **[確定失效取得來源]** 功能表指定用於確定進行取消佈建時間的方法：

備註 **[確定失效取得來源]** 功能表預設爲 **[無]** 選項，允許立即進行取消佈建。

   - **指定的時間** - 將取消佈建延遲到指定的未來時間。請檢閱第 334 頁的「指定時間」，以取得說明。
   - **指定的日期** - 將取消佈建延遲到指定的未來行事曆日期。請檢閱第 334 頁的「指定日期」，以取得說明。
   - **屬性** - 根據使用者帳號資料中的屬性值，將取消佈建延遲到指定的日期和時間。屬性必須包含日期/時間字串。指定屬性包含日期/時間字串後，您可以指定資料將遵循的日期格式。請檢閱第 335 頁的「指定屬性」，以取得說明。
   - **規則** - 根據規則延遲取消佈建，該規則經過計算後會產生日期/時間字串。同指定屬性時一樣，您可以指定資料將遵循的日期格式。

     請檢閱第 336 頁的「指定規則」，以取得說明。

2. 使用 **[失效作業]** 功能表指定作業，在指定的日期和 時間取消佈建使用者。

配置 [資料轉換] 標籤

本節提供配置 **[資料轉換]** 標籤的說明，此爲作業範本配置程序的一部份。如需如何啓動配置程序的說明，請參閱第 303 頁。

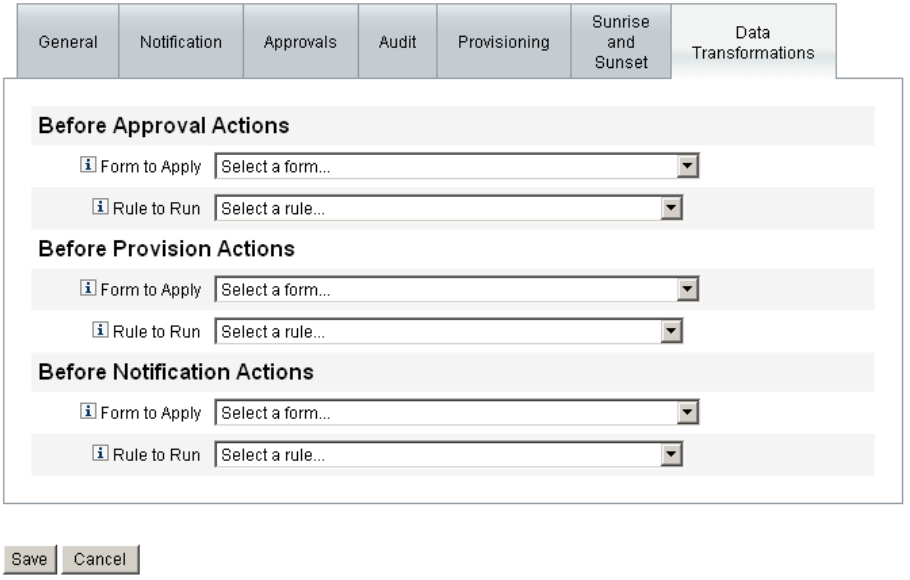
備註 此標籤僅對 [建立使用者範本] 和 [更新使用者範本] 可用。

如果您要在執行工作流程時變更使用者帳號資料，則可以使用 [資料轉換] 標籤指定在佈建期間 Identity Manager 如何變換資料。

例如，如果您希望表單或規則產生遵循公司策略的電子郵件地址，或者您要產生生效或失效日期。

選取 [資料轉換] 標籤後，將顯示以下頁面：

圖 9-36 [資料轉換] 標籤：建立使用者範本



此頁面包括以下區段：

- **核准前動作** - 如果您要在將核准請求傳送到指定的核准人之前變換使用者帳號資料，請配置此區段中的選項。
- **佈建前動作** - 如果您要在執行佈建動作之前變換使用者帳號資料，請配置此區段中的選項。
- **通知前動作** - 若要在將通知傳送到指定的收件者之前，變換使用者帳號資料，請配置此區段中的選項。

您可以在每個區段中配置以下選項：

- **要套用的表單**功能表 - 提供目前爲系統所配置之表單的清單。使用這些功能表可以指定表單，以用於從使用者帳號變換資料。
- **要執行的規則**功能表 - 提供目前爲系統所配置之規則的清單。使用這些功能表可以指定規則，以用於從使用者帳號變換資料。

第 10 章

稽核記錄

本章說明稽核系統記錄事件的方式。

本章分爲以下各節：

簡介

Identity Manager 稽核的目的，是記錄誰對哪些 Identity Manager 物件執行了什麼作業，以及執行的時間。

稽核事件透過一個或多個**發佈程式**處理。依預設，Identity Manager 使用儲存庫發佈程式將稽核事件記錄在儲存庫中。借助稽核群組，篩選可以允許管理員選取稽核事件子集進行記錄。您可爲每個發佈程式指定一個或多個最初已啓用的稽核群組。

備註 如需有關監視和管理使用者違規的資訊，請參閱第 13 章「身份識別稽核：基本概念」。

Identity Manager 稽核的內容為何？

大多數預設稽核都由內部 Identity Manager 元件執行。不過，有些介面可透過工作流程或透過 Java 程式碼產生事件。

預設 Identity Manager 稽核方法主要由四個主要區域執行：

- **佈建程式** - 稱爲佈建程式的內部元件可產生稽核事件。
- **檢視處理程式** - 在檢視架構中，檢視處理程式會產生稽核記錄。檢視處理程式應永遠在建立或修改物件時進行稽核。
- **階段作業** - 階段作業方法 (例如 `checkinObject`、`createObject`、`runTask`、`login` 和 `logout`) 會在完成可稽核作業後建立稽核記錄。該方法的大部分都將推入檢視處理程式中。
- **工作流程** - 依預設，僅核准工作流程會產生稽核記錄。當核准或拒絕請求時，它們會產生稽核事件。`com.waveset.session.WorkflowServices` 應用程式是工作流程功能與稽核記錄程式之間的介面。詳細資訊請參閱下一節。

透過工作流程建立稽核事件

依預設，只會將核准工作流程配置爲產生稽核記錄。本節說明如何使用 `com.waveset.session.WorkflowServices` 應用程式，以透過任何工作流程程序來產生額外的稽核事件。

若需要報告自訂工作流程，則可能需要額外的稽核事件。請參閱第 345 頁的「修改工作流程以記錄標準稽核事件」，以取得有關將稽核事件增加至工作流程的資訊。

您也可以將特殊的稽核事件增加至工作流程，以支援工作流程報告 (第 282 頁)。工作流程報告會報告爲完成工作流程所花的時間。需要有特殊的稽核事件，才能儲存計算時間所需的資料。請參閱第 348 頁的「修改工作流程以記錄計時稽核事件」，以取得有關將計時稽核事件增加至工作流程的資訊。

com.waveset.session.WorkflowServices 應用程式

com.waveset.session.WorkflowServices 應用程式可透過任何工作流程程序，產生稽核事件。表 10-1 說明適用於此應用程式的引數。

表 10-1 適用於 com.waveset.session.WorkflowServices 的引數

引數	類型	描述
op	字串	WorkflowServices 的作業。必須設為 audit 或 auditWorkflow。使用 audit 進行標準工作流程稽核。使用 auditWorkflow，儲存計算時間所需的計時稽核事件。必要。
type	字串	要稽核的物件類型名稱。表 B-5 (第 606 頁)會列出可稽核的物件類型。若要記錄標準稽核事件，則為必要項目。
action	字串	已執行之動作的名稱。表 B-6 (第 608 頁)會列出可稽核的動作。必要。
status	字串	指定動作的狀態名稱。表 B-7 (第 611 頁)的 [結果] 欄中會列出狀態。若要記錄標準稽核事件，則為必要項目。
name	字串	受指定動作影響的物件名稱。若要記錄標準稽核事件，則為必要項目。
資源	字串	(選擇性) 要變更物件所在之資源的名稱。
accountId	字串	(選擇性) 要修改的帳號 ID。 其應為本機資源帳號名稱。
error	字串	(選擇性) 發生任何失敗時，都會顯示已本土化的錯誤字串。
reason	字串	(選擇性) ReasonDenied 物件的名稱，會對映至說明一般失敗原因的國際化訊息。
屬性	對映	(選擇性) 已增加或已修改之屬性名稱和屬性值的對映。
參數	對映	(選擇性) 最多對映五個與一個事件相關的額外名稱或值。
組織	List	(選擇性) 要放置此事件的組織名稱或 ID 之清單。其用於設定稽核記錄的組織範圍。如果不存在，則處理程式將嘗試根據類型和名稱解析組織。如果無法解析組織，則會將事件放置在頂層 (組織階層的最高層級)。
originalAttributes	對映	(選擇性) 舊屬性值的對映。名稱應與屬性引數中列出的名稱相符。值將為您希望儲存在稽核記錄中之任何先前的值。

修改工作流程以記錄標準稽核事件

若要在工作流程中建立標準稽核事件，請在工作流程中增加下列 <Activity> 元素：

```
<Activity name='createEvent'>
```

接下來，在 <Activity> 元素中進行巢狀處理，加入一個參照 com.waveset.session.WorkflowServices 應用程式的<Action> 元素：

```
<Action class='com.waveset.session.WorkflowServices'>
```

在 <Action> 元素中進行巢狀處理，加入必要和選擇性 <Argument> 元素。請參閱表 10-1 (第 344 頁)，以取得引數清單。

若要記錄標準稽核事件，則 op 引數必須設爲 audit。

編碼樣例 10-1 顯示建立標準稽核事件所需最基本的程式碼。

範例

編碼樣例 10-1 說明了一個簡單工作流程作業。此範例顯示了事件產生過程，該事件將記錄由 ResourceAdministrator 執行之名爲 ADSIResource1 的資源刪除作業：

編碼樣例 10-1 簡單工作流程作業

```
<Activity name='createEvent'>
   <Action class='com.waveset.session.WorkflowServices'>
     <Argument name='op' value='audit'/>
     <Argument name='type' value='Resource'/>
     <Argument name='action' value='Delete'/>
     <Argument name='status' value='Success'/>
     <Argument name='subject' value='ResourceAdministrator'/>
     <Argument name='name' value='ADSIResource1'/>
   </Action>
   <Transition to='end'/>
</Activity>
```

編碼樣例 10-2 (第 346 頁) 顯示了如何將特定屬性增加至某個工作流程，該工作流程可追蹤每個使用者在核准程序中套用至顆粒性層級的變更。通常，此增加按照請求使用者輸入的 ManualAction 進行。

ACTUAL_APPROVER 是根據實際執行核准的人員，在表單和工作流程 (如果從核准表進行核准) 中設定的。APPROVER 可識別將其指定給誰。

編碼樣例 10-2 用於在核准程序中追蹤變更的已增加屬性 (第 1 頁，共 2 頁)

```
<Action name='Audit the Approval'
   application='com.waveset.session.WorkflowServices'>
     <Argument name='op' value='audit'/>
     <Argument name='type' value='User'/>
     <Argument name='name' value='$(CUSTOM_DESCRIPTION)'/>
     <Argument name='action' value='approve'/>
     <Argument name='accountId' value='$(accountId)'/>
     <Argument name='status' value='success'/>
     <Argument name='resource' value='$(RESOURCE_IF_APPLICABLE)'/>
     <Argument name='loginApplication' value='$(loginApplication)'/>
     <Argument name='attributes'>
       <map>
          <s>fullname</s><ref>user.accounts[Lighthouse].fullname</ref>
          <s>jobTitle</s><ref>user.accounts[Lighthouse].jobTitle</ref>
          <s>location</s><ref>user.accounts[Lighthouse].location</ref>
          <s>team</s><ref>user.waveset.organization</ref>
          <s>agency</s><ref>user.accounts[Lighthouse].agency</ref>
       </map>
    </Argument>
```

編碼樣例 10-2 用於在核准程序中追蹤變更的已增加屬性 (第 2 頁，共 2 頁)

```
    <Argument name='originalAttributes'>
      <map>
        <s>fullname</s>
        <s>User's previous fullname</s>
        <s>jobTitle</s>
        <s>User's previous job title</s>
        <s>location</s>
        <s>User's previous location</s>
        <s>team</s>
        <s>User's previous team</s>
        <s>agency</s>
        <s>User's previous agency</s>
      </map>
    </Argument>
    <Argument name='attributes'>
      <map>
         <s>firstname</s>

         <s>Joe</s>
         <s>lastname</s>
         <s>New</s>
      </map>
    </Argument>
    <Argument name='subject'>
      <or>
          <ref>ACTUAL_APPROVER</ref>
          <ref>APPROVER</ref>
      </or>
    </Argument>
    <Argument name='approver' value='$(APPROVER)'/>
</Action>
```

修改工作流程以記錄計時稽核事件

修改工作流程以記錄計時事件，以支援工作流程報告 (第 282 頁)。標準稽核事件只會記錄發生事件，而計時稽核事件則會記錄事件的開始和停止時間，因此可以進行時間的計算。除了計時事件資料之外，也會儲存標準稽核事件所記錄的大部分資訊。詳細資訊請參閱第 350 頁的 「計時稽核事件儲存的資訊爲何？」。

備註 爲了記錄計時稽核事件，您必須先啓動每個需稽核之工作流程類型的工作流程稽核。

- 若是您可以使用作業範本在管理員介面中配置的工作流程，則請先啓用與想要稽核之工作流程對應的作業範本。請參閱第 300 頁的 「啓用作業範本」，以取得說明。

  接著，選取 **[稽核整個工作流程]** 核取方塊，以開啓工作流程稽核。請參閱第 329 頁的 「配置 [稽核] 標籤」，以取得說明。

- 若是沒有作業範本的工作流程，請改爲定義名稱爲 `auditWorkflow` 的變數，並將其值設爲 `true`。

請注意，稽核工作流程會降低效能。

編碼樣例 10-3 顯示建立計時稽核事件所需的程式碼。若要記錄計時稽核事件，則 `op` 引數必須設爲 `auditWorkflow`。

`action` 也是必要引數，而且必須設爲下列其中一個值：

- StartWorkflow
- EndWorkflow
- StartProcess
- EndProcess
- StartActivity
- EndActivity

`auditconfig.xml` 中可能會定義額外的動作引數。

範例

編碼樣例 10-3 說明如何在工作流程中啓用計時稽核事件。若要配置工作流程，則應該在工作流程、程序和作業的開頭與結尾處，增加 auditWorkflow 事件。

auditWorkflow 作業定義於 com.waveset.session.WorkflowServices 中。詳細資訊請參閱第 344 頁。

編碼樣例 10-3 啓動工作流程中的計時稽核事件

```
<Action application='com.waveset.session.WorkflowServices'>
  <Argument name='op' value='auditWorkflow'/>
  <Argument name='action' value='StartWorkflow'/>
</Action>
```

若要停止記錄工作流程中的計時稽核事件，請將編碼樣例 10-4 中的程式碼增加至接近工作流程結束處的 pre-end 作業中。請注意，配置工作流程或程序時，並不允許您在 end 作業中放置任何項目。您必須建立 pre-end 作業，以執行最終的 auditWorkflow 事件，然後無條件地轉換爲 end 事件。

編碼樣例 10-4 停止工作流程中的計時稽核事件

```
<Action application='com.waveset.session.WorkflowServices'>
  <Argument name='op' value='auditWorkflow'/>
  <Argument name='action' value='EndWorkflow'/>
</Action>
```

計時稽核事件儲存的資訊為何？

計時稽核事件預設會記錄一般稽核事件所儲存的大部分資訊，包含下列屬性：

屬性	說明
WORKFLOW	正在執行之工作流程的名稱
PROCESS	正在執行之目前程序的名稱
INSTANCEID	正在執行之工作流程的唯一實例 ID
ACTIVITY	正在記錄之事件所在的作業
MATCH	工作流程實例內的唯一識別碼

上述屬性會儲存在 `logattr` 表格中，並且來自於 `auditableAttributesList`。Identity Manager 也會檢查是否已定義 `workflowAuditAttrConds` 屬性。

可能會在程序或工作流程的單一實例內呼叫多次某些作業。爲了符合特定活動實例的稽核事件，Identity Manager 會將唯一識別碼儲存在工作流程實例內的 `logattr` 表格中。

若要在 `logattr` 表格中儲存工作流程的額外屬性，則必須定義 `workflowAuditAttrConds` 清單，而此清單假設爲 `GenericObjects` 的清單。若在 `workflowAuditAttrConds` 清單內定義 `attrName` 屬性，則 Identity Manager 會提取程式碼內物件的 `attrName`，方法是先使用 `attrName` 作爲鍵值，然後儲存 `attrName` 值。所有鍵值和值都會儲存爲大寫值。

稽核配置

稽核配置由一個或多個發佈程式及數個預先定義的群組所組成。

稽核群組可以根據物件類型、動作和動作結果，定義所有稽核事件的子集。每個發佈程式都具有一個或多個指定的稽核群組。依預設，將儲存庫發佈程式指定給所有稽核群組。

稽核發佈程式可將稽核事件傳送至特定的稽核目標。預設的儲存庫發佈程式可將稽核記錄寫入儲存庫。每個稽核發佈程式均可具有實作特定選項。您可以爲稽核發佈程式指定文字格式化程式 (文字格式化程式可以文字說明稽核事件)。

稽核配置 (`#ID#Configuration:AuditConfiguration`) 物件在 `sample/auditconfig.xml` 檔案中定義。此配置物件具有一個延伸，該延伸是一個通用物件。其位於頂層，具有以下屬性：

- filterConfiguration
- extendedTypes
- extendedActions
- extendedResults
- publishers

filterConfiguration

filterConfiguration 屬性可列出**事件群組**，這些群組用於使一個或多個事件通過事件篩選器。filterConfiguration 屬性中列出的每個群組均包含表 10-2 中列出的屬性。

表 10-2 filterConfiguration 屬性

屬性	類型	描述
groupName	字串	事件群組名稱
displayName	字串	表示群組名稱的訊息目錄鍵值
enabled	字串	指示已啟用還是已停用整個群組的布林旗標。此屬性是篩選物件的最佳屬性。
enabledEvents	List	說明群組啟用哪些事件的通用物件清單。必須列出事件以啟用其記錄。列出的每個物件均必須具有以下屬性： • objectType (字串) - 命名物件類型。 • actions (清單) - 一個或多個動作的清單。 • results (清單) - 一個或多個結果的清單。

編碼樣例 10-5 說明了預設資源管理群組。

編碼樣例 10-5 預設資源管理群組

```
<Object name='Resource Management'>
  <Attribute name='enabled' value='true'/>
  <Attribute name='displayName'
             value='UI_RESOURCE_MGMT_GROUP_DISPLAYNAME'/>
  <Attribute name='enabledEvents'>
    <List>
      <Object>
        <Attribute name='objectType' value='Resource'/>
        <Attribute name='actions' value='ALL'/>
        <Attribute name='results' value='ALL'/>
      </Object>
      <Object>
        <Attribute name='objectType' value='ResourceObject'/>
        <Attribute name='actions' value='ALL'/>
        <Attribute name='results' value='ALL'/>
      </Object>
    </List>
  </Attribute>
</Object>
```

Identity Manager 提供下列預設稽核事件群組：

- 帳號管理
- 規範遵循管理
- 配置管理
- 事件管理
- 登入/登出
- 密碼管理
- 資源管理
- 角色管理
- 安全管理
- 作業管理
- Identity Manager 之外的變更
- Service Provider Edition

您可以從 Identity Manager 管理員介面的 [稽核配置] 頁面，配置每個群組 (**[配置] > [稽核]**)。請參閱第 185 頁的「配置稽核群組和稽核事件」。

[稽核配置] 頁面可讓您配置每個群組的成功或失敗事件。此介面不支援增加或修改群組的已啓用事件，但是您可以使用 Identity Manager 除錯頁面來執行這些作業 (第 59 頁)。

預設事件群組及其啓用的事件在以下各節中說明。

帳號管理

依預設啓用此群組。

表 10-3 預設帳號管理事件群組

類型	動作
加密金鑰	所有動作
Identity 系統帳號	所有動作
資源帳號	核准、變更密碼、建立、刪除、停用、啟用、修改、拒絕、重新命名、重設密碼、解除鎖定
工作流程情況	結束作業、結束程序、結束工作流程、啟動作業、啟動程序、啟動工作流程
使用者	核准、建立、憑證過期、刪除、停用、啟用、鎖定、登入、登出、修改、拒絕、重新命名、解除鎖定、使用者名稱回復

Identity Manager 之外的變更

依預設停用此群組。

表 10-4 Identity Manager 之外的變更事件群組和事件

類型	動作
ResourceAccount	本機變更

規範遵循管理

依預設啓用此群組。

表 10-5 預設規範遵循管理群組事件

類型	動作
AuditPolicy	所有動作
AccessScan	所有動作
ComplianceViolation	所有動作
Data Exporter	所有動作
UserEntitlement	核准的驗證者、拒絕的驗證者、請求的修正、已請求重新掃描、終止
Access Review Workflow	所有動作
Remediation Workflow	所有動作

配置管理

依預設啓用此群組。

表 10-6 預設配置管理事件群組

類型	動作
配置	所有動作
UserForm	所有動作
Rule	所有動作
EmailTemplate	所有動作
LoginConfig	所有動作
Policy	所有動作
XmlData	Import
Log	所有動作

事件管理

依預設啓用此群組。

表 10-7　預設事件管理事件群組

類型	動作
Email	Notify
TestNotification	Notify

登入/登出

依預設啓用此群組。

表 10-8　預設 Identity Manager 登入/登出事件群組

類型	動作
使用者	憑證過期、鎖定、登入、登出、解除鎖定、使用者名稱回復

密碼管理

依預設啓用此群組。

表 10-9　預設密碼管理事件群組和事件

類型	動作
資源帳號	變更密碼、重設密碼

資源管理

依預設啓用此群組。

表 10-10　預設資源管理事件群組和事件

類型	動作
資源	所有動作
資源物件	所有動作
ResourceForm	所有動作
ResourceAction	所有動作
AttrParse	所有動作
工作流程情況	結束作業、結束程序、結束工作流程、啟動作業、啟動程序、啟動工作流程

角色管理

依預設停用此群組。

表 10-11　預設角色管理事件群組和事件

類型	動作
角色	所有動作

安全管理

依預設啓用此群組。

表 10-12　預設安全管理事件群組和事件

類型	動作
權能	所有動作
EncryptionKey	所有動作
Organization	所有動作
Admin Role	所有動作

Service Provider Edition

依預設啓用此群組。

表 10-13 服務提供者事件群組和事件

類型	動作
Directory User	詰問回應、建立、刪除、修改、作業後圖說文字、作業前圖說文字、更新認證答案、使用者名稱回復

作業管理

依預設停用此群組。

表 10-14 作業管理事件群組和事件

類型	動作
TaskInstance	所有動作
TaskDefinition	所有動作
TaskSchedule	所有動作
TaskResult	所有動作
ProvisioningTask	所有動作

extendedTypes

每個您增加至 com.waveset.object.Type 類別的新類型都可以進行稽核。必須爲新類型指定唯一的雙字元資料庫鍵值，其將儲存在資料庫中。所有新類型均將增加至不同的稽核報告介面。必須將每個不經篩選就記錄至資料庫的新類型增加至稽核事件群組 enabledEvents 屬性中 (如 enabledEvents 屬性的說明)。

在某些情況下，您可能會想要稽核沒有相關之 com.waveset.object.Type 的物件，或者想要更詳細地表示現有類型。

例如，WSUser 物件會將使用者的所有帳號資訊儲存在儲存庫中。稽核程序將 WSUser 物件分割爲兩個不同的稽核類型 (資源帳號和 Identity Manager 帳號)，而不是將每個事件標記爲 USER 類型。以此方法分割物件可讓您更輕鬆地在稽核記錄中尋找特定帳號資訊。

透過增加至 extendedObjects 屬性來增加延伸式稽核類型。每個延伸式物件均必須具有下表中列出的屬性：

表 10-15 延伸式物件屬性

引數	類型	描述
name	字串	類型名稱，在建構稽核事件時和篩選事件期間使用。
displayName	字串	表示類型名稱的訊息目錄鍵值。
logDbKey	字串	在記錄表中儲存此物件時要使用的雙字元資料庫鍵值。請參閱第 606 頁的「稽核記錄資料庫對映」以取得保留值。
supportedActions	List	物件類型支援的動作。從使用者介面建立稽核查詢時將使用此屬性。如果該值為空值，則所有動作均會顯示為要針對此物件類型查詢的可能值。
mapsToType	字串	(選擇性) 對映至此類型的 com.waveset.object.Type 名稱 (如果有)。嘗試解析物件組織成員身份 (如果尚未在事件上指定) 時會使用此屬性。
organizationalMembership	List	(選擇性) 應放置此類型事件 (如果它們尚未具有指定的組織成員身份) 之組織 ID 的預設清單。

所有用戶特定鍵值均應以 # 符號開頭，以防止增加新的內部鍵值後出現重複的鍵值。

編碼樣例 10-6 說明了延伸式類型 Identity Manager 帳號。

編碼樣例 10-6 延伸式類型 Identity Manager 帳號

```
<Object name='LighthouseAccount'>
   <Attribute name='displayName' value='LG_LIGHTHOUSE_ACCOUNT'/>
   <Attribute name='logDbKey' value='LA'/>
   <Attribute name='mapsToType' value='User'/>
   <Attribute name='supportedActions'>
      <List>
         <String>password</String>
         <String>Enable</String>
         <String>Create</String>
         <String>Modify</String>
         <String>Delete</String>
         <String>Rename</String>
      </List>
   </Attribute>
</Object>
```

extendedActions

稽核動作通常對映至 com.waveset.security.Right 物件。增加新的 Right 物件時，您必須指定唯一的雙字元 logDbKey，其將儲存在資料庫中。您可能遇到這種情況，即無權與必須稽核之特定動作對應。您可以透過將動作增加至 extendedActions 屬性中的物件清單中來延伸動作。

每個 extendedActions 物件均必須包含表 10-16 中列出的屬性。

表 10-16 extendedAction 屬性

屬性	類型	描述
name	字串	動作名稱，在建構稽核事件時和篩選事件期間使用。
displayName	字串	表示動作名稱的訊息目錄鍵值。
logDbKey	字串	在記錄表中儲存此動作時要使用的雙字元資料庫鍵值。 請參閱第 606 頁的 「稽核記錄資料庫對映」以取得保留值。

所有用戶特定鍵值均應以 # 符號開頭，以防止增加新的內部鍵值後出現重複的鍵值。

編碼樣例 10-7 說明了如何增加登出動作。

編碼樣例 10-7 增加登出的動作

```
<Object name='Logout'>
  <Attribute name='displayName' value='LG_LOGOUT'/>
  <Attribute name='logDbKey' value='LO'/>
</Object>
```

extendedResults

除了延伸稽核類型和動作之外，您還可以增加結果。依預設，有兩種結果：成功和失敗。您可以透過將結果增加至 extendedResults 屬性中的物件清單中來延伸結果。

每個 extendedResults 物件均必須包含表 10-17 中說明的屬性。

表 10-17 extendedResults 屬性

屬性	類型	描述
name	字串	結果名稱，在設定稽核事件的狀態時和篩選事件期間使用。
displayName	字串	表示結果名稱的訊息目錄鍵值。
logDbKey	字串	在記錄表中儲存此結果時要使用的單字元資料庫鍵值。請參閱標題為資料庫鍵值的小節，以取得保留值。

所有用戶特定鍵值均應使用 0 到 9 之間的數字，以防止增加新的內部鍵值後出現重複的鍵值。

publishers

發佈程式清單中的每個項目均爲通用物件。每個發佈程式均具有以下屬性：

表 10-18 發佈程式屬性

屬性	類型	描述
class	字串	發佈程式類別的名稱。
displayName	字串	表示發佈程式名稱的訊息目錄鍵值。
description	字串	對發佈程式的說明。
filters	List	指定給此發佈程式的稽核群組清單。
formatter	字串	文字格式化程式的名稱 (如果有)。
options	List	發佈程式選項清單。這些選項是發佈程式特有的選項，而清單中的每個項目都是 PublisherOption 的對映表示。請參閱 sample/auditconfig.xml 以取得範例。

資料庫模式

Identity Manager 儲存庫中有兩個用以儲存稽核資料的表格：

- `waveset.log` - 儲存大部分事件的詳細資訊。
- `waveset.logattr` - 儲存每個事件所屬組織的 ID。

本節會先討論這些表格。

當稽核記錄資料超出上述表格中指定的欄長度限制時，Identity Manager 會截斷資料以放入欄中。第 366 頁會討論稽核記錄截斷。

稽核記錄中的一些欄具有可配置的欄長度限制。若要瞭解這些欄並學習如何變更其長度限制，請參閱第 367 頁的「稽核記錄配置」。

waveset.log

本小節列出了 `waveset.log` 表中的各欄名稱和資料類型。資料類型是根據 Oracle 資料庫定義取得的，並會因資料庫的不同而稍有不同。如需所有受支援資料庫的資料模式值清單，請參閱附錄 B「稽核記錄資料庫模式」。

爲節省空間，一些欄值在資料庫中儲存爲鍵值。如需鍵值定義，請參閱標題爲第 606 頁的「稽核記錄資料庫對映」的小節。

- `objectType` **CHAR(2)** - 表示要稽核之物件類型的雙字元鍵值。
- `action` **CHAR(2)** - 表示已執行之動作的雙字元鍵值。
- `actionStatus` **CHAR(1)** - 表示已執行動作之結果的單字元鍵值。
- `reason` **CHAR(2)** - 用於在發生故障時說明 `ReasonDenied` 物件的雙字元資料庫鍵值。`ReasonDenied` 是包含訊息目錄項目的類別，用於一般失敗 (例如憑證無效和權限不足)。
- `actionDateTime` **VARCHAR(21)** - 上述動作發生的日期和時間。該值以 GMT 時間儲存。
- `objectName` **VARCHAR(128)** - 作業期間已對其執行動作的物件名稱。
- `resourceName` **VARCHAR(128)** - 作業期間使用的資源名稱 (如果適用)。某些事件不參照資源；但是，在許多情況下，其都提供更多詳細資訊以記錄執行作業的資源。

- accountName **VARCHAR(255)** - 已對其執行動作的帳號 ID (如果適用)。
- server **VARCHAR(128)** - 已在其中執行動作的伺服器 (由事件記錄程式自動指定)。
- message **VARCHAR(255*) 或 CLOB** - 任何與動作相關聯的本土化訊息，包含錯誤訊息之類的訊息。文字將儲存爲已本土化的文字，因此其不會國際化。您可以配置此欄的欄長度限制。預設資料類型是 VARCHAR，而預設大小限制爲 255。請參閱第 367 頁的「稽核記錄配置」，以取得有關如何調整大小限制的資訊。
- interface **VARCHAR(50)** - 執行作業時透過的 Identity Manager 介面 (例如管理員、使用者、IVR 或 SOAP 介面)。
- acctAttrChanges **VARCHAR(4000)** - 儲存已在建立和更新期間變更的帳號屬性。永遠在資源帳號或 Identity Manager 帳號物件的建立或更新期間填寫屬性變更欄位。在動作期間變更的所有屬性均作爲字串儲存在此欄位中。資料的格式爲 NAME=VALUE NAME2=VALUE2。可透過對名稱或值執行 contains SQL 陳述式來查詢此欄位。

  編碼樣例 10-8 說明了 acctAttrChanges 欄中的值：

  編碼樣例 10-8 acctAttrChanges 欄中的值

```
COMPANY="COMPANY" DEPARTMENT="DEPT" DESCRIPTION="DSMITH
DESCRIPTION" FAX NUMBER="5122222222" HOME ADDRESS="12282
MOCKINGBIRD LANE" HOME CITY="AUSTIN" HOME PHONE="5122495555"
HOME STATE="TX" HOME ZIP="78729" JOB TITLE="DEVELOPER"
MOBILE PHONE="5125551212" WORK PHONE="5126855555"
EMAIL="someone@somecompany.COM" EXPIREPASSWORD="TRUE"
FIRSTNAME="DANIEL" FULLNAME="DANIEL SMITH" LASTNAME="SMITH"
```

- acctAttr01label-acctAttr05label **VARCHAR(50)** - 這五個額外的 NAME 槽是五個欄，最多可以升級五個要儲存在其各自欄中，而非儲存在大的二進位大型物件中的屬性名稱。您可以使用「稽核？」設定，從 [資源模式配置] 頁面升級屬性，這樣該屬性將適用於資料堪查。
- acctAttr01value-acctAttr05value **VARCHAR(128)** - 五個額外的 VALUE 槽，最多可以升級五個要儲存在不同欄中，而非儲存在二進位大型物件欄中的屬性值。
- parm01label-parm05label **VARCHAR(50)** - 五個用於儲存與事件相關聯之參數的槽。其範例爲用戶端 IP 和階段作業 ID 名稱。

- parm01value-parm05value **VARCHAR(128*) 或 CLOB** - 五個用於儲存與事件相關聯之參數的槽。其範例爲用戶端 IP 和階段作業 ID 值。您可以配置這些欄的欄長度限制。預設資料類型是 VARCHAR，而預設大小限制爲 128。請參閱第 367 頁的「稽核記錄配置」，以取得有關如何調整大小限制的資訊。
- id **VARCHAR(50)** - 透過 waveset.logattr 表格中所參照的儲存庫，指定給每個記錄的唯一 ID。
- name **VARCHAR(128)** - 指定給每個記錄的已產生名稱。
- xml**BLOB** - 供 Identity Manager 內部使用。

waveset.logattr

waveset.logattr 表用於儲存每個事件的組織成員身份 ID，這可以依組織設定稽核記錄範圍。

- id **VARCHAR(50)** - waveset.log 記錄的 ID。
- attrname **VARCHAR(50)** - 目前一律爲 MEMBEROBJECTGROUPS。
- attrval **VARCHAR(255)** - 事件所屬之 MemberObject 群組的 ID。

稽核記錄截斷

當稽核記錄資料的一個或多個欄超出指定的欄長度限制時，會截斷欄資料以放入欄中。明確地說，資料會截斷爲符合指定的限制 (欄長度減去三個字元)。省略符號 (...) 會附加至欄資料，表示發生截斷。

此外，該稽核記錄之 NAME 欄的前方會加上字串 #TRUNCATED# ，以利查詢截斷的記錄。

備註 Identity Manager 計算在何處截斷訊息時，採用的是 UTF8 編碼。若配置所使用的編碼不是 UTF8，則截斷的資料還是可能仍然會超出資料庫中實際的欄大小。若發生此情況，則截斷的訊息不會顯示在稽核記錄中，而是在系統記錄檔中寫入錯誤。

稽核記錄配置

稽核記錄中的特定欄可以配置爲儲存儲存庫中的大量資料。

調整欄長度限制

稽核記錄中的數個欄具有可配置的欄長度限制。這些欄如下：

- message 欄
- parmNNvalue 欄 (其中 NN = 01、02、03、04 或 05)
- xml 欄

備註 如需稽核記錄欄說明，請參閱第 364 頁的 「資料庫模式」。

您可以編輯 RepositoryConfiguration 物件，變更欄長度限制。如需有關編輯 RepositoryConfiguration 物件的說明，請參閱第 197 頁的 「編輯 Identity Manager 配置物件」。

- 若要變更 message 欄的欄長度限制，請修改 maxLogMessageLength 值。
- 若要變更 parmNNvalue 欄的欄長度限制，請修改 maxLogParmValueLength 值。相同的限制值會套用至這五個欄 (您無法定義個別的欄長度值)。
- 若要變更 xml 欄的欄長度限制，請修改 maxLogXmlLength 值。

需要重新啓動伺服器，新值才會生效。

RepositoryConfiguration 物件中的欄長度限制設定，可決定欄中可以儲存的最大資料量。若要儲存的資料超出這些設定，則 Identity Manager 會截斷資料。詳細資訊請參閱第 366 頁的 「稽核記錄截斷」。

若增加 RepositoryConfiguration 物件中的欄長度設定，則也請確認資料庫中的欄大小設定至少與 RepositoryConfiguration 物件中所配置的大小相同。

移除稽核記錄中的記錄

稽核記錄應該定期進行截斷，以避免擴充得太大。使用 [稽核記錄維護作業] 可以移除稽核記錄中的舊記錄。

若要排程作業以移除稽核記錄中的舊記錄，請執行以下步驟：

1. 在管理員介面中，按一下 **[伺服器作業] > [管理排程]**。
2. 在 [可用於排程的作業] 區段中，按一下 **[稽核記錄維護作業]**。

   [建立新的稽核記錄維護作業作業排程] 頁面會隨即開啓。
3. 填寫表單並按一下 **[儲存]**。

防止稽核記錄竄改

您可以配置 Identity Manager 以防止以下形式的稽核記錄竄改：

- 增加或插入稽核記錄檔記錄
- 修改現有稽核記錄中的記錄
- 刪除稽核記錄檔記錄或整個稽核記錄檔
- 截斷稽核記錄檔

所有 Identity Manager 稽核記錄中的記錄均具有唯一的、視伺服器而定的序號以及記錄和序號的加密雜湊。當您建立竄改偵測報告時，它會對每個伺服器的稽核記錄掃描以下各項：

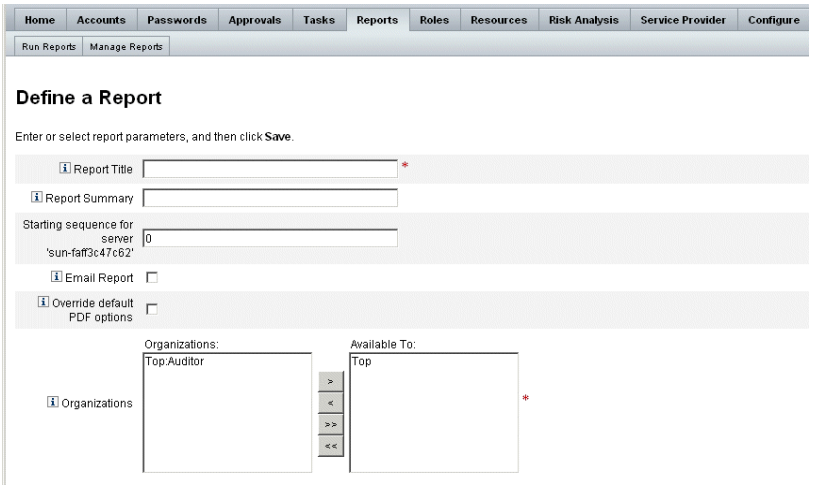
- 序號中的間隔 (表示已刪除某記錄)
- 雜湊不相符 (表示已修改某記錄)
- 重複的序號 (表示已複製某記錄)
- 小於預期序號的最後一個序號 (表示已截斷某記錄)

配置防竄改記錄

若要配置防竄改記錄，請執行以下步驟：

1. 選取 **[報告] > [新增] > [稽核記錄竄改報告]**，以建立竄改報告。
2. 當顯示 [定義竄改報告] 頁面 (請參閱圖 10-1) 時，爲報告輸入標題，然後 **[儲存]** 該報告。

圖 10-1 配置稽核記錄竄改報告

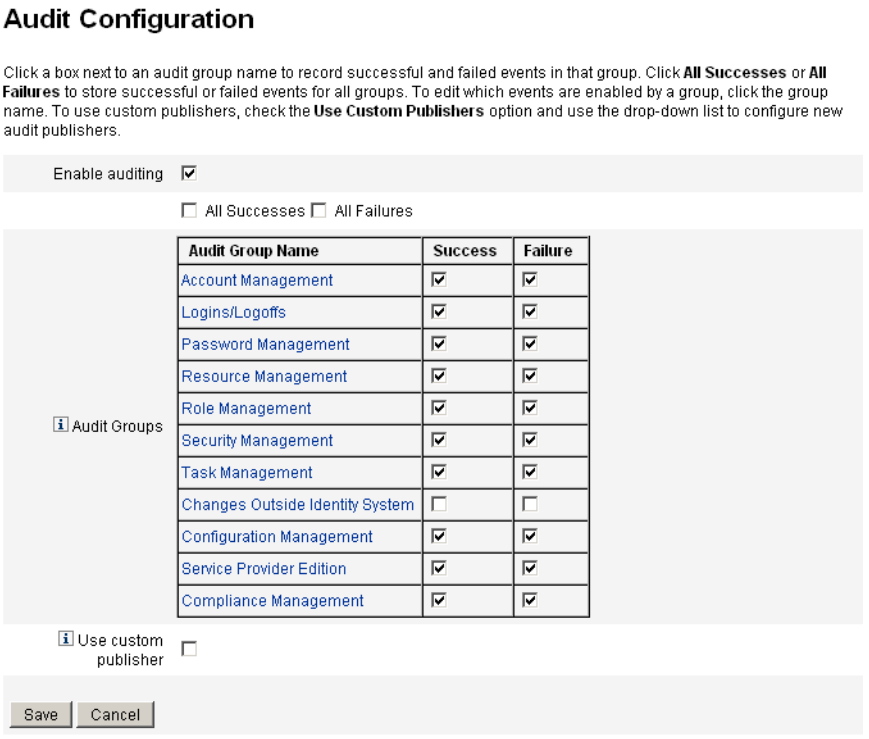


您也可以指定以下可選參數：

- **報告摘要** - 輸入報告的說明性摘要。
- **伺服器「<*server_name*>」的起始序列** - 輸入伺服器的起始序號。
- 此選項可讓您刪除舊的記錄項目而無需將其標記爲竄改，並可以限制報告範圍以提高效能。
- **電子郵件報告** - 可將報告結果透過電子郵件傳送至指定的電子郵件地址。
- 選取此選項時，頁面會重新整理並提示您輸入電子郵件地址。但是請記住，透過電子郵件傳送文字內容是不安全的 - 這樣可能會洩漏機密資訊 (例如帳號 ID 或帳號歷程記錄)。
- **置換預設 PDF 選項** - 選取此選項可置換此報告的預設 PDF 選項。
- **組織** - 選取應具有此報告之存取權的組織。

3. 接下來選取 **[配置] > [稽核]**，以開啓 [稽核配置] 頁面 (如圖 10-2 所示)。

圖 10-2　防竄改稽核記錄配置



4. 選取 **[使用自訂發佈程式]**，然後按一下 [儲存庫發佈程式] 連結。
5. 選取 **[啓用防篡改稽核記錄]**，然後按一下 **[確定]**。
6. 按一下 **[儲存]** 儲存設定。

   您可以再次關閉此選項，但是未簽署的項目本身將在稽核記錄竄改報告中進行標記，您必須重新配置報告才能忽略這些項目。

使用自訂稽核發佈程式

Identity Manager 可以將稽核事件提交給自訂稽核發佈程式。下列是提供的自訂發佈程式：

- 主控台 - 將稽核事件列印至標準輸出或標準錯誤。
- 檔案 - 將稽核事件寫入平面檔案。
- JDBC - 將稽核事件記錄在 JDBC 資料存放區中。
- JMS - 將稽核事件記錄在 JMS 佇列或主題中。
- JMX - 發佈稽核事件，讓 JMX (Java 管理延伸) 用戶端可以監視 Identity Manager 稽核記錄作業。
- 執行程序檔 - 允許執行自訂程序檔以儲存稽核事件。

若想要建立自己的發佈程式，請參閱第 381 頁的 「開發自訂稽核發佈程式」。

啟用自訂稽核發佈程式

自訂稽核發佈程式可由 [稽核配置] 頁面啓用。

若要啓用自訂稽核發佈程式，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[配置]**，然後按一下輔助功能表的 **[稽核]**。

   [稽核配置] 頁面會隨即開啓。

2. 選取頁面底端的 **[使用自訂發佈程式]** 選項。

   表格會隨即開啓，並會列出目前配置的稽核發佈程式。

3. 若要配置新的稽核發佈程式，請從 **[新增發佈程式]** 下拉式功能表中，選取自訂發佈程式類型。

   完成 [配置新的稽核發佈程式] 表單。按一下 **[確定]**。

4. 重要事項！ 按一下 **[儲存]** 以儲存新的稽核發佈程式！

主控台、檔案、JDBC 和執行程序檔的發佈程式類型

若要啓用 [主控台]、[檔案]、[JDBC] 和 [已執行程序檔] 稽核發佈程式，請執行第 372 頁的「啓用自訂稽核發佈程式」中的步驟。從 **[新增發佈程式]** 下拉式功能表中選取適當的發佈程式類型。

完成 [配置新的稽核發佈程式] 表單。若對表單有任何問題，請參閱 i-Helps 及線上說明。

- [主控台] 稽核發佈程式會將稽核事件列示至標準輸出或標準錯誤。
- [檔案] 稽核發佈程式會將稽核事件寫入平面檔案。
- [JDBC] 稽核發佈程式會將稽核事件記錄在 JDBC 資料存放區中。
- [已執行程序檔] 稽核發佈程式允許使用 JavaScript 或 BeanShell 撰寫的自訂程序檔，儲存稽核事件。

JMS 發佈程式類型

JMS 稽核記錄自訂發佈程式可以將稽核事件記錄發佈至 JMS (Java Message Service) 佇列或主題。

為何要使用 JMS？

發佈至 JMS 可爲具有多部 Identity Manager 伺服器的環境，提供更多相互關聯作業的彈性。此外，在限制使用 [檔案] 稽核記錄發佈程式的情況下，可以使用 JMS (例如，用戶端報告工具在伺服器執行時就無法存取記錄的 Windows 環境中)。

JMS 提供在多部伺服器環境下的多項優點：

- JMS 訊息儲存區可集中 (和簡化) 訊息的儲存與擷取。
- JMS 架構不會限制可以存取服務的用戶端數目。
- JMS 協定可以輕易透過防火牆和其他網路基礎架構傳送。

點對點或發佈與訂閱？

Java 訊息系統提供兩種訊息傳送模型：點對點或**佇列**模型，以及發佈及訂閱或**主題**模型。Identity Manager 支援這兩種模型。

在點對點模型中，**生產者**會將訊息發佈至特定佇列，而**用戶**會從該佇列讀取訊息。在此處，生產者知道訊息的目標，並會將訊息直接發佈至用戶的佇列。

點對點模型的特性如下：

- 只有一個用戶會收到訊息。
- 收件者使用訊息時，生產者不需要處於執行狀態；傳送訊息時，收件者也不需要處於執行狀態。
- 收件者會確認每則成功處理的訊息。

反之，發佈與訂閱模型則支援將訊息發佈至特定訊息**主題**。零或多位訂閱者可能會希望收到與特定訊息主題相關的訊息。在此模型中，發佈者與訂閱者彼此並不認識。此模型的最佳比喻方式就是匿名佈告欄。

發佈與訂閱模型的特性如下：

- 多位用戶可接收訊息。
- 發佈者與訂閱者之間存在時間相依性。發佈者必須先建立訂閱，用戶端才可進行訂閱。訂閱之後，除非已建立長期訂閱，否則訂閱者必須持續保持在使用中狀態才會收到訊息。若是長期訂閱，則會在訂閱者重新連線時，重新發行在訂閱者未連線時所發佈的訊息。

備註 如需有關 JMS 的更多資訊，請參閱 http://www.sun.com/software/products/message_queue/index.xml

配置 JMS 發佈程式類型

JMS 發佈程式會將稽核事件格式化爲 JMS TextMessage。這些 TextMessage 接著會視配置之不同，而傳送至佇列或主題。文字訊息可視配置之不同，而格式化爲 XML 或 ULF (通用記錄格式)。

若要啓用 JMS 發佈程式類型，請執行第 372 頁的「啓用自訂稽核發佈程式」中的步驟，然後從 **[新增發佈程式]** 下拉式功能表中選取 **[JMS]**。

若要配置 JMS 發佈程式類型，請完成 [配置新的稽核發佈程式] 表單。若對表單有任何問題，請參閱 i-Helps 及線上說明。

JMX 發佈程式類型

JMX 稽核記錄發佈程式會發佈稽核事件，讓 JMX (Java 管理延伸) 用戶端可以監視 Identity Manager 稽核記錄作業。

何謂 JMX？

Java 管理延伸 (JMX) 是一項 Java 技術，可讓您管理及 (或) 監視應用程式、系統物件、裝置及服務導向的網路。受管理/監視的實體以稱之爲 MBean 的物件表示 (意即「管理式 Bean」)。

Identity Manager 的 JMX 發佈程式實作

Identity Manager 的 JMX 稽核記錄發佈程式會監視事件的稽核記錄。偵測到事件時，JMX 發佈程式會使用 MBean 包裝稽核事件記錄，而且會更新保留在記憶體中的臨時歷程記錄。每發生一次事件，都會傳送給 JMX 用戶端一則小型通知。若是感興趣的事件，則 JMX 用戶端可以查詢包裝稽核事件的 MBean，以取得額外資訊。

備註 請參閱 `com.waveset.object.AuditEvent` Javadoc，以取得有關稽核事件記錄的資訊。您可以在 REF 工具組中取得此 Javadoc，而此工具組會於第 381 頁的「開發自訂稽核發佈程式」中討論。

若要從正確的 MBean 中擷取資訊，則需要歷程記錄序號。事件通知中會包含此號碼。

每則事件通知都會包含下列資訊：

- 類型 - 說明事件類型的字串。字串的格式爲 `AuditEvent.<ObjectType>.<Action>`，其中 `ObjectType` 和 `Action` 會從 `com.waveset.AuditEvent` 傳回。例如，若送出解除鎖定事件，則類型會是 `AuditEvent.LighthouseAccount.Unlock`。
- SequenceNumber - 用以查詢 MBean 中資訊的歷程記錄緩衝區鍵值。

配置 JMX 發佈程式類型

若要配置 JMX 發佈程式類型，請執行以下步驟：

1. 若要啓用 JMX 發佈程式類型，請執行第 372 頁的「啓用自訂稽核發佈程式」中的步驟，然後從 **[新增發佈程式]** 下拉式功能表中選取 **[JMX]**。
2. 若要配置 JMX 發佈程式類型，請完成 [配置新的稽核發佈程式] 表單。若對表單有任何問題，請參閱 i-Helps 及線上說明。

   發佈程式名稱 - 鍵入 JMX 稽核事件發佈程式的唯一名稱。

   歷程記錄限制 - 此爲發佈應保留在記憶體中的事件項目數。預設值爲 100。若要變更此限制，請輸入另一個值。
3. 按一下 **[測試]**，驗證 **[發佈程式名稱]** 是否爲可接受的名稱。
4. 按一下 **[確定]**。[配置新的稽核發佈程式] 表單會隨即關閉。
5. 重要事項！按一下 **[儲存]**。

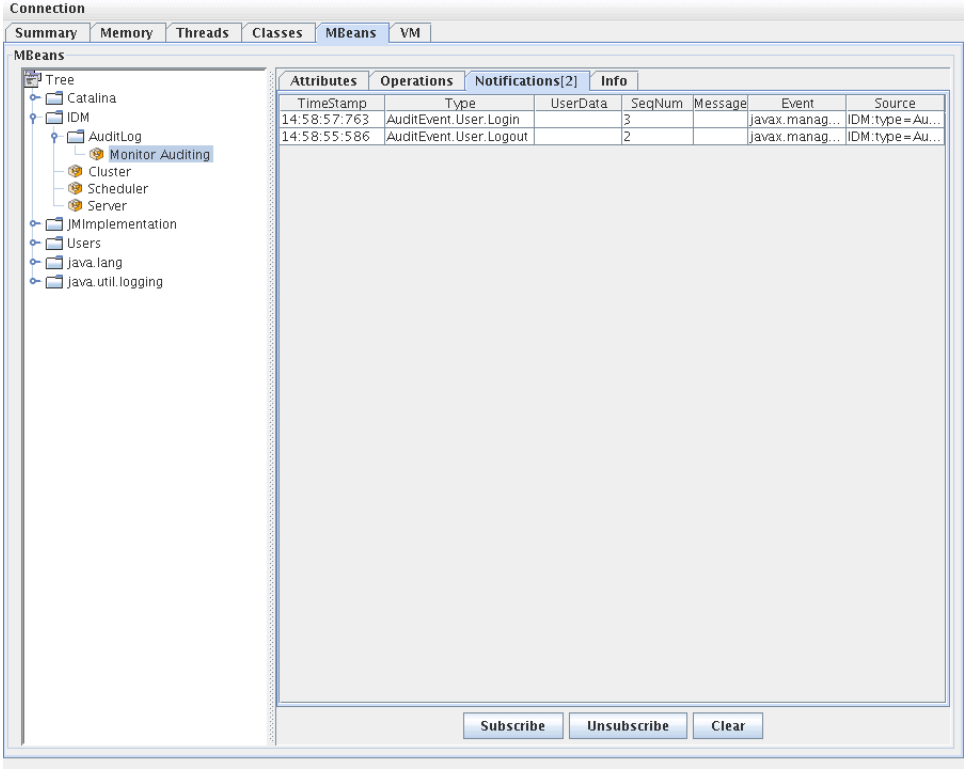
使用 JMX 用戶端檢視稽核事件

使用 JMX 用戶端可檢視 JMX 發佈程式。JDK 1.5 隨附的 JConsole 可用以建立下列螢幕擷取。

若使用 JConsole，請選擇「附加以處理」來檢視 `IDM:type=AuditLog` MBean。如需有關配置 JConsole 以用爲 JMX 用戶端的資訊，請參閱第 190 頁的「檢視 JMX 資料」。

在 JConsole 中按一下 **[通知]** 標籤，即可檢視稽核事件。請記下通知中的序號。查詢 MBean 以取得額外資訊時，需要有序號。

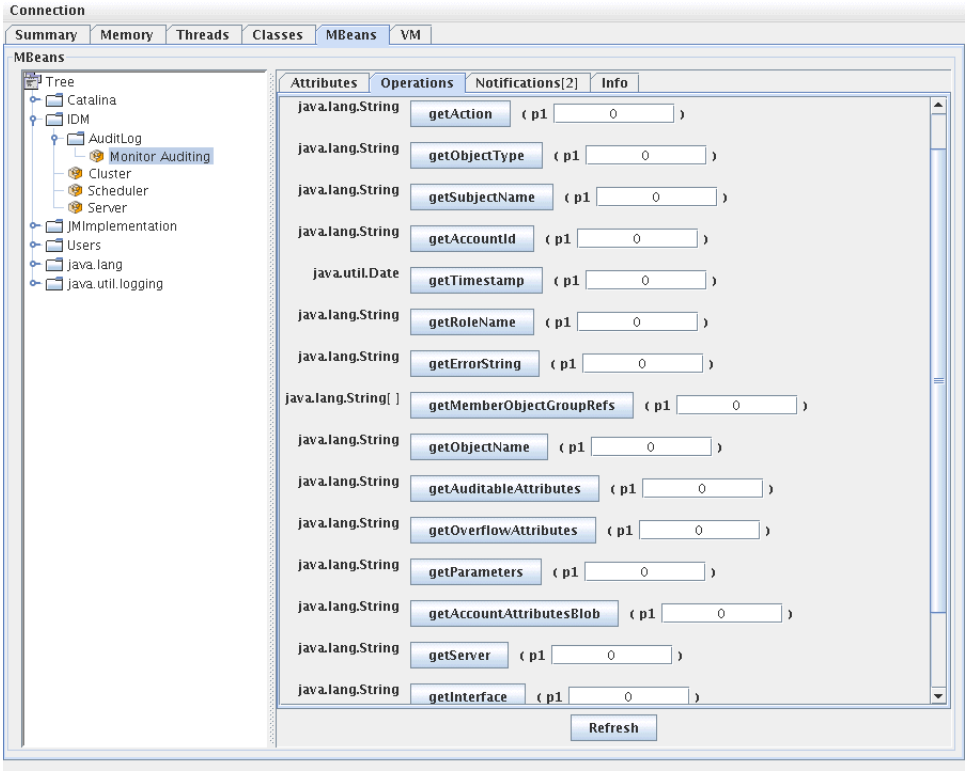
圖 10-3 在 JConsole 中檢視 JMX 稽核事件通知



查詢 MBean 以取得額外資訊

請在 JConsole 中按一下 **[作業]** 標籤。使用通知中的序號，可查詢 MBean 以取得事件詳細資訊。每個作業前方都會加上「get」，而唯一的參數是「序列號」。

圖 10-4 在 JConsole 中查詢 MBean 以取得額外資訊



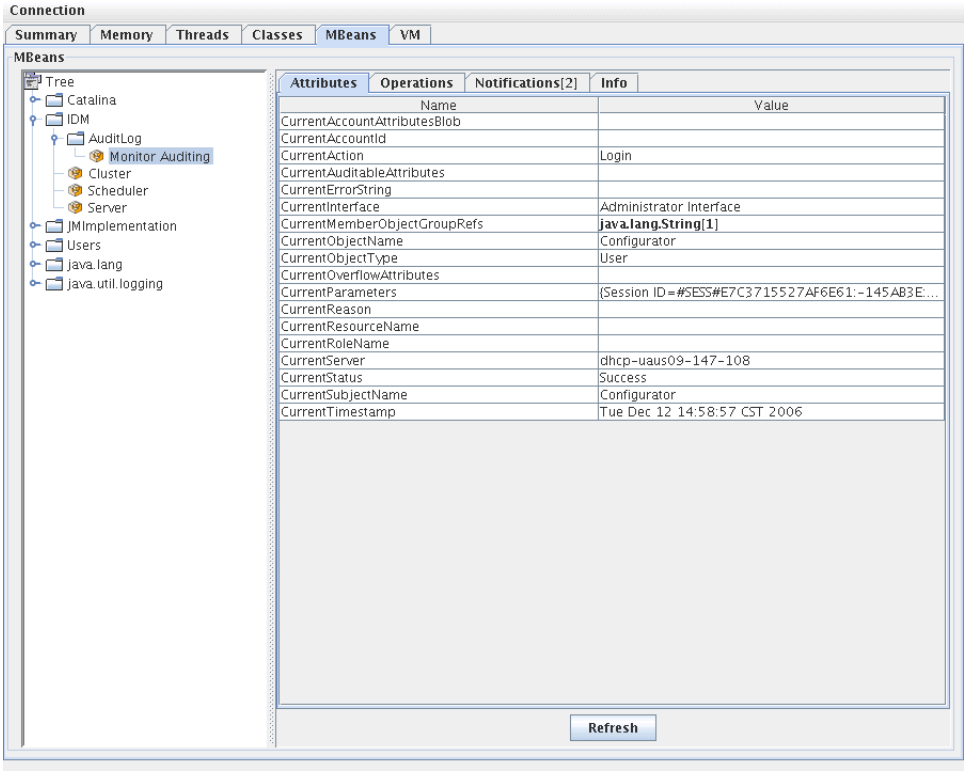
MBean 其實是一對一對映到 com.waveset.object.AuditEvent 類別。表 10-19 提供 MBean 所提供之每個屬性/作業的說明。

表 10-19　MBeanInfo 屬性/作業說明

屬性 / 作業	說明
AccountAttributesBlob	已變更屬性的清單
AccountId	與事件相關聯的帳號 ID
Action	在事件期間所採取的動作
AuditableAttributes	可稽核的屬性
ErrorString	任何錯誤字串
Interface	稽核介面
MemberObjectGroupRefs	成員物件群組參照
ObjectName	物件名稱
ObjectType	物件類型
OverflowAttributes	所有溢位屬性
Parameters	所有參數
Reason	事件的原因
ResourceName	與事件相關聯的資源
RoleName	與事件相關聯的角色
SubjectName	與事件相關聯的使用者或服務
Server	發生事件的伺服器名稱
Status	稽核事件的狀態
Timestamp	稽核事件的日期/時間

請在 JConsole 中按一下 **[屬性]** 標籤。屬性前方會加上 `Current`，表示該屬性包含傳送至系統的最新稽核事件。

圖 10-5 在 JConsole 中檢視 MBean 屬性



開發自訂稽核發佈程式

本節記載如何使用 Java 建立新的自訂稽核發佈程式。

Identity Manager 提供的 [主控台]、[檔案] 和 [JDBC] 自訂發佈程式，會實作 AuditLogPublisher 介面。您可以在 REF 工具組中找到這些發佈程式的原始碼。REF 工具組還會提供 Javadoc 格式的介面文件 (請參閱 Javadoc，以取得有關介面的詳細資訊)。

備註 REF (資源擴充工具) 工具組隨附於產品 CD 的 /REF 目錄中，或隨附於安裝映像檔。

開發者可以延伸 AbstractAuditLogPublisher 類別。此類別可剖析配置並確保已爲發佈程式提供所有必要選項。(請參閱 REF 工具組中的發佈程式範例)。

發佈程式必須具有一個無引數建構子。

生命週期

以下步驟說明了發佈程式的生命週期：

1. 實例化物件。
2. 使用 setFormatter() 方法設定格式化程式 (如果有)。
3. 使用 configure(*Map*) 方法提供選項。
4. 使用 publish(*Map*, *LoggingErrorHandler*) 方法發佈事件。
5. 使用 shutdown() 方法終止發佈程式。

Identity Manager 啓動以及無論何時更新稽核配置時，均執行步驟 1 到 3。如果在呼叫關閉之前未產生稽核事件，則不執行步驟 4。

在同一發佈程式物件上僅呼叫一次 configure(Map)。(發佈程式無需爲作用中的配置變更做準備)。更新稽核配置後，首先會關閉目前的發佈程式，然後建立新的發佈程式。

步驟 3 中的 configure() 方法可能會丟出 WavesetException。在此情況下，將忽略發佈程式，且不會對此發佈程式進行任何其他呼叫。

配置

發佈程式可以沒有選項，也可以有多個選項。getConfigurationOptions() 方法可傳回發佈程式支援的選項清單。這些選項使用 PublisherOption 類別 (請參閱 Javadoc 以取得有關此類別的詳細資訊) 進行封裝。稽核配置檢視器在建立發佈程式的配置介面時會呼叫此方法。

Identity Manager 會在伺服器啓動時以及稽核配置變更之後，使用 configure(Map) 方法配置發佈程式。

開發格式化程式

REF 工具組包含下列格式化程式的原始碼：

- XmlFormatter - 將稽核事件格式化爲
- XML 字串
- UlfFormatter - 根據通用記錄格式 (ULF) 對稽核事件進行格式化。Sun Application Server 使用此格式。

格式化程式必須實作 AuditRecordFormatter 介面。此外，格式化程式必須具有一個無引數建構子。請參閱 REF 工具組中所含的 Javadoc，以取得詳細資訊。

註冊發佈程式/格式化程式

#ID#Configuration:SystemConfiguration 物件的稽核屬性列出所有已註冊的發佈程式和格式化程式。只有這些發佈程式和格式化程式可在稽核配置使用者介面中使用。

第 11 章

PasswordSync

PasswordSync 可偵測 Windows 網域上啓動的使用者密碼變更，並將這些變更轉寄至 Identity Manager。Identity Manager 接著會使這些密碼變更與 Identity Manager 中定義的其他資源同步化。

本章包含以下主題：

什麼是 PasswordSync？

PasswordSync 功能可以使在 Windows Active Directory 網域上所做的使用者密碼變更，與 Identity Manager 中定義的其他資源保持同步。您必須在要與 Identity Manager 同步化之網域中的每個網域控制器上安裝 PasswordSync。您必須將 PasswordSync 與 Identity Manager 分開安裝。

PasswordSync 包含位於每個網域控制器上的 DLL (`lhpwic.dll`)。此 DLL 會收到 Windows 傳送的密碼更新通知、將其加密，並透過 HTTPS 將通知傳送至 PasswordSync Servlet。PasswordSync Servlet 位在執行 Identity Manager 的應用程式伺服器上。

備註 Sun 建議使用 HTTPS，但也支援 HTTP。

PasswordSync Servlet 會將通知轉譯爲 Identity Manager 可瞭解的格式。然後再使用下列方法之一，將密碼變更 (仍處於加密情況) 傳送至 Identity Manager：

- **直接方法** - Servlet 使用本機 Identity Manager 類別，直接將密碼變更傳送至 Identity Manager (請參閱圖 11-1 (第 385 頁))。

  只有需要將訊息傳送至一部系統，且不需要擔保訊息傳送的較小型且不複雜的環境，才建議使用直接連線方法 (如果因爲某些原因而導致直接訊息傳送失敗，則訊息會遺失。您無法備份傳送)。

- **JMS 方法** - Servlet 使用 JMS (Java Message Service)，將密碼資訊傳送至 Identity Manager。Servlet 使用 JMS 提交密碼變更給 JMS Message Queue。另一方面，Identity Manager 的 JMS 偵聽程式資源配接卡會檢查佇列是否有新訊息。若佇列中發現有等候的密碼變更訊息，JMS 偵聽程式介面會從佇列中取出訊息，並匯入至 Identity Manager (請參閱圖 11-2 (第 385 頁))。

  若是需要將訊息傳送至多部系統，且需要擔保訊息傳送的較複雜環境，則建議使用 JMS 方法 (JMS Message Queue 可設定爲高度可用。此外，若訊息傳送失敗，佇列會保留變更直到可傳送至 Identity Manager 爲止)。

  但是，必須要分開安裝及配置 JMS。

圖 11-1 圖示直接連線。在此配置中，PasswordSync Servlet 會將更新訊息直接傳送至 Identity Manager

圖 11-1 PasswordSync 邏輯圖表 (直接連線)

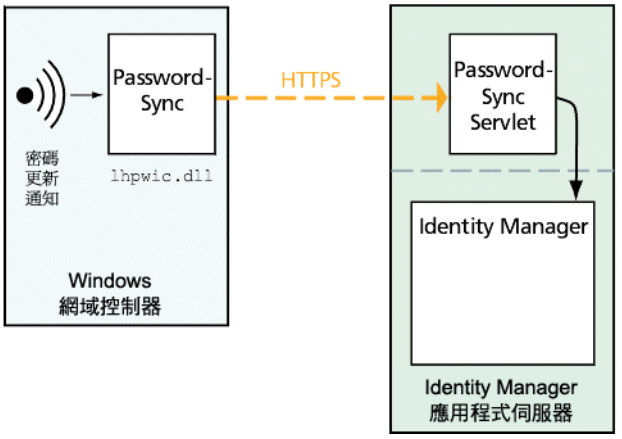
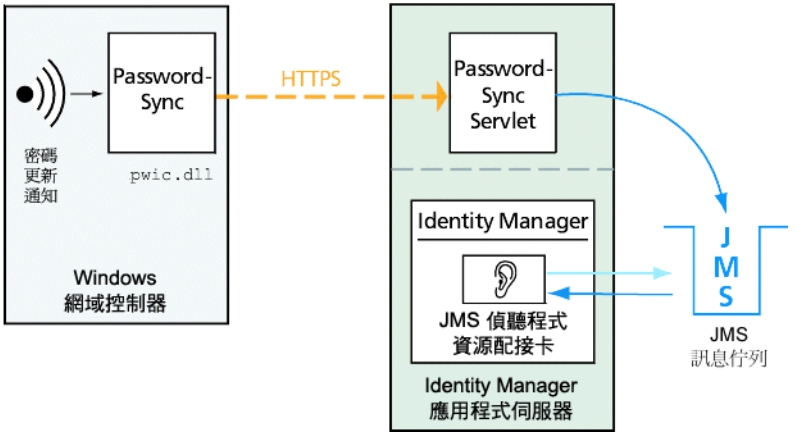


圖 11-2 圖示 JMS 連線。在此配置中，PasswordSync Servlet 會將更新訊息傳送至 JMS Message Queue。Identity Manager 的 JMS 偵聽程式資源配接卡會定期檢查佇列 (在圖表中以淺藍色的箭頭表示) 中是否有新訊息。而佇列的回應是將訊息傳送至 Identity Manager (以深藍色箭頭表示)。

圖 11-2 PasswordSync 邏輯圖表 (JMS 連線)

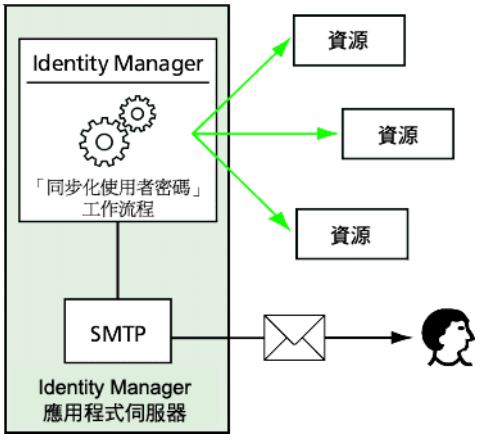


Identity Manager 收到密碼變更通知之後，會將其解密，並使用工作流程作業處理該變更。密碼將在使用者的所有指定資源中更新，同時 SMTP 伺服器會向使用者傳送電子郵件，以通知使用者密碼變更的狀態。

備註 Windows 僅會在密碼變更成功時，傳送更新通知。若密碼變更請求不符合網域的密碼策略，Windows 即會拒絕，而且不會向 Identity Manager 傳送任何同步化資料。

圖 11-3 顯示 Identity Manager 啓動工作流程，並在收到密碼更新通知之後，傳送電子郵件給使用者。

圖 11-3 PasswordSync 觸發工作流程



備註 PasswordSync 會捨棄帳號名稱結尾爲 $ (美元符號) 的所有帳號變更通知。結尾爲 $ 的帳號名稱會假設爲 Windows 電腦帳號。所有結尾是美元符號的**使用者**帳號，均不會轉寄至 Identity Manager。

安裝前注意事項

PasswordSync 功能只能設定在 Windows 2003 和 Windows 2000 網域控制器上 (Identity Manager 8.0 版起已停止支援 Windows NT 網域控制器)。您必須在會與 Identity Manager 同步化的網域中之每個主要與備份網域控制器上，安裝 PasswordSync。強烈建議配置 PasswordSync 使用 HTTPS。

備註 所有網域控制器上 7.1.1 版以前的 PasswordSync，都至少應更新爲 7.1.1 版。

8.0 版已不再支援 rpcrouter2 Servlet，且會自後續發行版本中移除。PasswordSync 7.1.1 版及更新版本支援新的協定。

若使用 JMS，PasswordSync 需要與 JMS 伺服器的連結。如需有關 JMS 系統需求的更多資訊，請參閱「Sun Identity Manager Resources Reference」中的「JMS 偵聽程式資源配接卡」一節。

此外，PasswordSync 還需要

- 在每個網域控制器上至少要安裝 Microsoft .NET 1.1
- 移除所有舊版的 PasswordSync

以下各節將更詳細地討論這些需求。

安裝 Microsoft .NET 1.1

若要使用 PasswordSync，則必須安裝 Microsoft .NET 1.1 Framework。如果您使用 Windows 2003 網域控制器，則依預設安裝此 Framework。若使用 Windows 2000 網域控制器，則可以從 Microsoft 下載中心下載此工具組，網址爲：

http://www.microsoft.com/downloads

備註

- **在 [關鍵字] 搜尋欄位中輸入 `NET Framework 1.1 Redistributable`，以快速尋找架構工具組。**
- **該工具組將安裝** .NET 1.1 Framework。

配置 PasswordSync 使用 SSL

雖然機密資料在傳送至 Identity Manager 伺服器之前會經過加密，但是 Sun Microsystems 還是建議您配置 PasswordSync 使用安全的 SSL 連線 (亦即 *HTTPS* 連線)。

如需有關如何安裝匯入的 SSL 憑證的資訊，請參閱以下 Microsoft 知識庫 How-To 文章：

http://support.microsoft.com/kb/816794

安裝 PasswordSync 之後，可在 [PasswordSync 配置] 對話方塊中指定 HTTPS URL，以測試 SSL 連線是否配置正確。請參閱第 416 頁的「測試您的配置」，以取得說明。

解除安裝舊版的 PasswordSync

安裝更高版本之前，您必須先移除先前安裝的所有 PasswordSync 實例。

- 如果先前安裝的 PasswordSync 版本支援 `IdmPwSync.msi` 安裝程式，您可以使用標準的 Windows [新增/移除程式] 公用程式來移除該程式。
- 如果先前安裝的 PasswordSync 版本不支援 `IdmPwSync.msi` 安裝程式，則可以使用 InstallAnywhere 解除安裝程式來移除該程式。

在 Windows 上安裝 PasswordSync

以下程序說明了如何安裝 PasswordSync 配置應用程式。

備註 您必須在會與 Identity Manager 同步化的網域中之每個網域控制器上安裝 PasswordSync。

請務必先解除安裝所有之前安裝的 PasswordSync 版本，再繼續安裝。

若要安裝 PasswordSync，請執行以下步驟：

1. 若安裝至 32 位元版本的 Windows，請從 Identity Manager 安裝媒體連按兩下 `pwsync\IdmPwSync_x86.msi`，而若安裝至 64 位元版本的 Windows，請連按兩下 `pwsync\IdmPwSync_x64.msi`。

   將顯示歡迎視窗。

   安裝精靈提供了以下瀏覽按鈕：

   - **[取消]**：按一下可隨時結束精靈，而不儲存任何變更。
   - **[上一步]**：按一下可返回前一個對話方塊。
   - **[下一頁]**：按一下可進入下一個對話方塊。

2. 請閱讀 [歡迎] 螢幕上顯示的資訊，然後按 **[下一步]** 以顯示 [選擇安裝類型 PasswordSync 配置] 視窗。

3. 按一下 **[一般]** 或 **[完成]** 以安裝完整的 PasswordSync 套裝軟體，或按一下 **[自訂]** 以控制要安裝的套裝軟體部分。

4. 按一下 **[安裝]** 以安裝產品。

   成功安裝 PasswordSync 後，螢幕上將顯示訊息告知您安裝成功。

5. 按一下 **[完成]** 以完成安裝程序。

   請務必選取 **[啓動配置應用程式]**，以開始配置 Password Sync。請參閱第 391 頁的「配置 PasswordSync」，以取得有關該程序的詳細資訊。

備註 螢幕上將顯示對話方塊，表明您必須重新啓動系統才能使變更生效。完成配置 PasswordSync 之前不必重新啓動系統，但必須在實作 PasswordSync 之前重新啓動網域控制器。

表 11-1 說明了安裝在每個網域控制器上的檔案。

表 11-1 網域控制器檔案

安裝的元件	說明
%$INSTALL_DIR$%\configure.exe	PasswordSync 配置程式
%$INSTALL_DIR$%\configure.exe.manifest	配置程式的資料檔
%$INSTALL_DIR$%\passwordsyncmsgs.dll	處理 PasswordSync 訊息的 DLL
%SYSTEMROOT%\SYSTEM32\lhpwic.dll	實作 Windows `PasswordChangeNotify ()` 函數的密碼通知 DLL

配置 PasswordSync

如果您從安裝程式執行配置應用程式，則該應用程式會將配置螢幕顯示爲精靈。完成精靈後，以後每次執行 PasswordSync 配置應用程式時，都可以透過選取標籤在螢幕之間瀏覽。

若要配置 PasswordSync，請執行以下步驟：

1. 請啓動 PasswordSync 配置應用程式 (若尚未執行)。

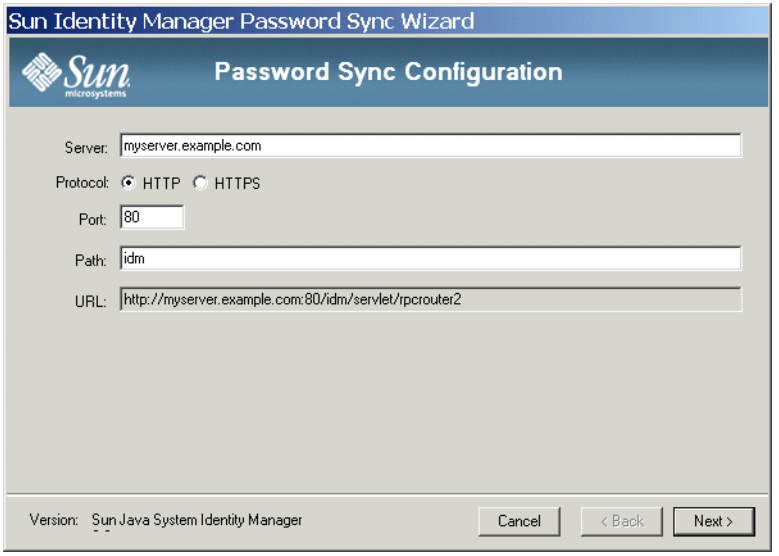
   依預設，此配置應用程式安裝在 [Program Files] > Sun Identity Manager PasswordSync > [配置] 中。

   若不打算使用 JMS，請從指令行啓動配置應用程式。請務必要包含 `-direct` 旗標：

   ```
   C:\InstallDir\Configure.exe -direct
   ```

   螢幕上將顯示 [PasswordSync 配置] 對話方塊 (請參閱圖 11-4)。

圖 11-4 PasswordSync 精靈配置對話方塊

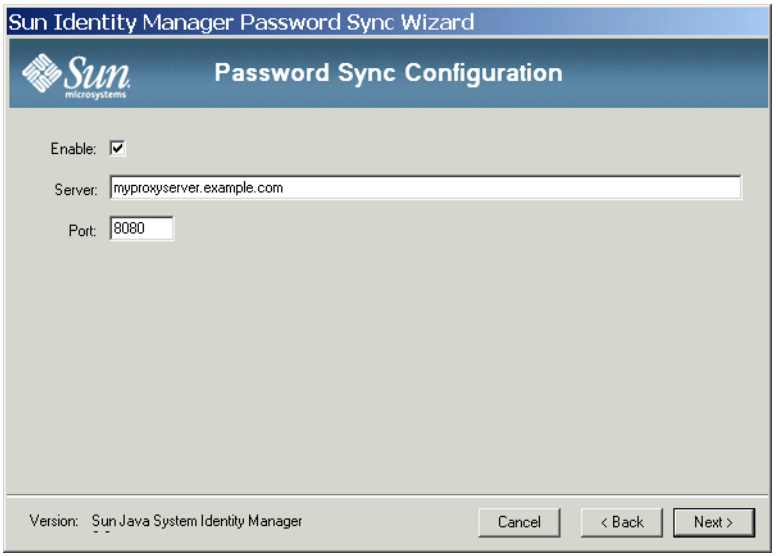


依需要編輯以下欄位。

- **[伺服器]** 必須用安裝 Identity Manager 的完全合格的主機名稱或 IP 位址替代。
- **[協定]** 指示是否與 Identity Manager 進行安全連線。如果選取 HTTP，則預設連接埠爲 80。如果選取 HTTPS，則預設連接埠爲 443。
- **[路徑]** 指定應用程式伺服器上 Identity Manager 的路徑。
- **[URL]** 透過將其他欄位鏈結在一起產生。不能在 URL 欄位中編輯值。

2. 按 [下一頁] 以顯示代理伺服器配置頁面 (圖 11-5)。

圖 11-5 PasswordSync 精靈代理伺服器對話方塊



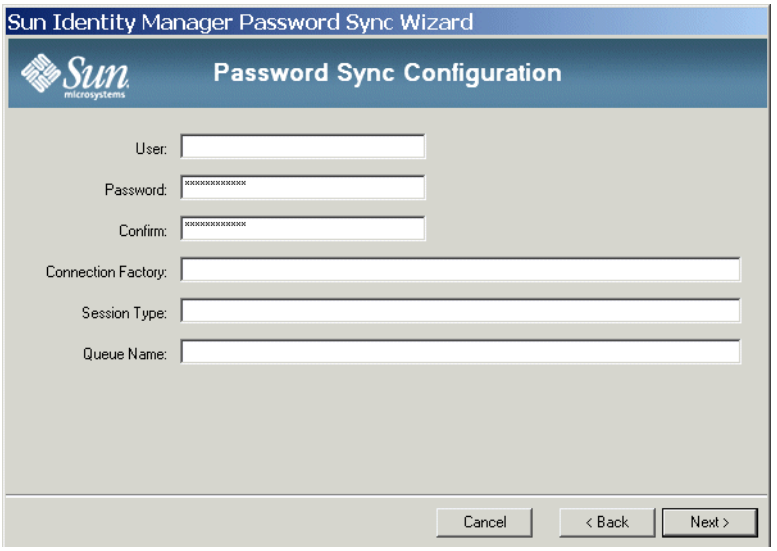
依需要編輯以下欄位。

- 若需要代理伺服器，請選取 **[啓用]**。
- **[伺服器]** 必須以代理伺服器的完全合格主機名稱或 IP 位址替代。
- **Port**：指定可用的伺服器連接埠號碼 (預設代理伺服器連接埠爲 8080，預設 HTTPS 連接埠爲 443)。

3. 按 [下一頁] 以顯示 JMS 設定對話方塊 (圖 11-6)。

   或者，若不打算使用 JMS，且已使用 `-direct` 旗標啓動配置精靈，則請按 **[下一步]** 以顯示 [使用者] 對話方塊。跳至第 394 頁的步驟 5。

圖 11-6 PasswordSync 精靈 JMS 設定對話方塊

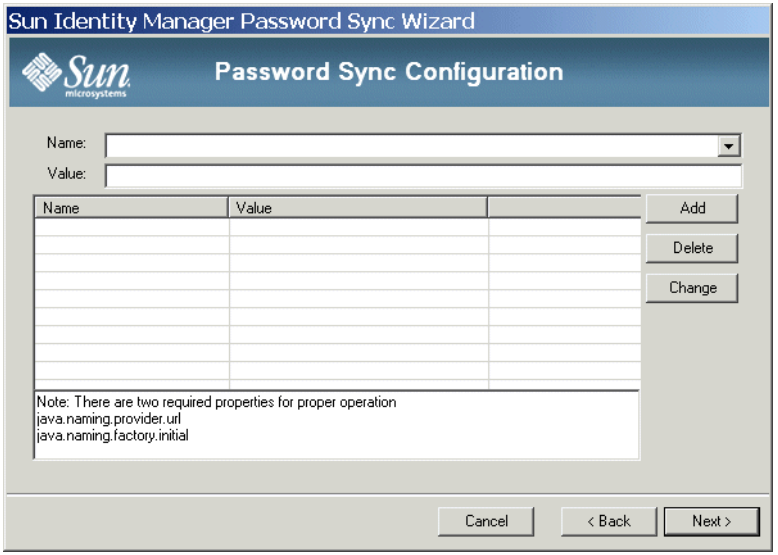


依需要編輯以下欄位。

- **[使用者]** 指定在佇列中置入新訊息的 JMS 使用者名稱。
- **[密碼]** 和 **[確認]** 指定 JMS 使用者的密碼。
- **[連線工廠]** 指定要使用之 JMS 連線工廠的名稱。該工廠必須已存在於 JMS 系統中。
- 在大多數情況下，應將 **[階段作業類型]** 設定爲 `[LOCAL]`，這表示將使用本機階段作業作業事件。系統收到每條訊息後，將提交階段作業。其他可能的值包括 `[AUTO]`、`[CLIENT]` 和 `[DUPS_OK]`。
- **[佇列名稱]** 指定密碼同步化事件的目標查詢名稱。

4. 按 [下一頁] 以顯示 JMS 特性對話方塊 (圖 11-7)。

圖 11-7 PasswordSync 精靈 JMS 特性對話方塊



JMS 特性對話方塊可讓您定義用於建立初始 JNDI 環境的特性集。必須定義以下名稱/值對：

- `java.naming.provider.url` - 必須將該值設定爲執行 JNDI 服務之機器的 URL。
- `java.naming.factory.initial` - 必須將該值設定爲 JNDI 服務提供者的初始環境工廠之類別名稱 (包括套裝模組)。

[名稱] 下拉式功能表包含 `java.naming` 套裝模組中的類別清單。選取類別或鍵入類型名稱，然後在 [值] 欄位中輸入其對應的值。

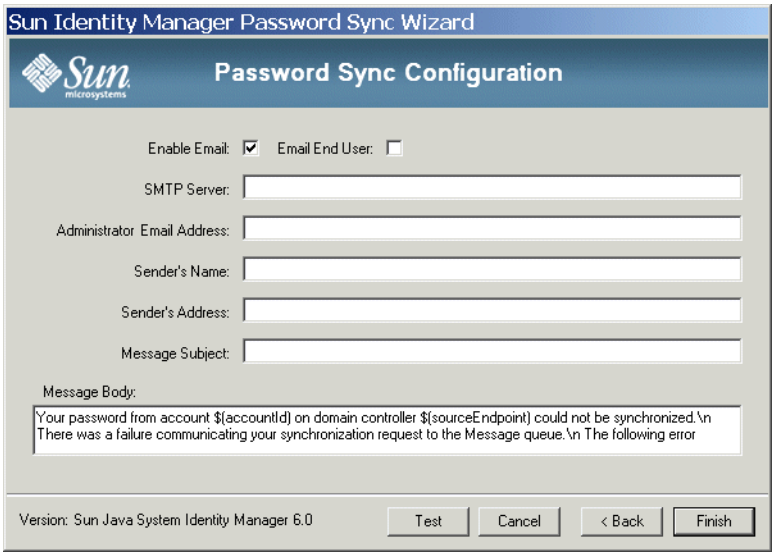
5. 若不打算使用 JMS，且已使用 `-direct` 旗標啓動配置精靈，則請配置 [使用者] 標籤。否則，請略過此步驟並進入下一個步驟。

   若要配置 [使用者] 標籤，請視需要編輯欄位。

   - **[帳號 ID]** 可指定連線至 Identity Manager 所使用的使用者名稱。
   - **[密碼]** 可指定連線至 Identity Manager 所使用的密碼。

6. 按 [下一頁] 以顯示電子郵件對話方塊 (圖 11-8)。

圖 11-8 PasswordSync 精靈電子郵件對話方塊



透過 [電子郵件] 對話方塊，您可以配置當使用者的密碼變更未成功同步化 (由於通訊錯誤或 Identity Manager 之外的其他錯誤) 時，是否傳送電子郵件通知。

依需要編輯以下欄位。

- 選取 **[啓用電子郵件]** 以啓用該功能。如果使用者要接收通知，請選取 **[電子郵件一般使用者]**。否則，將僅通知管理員。
- **[SMTP 伺服器]** 是傳送故障通知時要使用之 SMTP 伺服器的完全合格名稱或 IP 位址。
- **[管理員電子郵件地址]** 是用於傳送通知的電子郵件位址。
- **[寄件者名稱]** 是方便易用的寄件者名稱。
- **[寄件者地址]** 是寄件者的電子郵件地址。
- **[訊息主旨]** 指定所有通知的主旨行
- **[訊息內文]** 指定通知的文字。

郵件內文可能包含以下變數。

- `$(accountId)` - 嘗試變更密碼的使用者之帳號 ID。
- `$(sourceEndpoint)` - 安裝密碼提示程式的網域控制器之主機名稱，有助於找到發生問題的機器。
- `$(errorMessage)` - 對所發生的錯誤進行說明的錯誤訊息。

7. 按一下 **[完成]** 以儲存變更。

若再次執行配置應用程式，則螢幕上將會顯示一組標籤，而非精靈。若希望將應用程式顯示爲精靈，請從指令行鍵入以下指令：

`C:\`*InstallDir*`\Configure.exe -wizard`

若要測試 PasswordSync 配置，請參閱第 416 頁的 「測試您的配置」。

在 Windows 上對 PasswordSync 執行除錯

請參閱「Identity Manager Tuning, Troubleshooting, and Error Messages」一書，以取得有關在 Windows 上對 PasswordSync 進行疑難排解的資訊。

錯誤記錄

PasswordSync 會將所有故障寫入 Windows 事件檢視器 (如需使用事件檢視器的說明，請參閱 Windows 說明)。錯誤記錄項目的來源名稱是 PasswordSync。

解除安裝 Windows 上的 PasswordSync

若要解除安裝 PasswordSync 應用程式，請至 Windows [控制面板] 並選取**[新增/移除程式]**。然後選取 **[Sun Identity Manager PasswordSync]** 並按一下 **[移除]**。

備註	您也可以放入 Identity Manager 安裝媒體並按一下 `pwsync\IdmPwSync.msi` 圖示，以解除安裝 (或重新安裝) PasswordSync。

必須重新啓動系統才能完成該程序。

在應用程式伺服器上部署 PasswordSync

在 Windows 網域控制器上安裝 PasswordSync 之後，必須在執行 Identity Manager 的應用程式伺服器上進行額外的步驟。

您不需要在應用程式伺服器上安裝 PasswordSync Servlet。它會隨著 Identity Manager 安裝時自動安裝。

但是，若要完成部署 PasswordSync，則**必須**在 Identity Manager 中執行以下動作：

- 增加及配置 JMS 偵聽程式介面 (若使用 JMS)
- 實作「同步化使用者密碼」工作流程
- 設定通知

增加及配置 JMS 偵聽程式介面

若 PasswordSync Servlet 使用 JMS 將訊息傳送至 Identity Manager，則必須增加 Identity Manager 的 JMS 偵聽程式資源配接卡。JMS 偵聽程式資源配接卡會定期檢查 JMS Message Queue 中是否有 PasswordSync Servlet 放置的訊息。若佇列包含新訊息，則會將之傳送至 Identity Manager 進行處理。

若要增加 JMS 偵聽程式資源配接卡，請執行以下步驟。

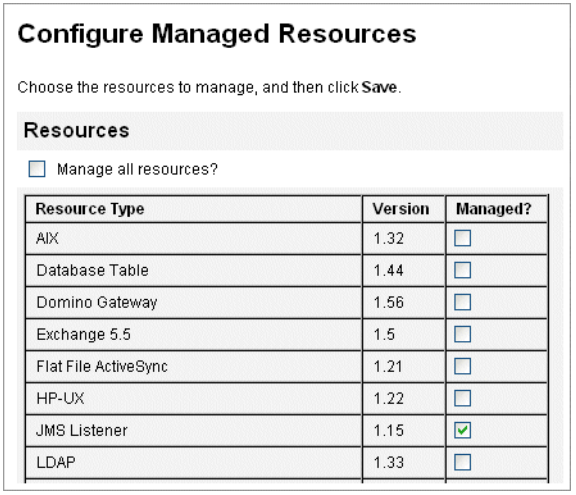
1. 登入 Identity Manager 管理員介面 (第 50 頁)。
2. 按一下 **[資源]**。
3. 按一下輔助功能表的 **[配置類型]**。

   [配置受管資源] 頁面會隨即開啓。
4. 確認已爲 **[JMS 偵聽程式]** 選取了 **[受管理？]** 欄中的核取方塊 (請參閱圖 11-9 (第 399 頁))。

   若未選取，請選取核取方塊，然後按一下 **[儲存]**。否則，請前往下一個步驟。

圖 11-9 顯示 [配置受管資源] 頁面。確認已選取了 **[JMS 偵聽程式]**。

圖 11-9 [配置受管資源] 頁面



5. 按一下輔助功能表的 **[列出資源]**。
6. 找到 **[資源類型動作]** 下拉式功能表，然後選取 **[新資源]**。

   [新資源] 頁面會隨即開啓。
7. 從下拉式功能表選取 **[JMS 偵聽程式]**，然後按一下 **[新增]** (請參閱圖 11-10 (第 400 頁))。

   [建立 JMS 偵聽程式資源精靈] 的 [歡迎] 頁面會隨即開啓。按 **[下一步]** 啓動配置精靈。

圖 11-10 顯示 [新增資源精靈]。若要增加 JMS 偵聽程式介面，請從清單中選取 **[JMS 偵聽程式]**。

圖 11-10 新增資源精靈

8. 完成 [資源參數] 精靈頁面上的表單。完成時按 **[下一步]**。

您必須配置以下設定：

- **目標類型** - 通常會將該值設定爲 **[佇列]** (因爲有一個訂閱者以及多個可能的發佈程式，所以主題通常不相關)。
- **初始環境 JNDI 特性** - 該文字方塊定義用於建立初始 JNDI 環境的特性集。必須定義以下名稱/值對：
  - `java.naming.factory.initial` - 必須將該值設定爲 JNDI 服務提供者的初始環境工廠之類別名稱 (包括套裝模組)。
  - `java.naming.provider.url` - 必須將該值設定爲執行 JNDI 服務之機器的 URL。

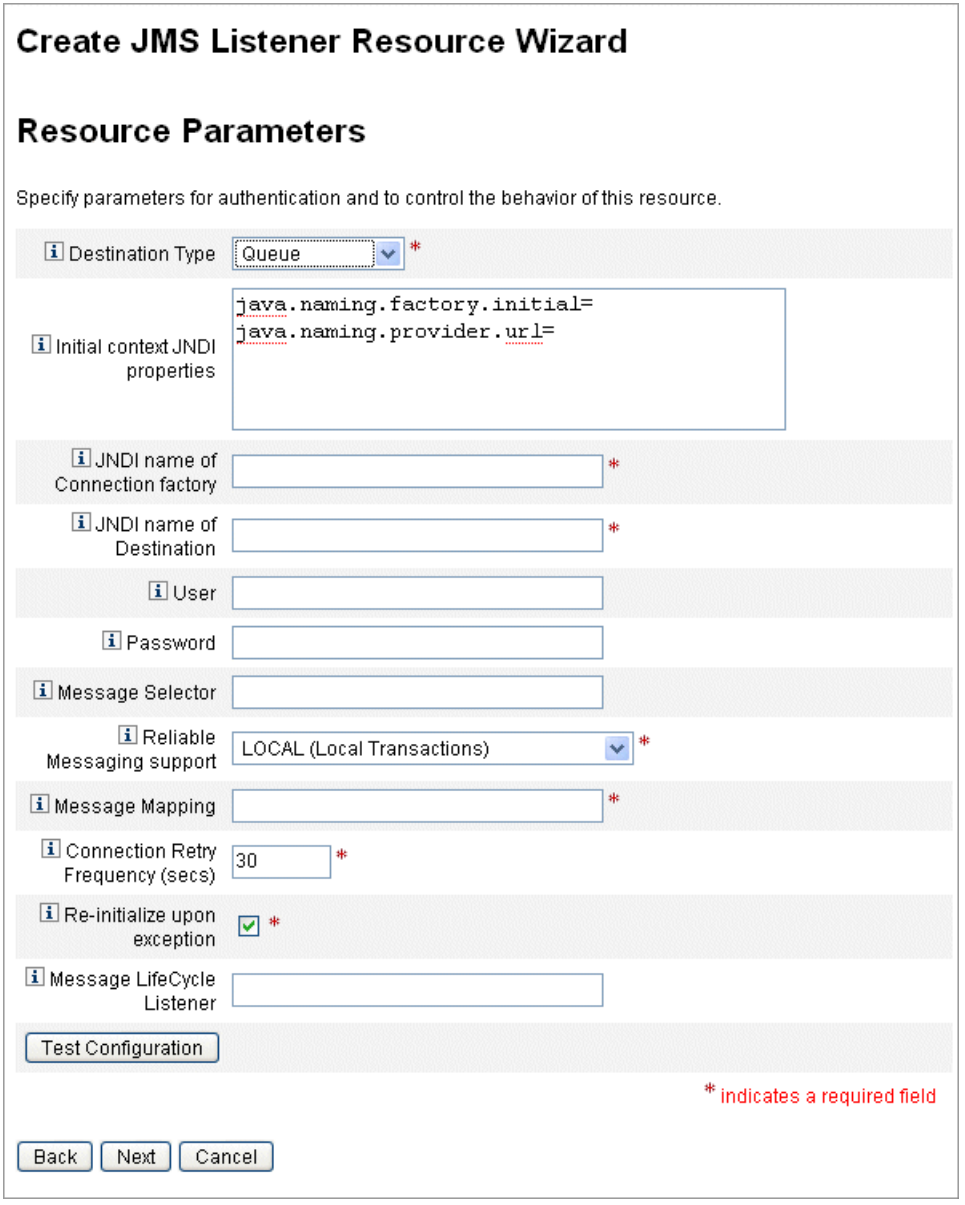
可能需要定義其他特性。特性和值清單應與 JMS 伺服器的 JMS 設定頁上指定的特性和值相符。

例如，若要提供憑證和連結方法，您必須指定以下特性範例：

- `java.naming.security.principal`：連結 DN (例如，cn=Directory manager)
- `java.naming.security.authentication`：連結方法 (例如，簡單)
- `java.naming.security.credentials`：密碼

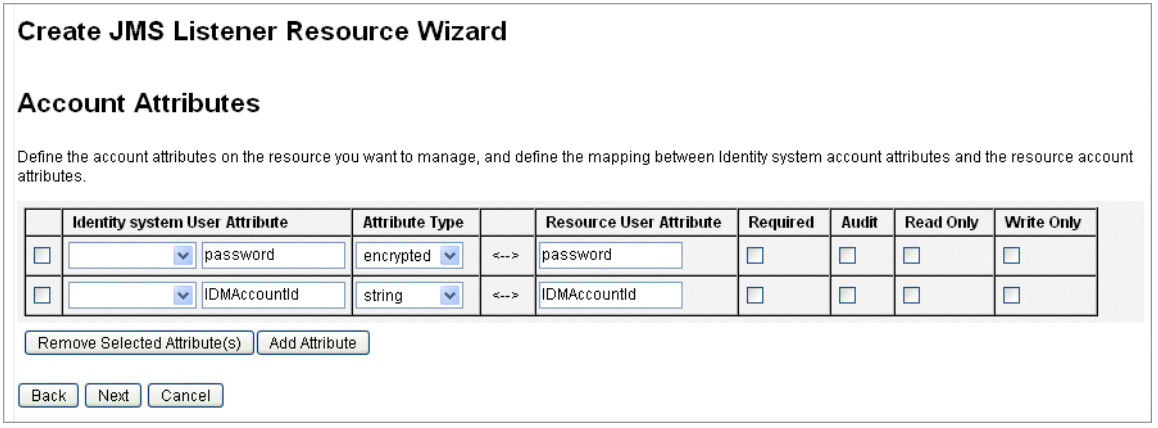
- **連線工廠的 JNDI 名稱** - 在 JMS 伺服器中定義的連線工廠名稱。
- **目標的 JNDI 名稱** - 在 JMS 伺服器中定義的目標名稱。
- **使用者**與**密碼** - 從佇列中請求新事件的管理員之帳號名稱和密碼。
- **可靠的訊息傳送支援** - 選取 `LOCAL`（本機作業事件）。其他選項不適用於密碼同步化。
- **訊息對映** - 輸入 `java:com.waveset.adapter.jms.PasswordSyncMessageMapper`。該類別可將來自 JMS 伺服器的郵件變換爲同步化使用者密碼工作流程可以使用的格式。

圖 11-11　JMS 偵聽程式資源精靈的資源參數頁面



9. 在 [帳號屬性] 精靈頁面上，按一下 **[增加屬性]**。

圖 11-12　[建立 JMS 偵聽程式資源精靈] 的 [帳號屬性] 頁面



10. 對映以下屬性，JMS 偵聽程式介面可透過 `PasswordSyncMessageMapper` 使用這些屬性。請參閱圖 11-12。完成時按 **[下一步]**。

    - `IDMAccountId`：此屬性由 PasswordSyncMessageMapper 根據 JMS 訊息中傳送的 `resourceAccountId` 和 `resourceAccountGUID` 屬性進行解析。
    - `password`：在 JMS 訊息中轉寄的已加密密碼。

    按 **[下一步]**。

11. [身份識別範本] 精靈頁面會隨即開啓。

    請注意，您在前一個步驟中增加的屬性，會出現在 [資源精靈] 的 [屬性對映] 區段中 (圖 11-13)。

    按 **[下一步]**。

圖 11-13　JMS 偵聽程式資源精靈屬性對映

12. [身份識別系統參數] 精靈頁面會隨即開啓。

    請視需要配置此頁面上的選項。

請參閱「Sun Identity Manager Resources Reference」，以取得有關設定 JMS 偵聽程式資源配接卡的更多資訊。

實作同步化使用者密碼工作流程

Identity Manager 收到密碼變更通知之後，會啓動「同步化使用者密碼」工作流程。預設的「同步化使用者密碼」工作流程會簽出 ChangeUserPassword 檢視器，然後再重新簽入。接著，工作流程會處理所有資源帳號 (傳送初始密碼變更通知的 Windows 資源除外)。最後，Identity Manager 會傳送使用者電子郵件，指出所有資源上的密碼變更是否成功。

若要使用預設實作「同步化使用者密碼」工作流程，請將其指定爲 JMS 偵聽程式介面實例的處理規則。處理規則可在配置 JMS 偵聽程式進行同步化時指定 (請參閱第 413 頁的「配置 Active Sync」)。

若要修改工作流程，請複製 `$WSHOME/sample/wfpwsync.xml` 檔案並進行修改。然後將修改的工作流程匯入 Identity Manager。

您可能要對預設工作流程執行的一些修改包括：

- 變更密碼後通知哪些實體。
- 找不到 Identity Manager 帳號時會發生什麼情況。
- 在工作流程中選取資源的方式。
- 是否允許從 Identity Manager 變更密碼。

如需有關使用工作流程的詳細資訊，請參閱「Sun Identity Manager Workflows, Forms, and Views」。

設定通知

Identity Manager 提供兩種電子郵件範本，可通知使用者所有資源上的密碼變更是否成功。這些範本如下：

- 密碼同步通知
- 密碼同步失敗通知

兩個範本均應更新，以便在使用者需要進一步幫助時，爲其提供有關下一步操作的公司特定資訊。如需更多資訊，請參閱第 181 頁的「自訂電子郵件範本」。

使用 Sun JMS 伺服器配置 PasswordSync

Identity Manager 可使用 Java Message Service (JMS) 從 PasswordSync Servlet 接收密碼變更通知。除了擔保傳送之外，JMS 還可將訊息傳送至多部系統。

備註 請參閱「Sun Identity Manager Resources Reference」以取得有關此介面的更多資訊。

本小節透過方案範例提供了使用 Sun JMS 伺服器配置 PasswordSync 的說明。相關資訊編排如下：

簡介

本小節說明了方案範例、Windows PasswordSync 解決方案以及 JMS 解決方案。

方案範例

使用 JMS 伺服器配置 PasswordSync 的典型 (簡單) 用途是，可讓使用者變更其在 Windows 上的密碼，使 Identity Manager 取得新密碼，然後在 Sun Directory Server 上使用新密碼更新使用者帳號。

爲此方案配置了以下環境：

- Windows Server 2003 Enterprise Edition - Active Directory
- Sun Identity Manager 6.0 2005Q4M3
- 在 Suse Linux 10.0 上執行的 MySQL
- Tomcat 5.0.28 running on Suse Linux 10.0

- 在 Suse Linux 10.0 上執行的 Sun Message Queue 3.6 SP3 2005Q4
- 在 Suse Linux 10.0 上執行的 Sun Directory Server 5.2 SP4
- Java 1.5 (Java 5.0)

已將以下文件複製到 Tomcat `common/lib` 目錄來啓用 JMS 和 JNDI：

- `jms.jar` (自 Sun Message Queue)
- `fscontext.jar` (自 Sun Message Queue)
- `imq.jar` (自 Sun Message Queue)
- `jndi.jar` (自 Java JDK)

建立與儲存受管理物件

本小節提供了建立與儲存以下管理物件的說明，這些物件是使方案範例順利工作所必需的：

- 連線工廠物件
- 目標物件

受管理物件可儲存在 LDAP 目錄或檔案中。若使用檔案，則檔案的所有實例必須相同。

首先會介紹如何將受管理物件儲存在 LDAP 目錄中。如需有關將受管理物件儲存在檔案中的說明，請參閱第 411 頁。

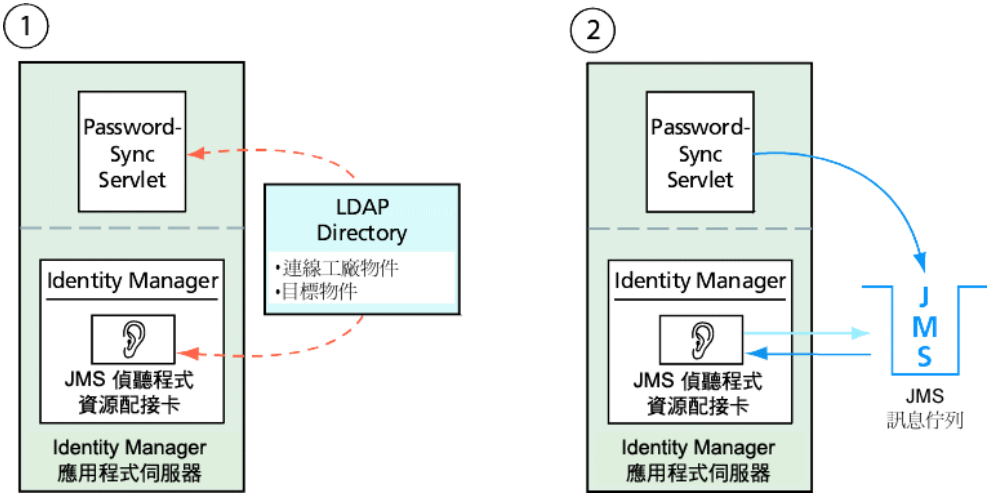
備註

- **本小節中的說明假設您已安裝 Sun Message Queue (必要的工具位於 Message Queue 安裝目錄的 `bin/` 中)。**
- **您可以使用 Message Queue 管理 GUI (`imqadmin`) 或指令行工具 (`imqobjmgr`) 建立這些受管理物件。以下說明使用指令行工具。**

將受管理物件儲存在 LDAP 目錄中

PasswordSync 與 JMS 偵聽程式可配置爲使用 LDAP 目錄中所儲存的受管理物件。圖 11-14 說明此程序。PasswordSync Servlet 和 JMS 偵聽程式介面都必須從 LDAP 目錄擷取連線工廠和目標設定，以便傳送及接收訊息。

圖 11-14　從 LDAP 目錄擷取連線工廠與目標物件



本節說明如何使用 Message Queue 指令行工具 (`imqobjmgr`) 將受管理物件儲存在 LDAP 目錄中。

儲存連線工廠物件

開啓 Message Queue 指令行工具 (imqobjmgr)，並鍵入編碼樣例 11-1 中的指令以儲存連線工廠物件。

編碼樣例 11-1 儲存連線工廠物件

```
#> ./imqobjmgr add -l "cn=mytestFactory"
-j "java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory"
-j "java.naming.provider.url=ldap://gwenig.coopsrc.com:389/ou=sunmq,dc=coopsrc,dc=com"
-j "java.naming.security.principal=cn=directory manager"
-j "java.naming.security.credentials=password"
-j "java.naming.security.authentication=simple"
-t qf
-o "imqAddressList=mq://gwenig.coopsrc.com:7676/jms"
Adding a Queue Connection Factory object with the following attributes:
imqAckOnAcknowledge [Message Service Acknowledgement of Client Acknowledgements]
...
imqSetJMSXUserID [Enable JMSXUserID Message Property] false

Using the following lookup name:
cn=mytestFactory
The object's read-only state:false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.ldap.LdapCtxFactory
java.naming.provider.url ldap://gwenig.coopsrc.com:389/ou=sunmq,dc=coopsrc,dc=com
java.naming.security.authentication simple
java.naming.security.credentials netscape
java.naming.security.principal cn=directory manager
Object successfully added.
```

在編碼樣例 11-1 中，imqAddressList 會定義 JMS 伺服器/代理程式主機名稱 (gwenig.coopsrc.com)、連接埠 (7676) 以及存取方法 (jms)。

儲存目標物件

在 Message Queue 指令行工具 (imqobjmgr) 中，鍵入編碼樣例 11-2 中的指令以儲存目標物件。

編碼樣例 11-2 儲存目標物件

```
#> ./imqobjmgr add -l "cn=mytestDestination"
-j "java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory"
-j "java.naming.provider.url=ldap://gwenig.coopsrc.com:389/ou=sunmq,dc=coopsrc,dc=com"
-j "java.naming.security.principal=cn=directory manager"
-j "java.naming.security.credentials=password"
-j "java.naming.security.authentication=simple"
-t q
-o "imqDestinationName=mytestDestination"
Adding a Queue object with the following attributes:
imqDestinationDescription [Destination Description] A Description for the Destination Object
imqDestinationName [Destination Name] mytestDestination
Using the following lookup name:
cn=mytestDestination
The object's read-only state:false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.ldap.LdapCtxFactory
java.naming.provider.url ldap://gwenig.coopsrc.com:389/
    ou=sunmq,dc=coopsrc,dc=com
java.naming.security.authentication simple
java.naming.security.credentials netscape
java.naming.security.principal cn=directory manager
Object successfully added.
```

備註 您可以使用 ldapsearch 或 LDAP 瀏覽器，檢查新建立的物件。

將受管理物件儲存在 LDAP 伺服器上的小節到此結束。請略過下一節有關將受管理物件儲存在檔案中的說明，並前往第 413 頁的「爲此方案配置 JMS 偵聽程式介面」小節。

將受管理物件儲存在檔案中

PasswordSync 與 JMS 偵聽程式可配置爲使用檔案中所儲存的受管理物件。若不是在 LDAP 伺服器上儲存受管理物件 (第 408 頁)，請遵循本小節的指示進行。

儲存連線工廠物件

開啓 Message Queue 指令行工具 (`imqobjmgr`)，並鍵入編碼樣例 11-3 中的指令以儲存連線工廠物件，並指定查找名稱。

編碼樣例 11-3 儲存連線工廠物件和指定查詢名稱

```
#> ./imqobjmgr add -l "mytestFactory" -j "java.naming.factory.initial=
com.sun.jndi.fscontext.RefFSContextFactory"
-j "java.naming.provider.url=file:///home/gael/tmp" -t qf -o
"imqAddressList=mq://gwenig.coopsrc.com:7676/jms"
Adding a Queue Connection Factory object with the following attributes:
imqAckOnAcknowledge [Message Service Acknowledgement of    Client Acknowledgements]
...
imqSetJMSXUserID [Enable JMSXUserID Message Property] false
Using the following lookup name:
mytestFactory
The object's read-only state:false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.fscontext.RefFSContextFactory
java.naming.provider.url file:///home/gael/tmp
Object successfully added.
To specify a destination:
#> ./imqobjmgr add -l "mytestQueue" -j
"java.naming.factory.initial=com.sun.jndi.fscontext.RefFSContextFactory"
-j "java.naming.provider.url=file:///home/gael/tmp" -t q -o
   "imqDestinationName=myTestQueue"
Adding a Queue object with the following attributes:
imqDestinationDescription [Destination Description] A Description for the Destination Object
imqDestinationName [Destination Name] myTestQueue
Using the following lookup name:
mytestQueue
The object's read-only state:false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.fscontext.RefFSContextFactory
java.naming.provider.url file:///home/gael/tmp
Object successfully added.
```

在代理程式上建立目標

依預設，Sun Message Queue 代理程式允許自動建立佇列目標 (請參閱 config.properties，其中 imq.autocreate.queue 的預設值爲 true)。

如果未自動建立佇列目標，則您必須使用編碼樣例 11-4 (其中 *myTestQueue* 爲目標) 中顯示的指令在代理程式上建立目標物件：

編碼樣例 11-4 在代理程式上建立目標物件

```
name (Queue name):
#> cd /opt/sun/mq/bin
#>./imqcmd create dst -t q -n mytestQueue
Username:<admin>
Password:<admin>
Creating a destination with the following attributes:
Destination Name mytestQueue
Destination Type Queue
On the broker specified by:
-------------------------
Host Primary Port
-------------------------
localhost 7676
Successfully created the destination.
```

您可以將受管理物件儲存在目錄或檔案中：

- **在目錄中：**使用目錄是儲存連線工廠和目標物件的集中方式。

  使用目錄時，這些受管理物件作爲目錄項目儲存。

  備註 若 Identity Manager PasswordSync Servlet 和 Identity Manager 伺服器不在同一台機器上，則二者都必須可以存取 .bindings 檔案。您可以重複建立兩次受管理物件 (在每台機器上)，或將 .bindings 檔案複製到每台機器上的適當位置。

- **在檔案中：**若 Identity Manager PasswordSync Servlet 和 Identity Manager 伺服器均在相同的伺服器上執行 (或是如果沒有可用的目錄)，則可以將管理物件儲存在檔案中。

使用檔案時，兩個受管理物件均儲存在單一檔案中 (在 Windows 和 Unix 上均稱爲 `.bindings`)，其位於您爲 java.naming.provider.url 指定的目錄 (例如，Windows 上的 `file:///c:/temp` 或 Unix 上的 `file:///tmp`) 下。

為此方案配置 JMS 偵聽程式介面

在應用程式伺服器上配置 JMS 偵聽程式介面。請遵循第 398 頁的 「增加及配置 JMS 偵聽程式介面」一節的指示進行。

配置 Active Sync

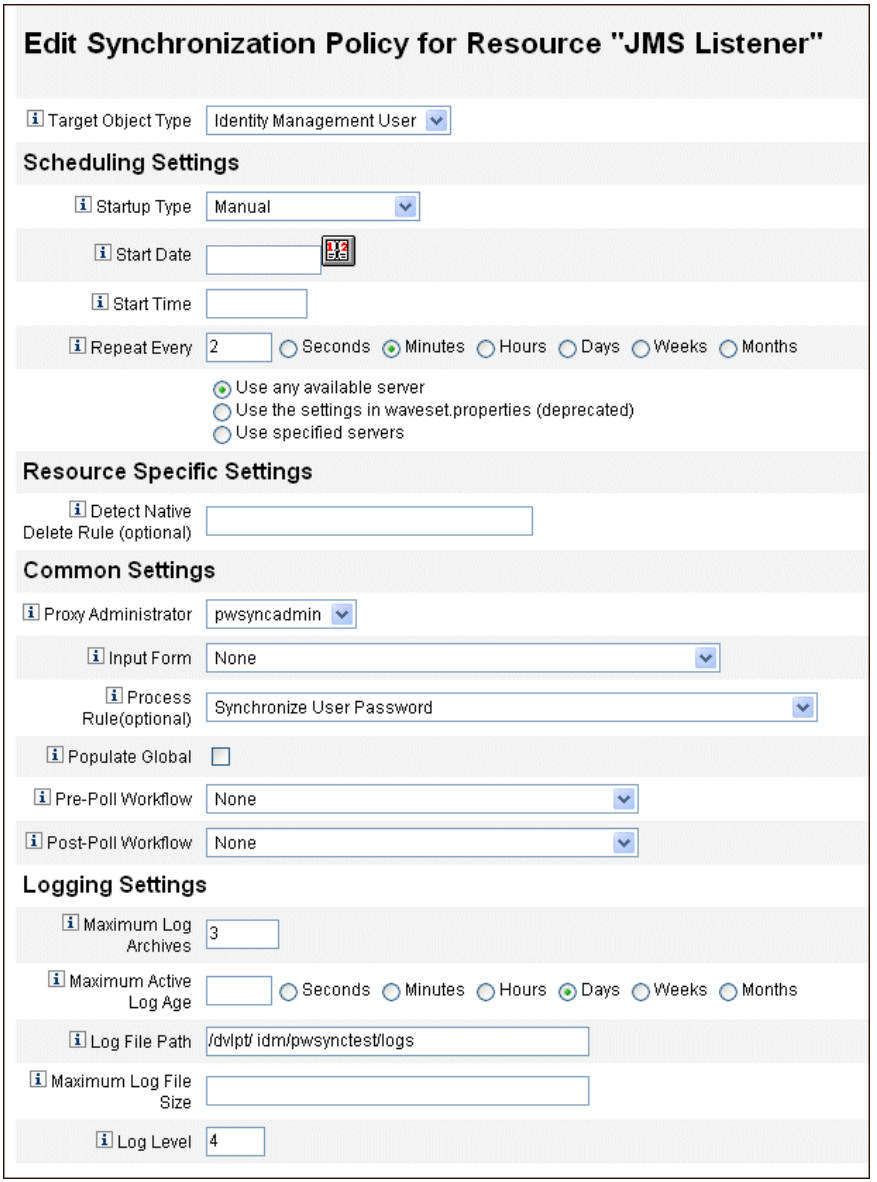
接著配置 JMS 偵聽程式進行同步化。使用 JMS 時需要 Active Sync，但直接連線則不會用到。

若要配置 JMS 偵聽程式進行同步化，請執行以下步驟：

1. 在管理員介面中，按一下功能表的 **[資源]**。
2. 在 **[資源清單]** 中，選取 **[JMS 偵聽程式]** 核取方塊。
3. 在 **[資源動作]** 清單中，選取 **[編輯同步化策略]**。

   JMS 偵聽程式資源的 [編輯同步化] 頁面會隨即開啓 (圖 11-15)。

圖 11-15　為 JMS 偵聽程式配置 Active Sync



4. 在 **[共用設定]** 下，找到 **[代理管理員]**，然後選取 [pwsyncadmin] (此管理員與空白表單相關聯)。

5. 在 **[共用設定]** 下，找到 **[處理規則]**，然後從清單中選取 **[同步化使用者密碼]**。預設的同步化使用者密碼工作流程接受來自 JMS 偵聽程式介面的每個請求，出庫使用 ChangeUserPassword 檢視器，然後再將 ChangeUserPassword 檢視器入庫納管。
6. 在 **[記錄檔路徑]** 方塊中，指定要在其中建立使用中與已歸檔記錄檔的目錄路徑。
7. 若爲除錯目的，請將 **[記錄層級]** 設定爲 **[4]** 以產生詳細的記錄。
8. 按一下 **[儲存]**。

測試您的配置

您可以使用 Windows PasswordSync 配置應用程式來對 Windows 端的配置執行除錯。

若要測試 PasswordSync 配置，請執行以下步驟：

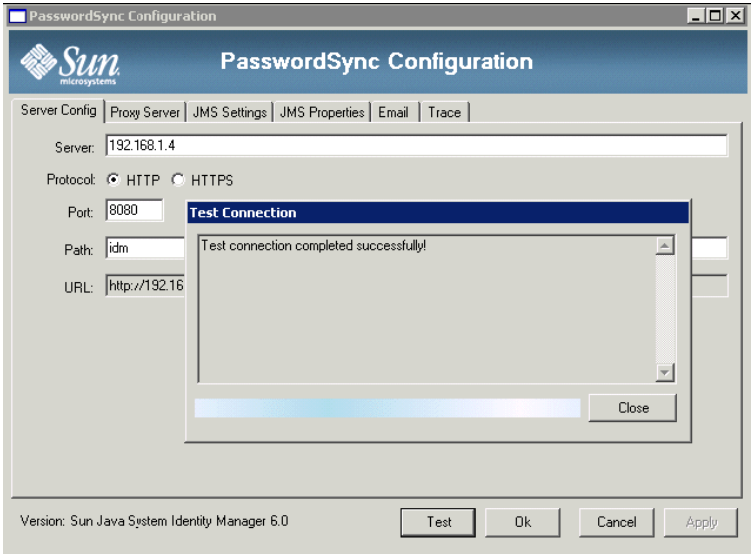
1. 如果尚未執行 PasswordSync 配置應用程式，請將其啓動。

   依預設，此配置應用程式安裝在 [Program Files] > Sun Identity Manager PasswordSync > [配置] 中。

2. 顯示 [PasswordSync 配置] 對話方塊時，按一下 **[測試]** 按鈕。

3. 若使用 JMS，將會顯示 [測試連線] 對話方塊 (圖 11-16)，其中包含一條訊息表明測試連線是否成功完成。

圖 11-16　[測試連線] 對話方塊

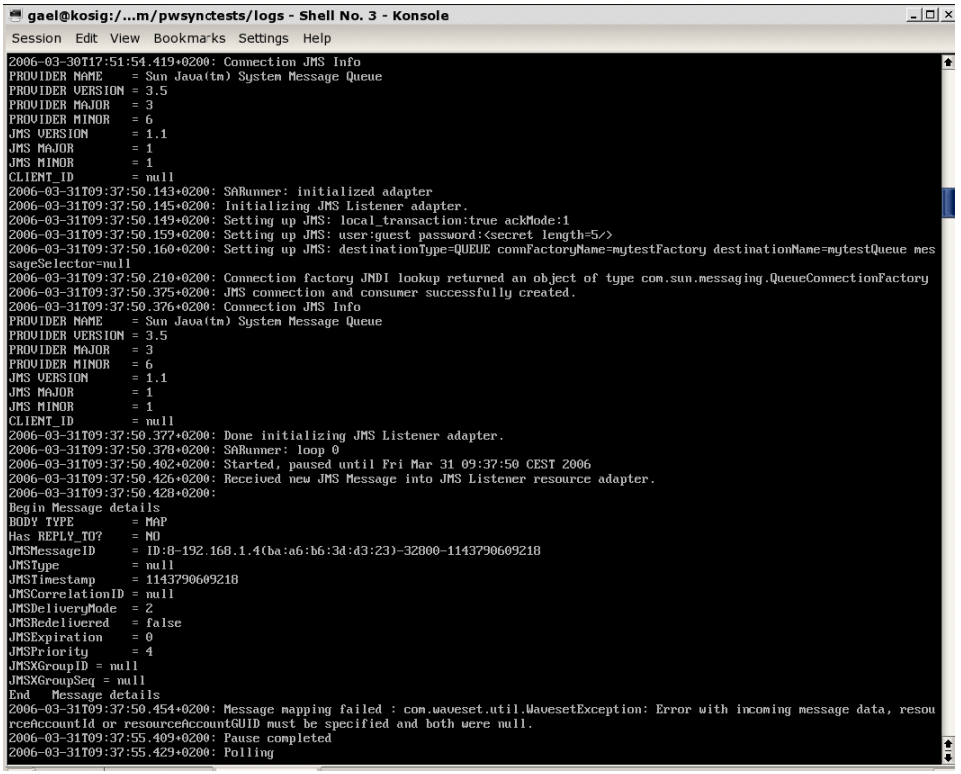


4. 按一下 **[關閉]** 以關閉 [測試連線] 對話方塊。

5. 按一下 **[確定]** 以關閉 [PasswordSync 配置] 對話方塊。

   然後 JMS 偵聽程式介面將會以除錯模式執行，並在檔案中產生除錯資訊，與圖 11-17 所示相似。

圖 11-17　除錯資訊檔案



相關常見問題 PasswordSync

是否可以不使用 Java Messaging Service 而實作 PasswordSync？

可以，但這種做法會犧牲使用 JMS 追蹤密碼變更事件的好處。

若要不使用 JMS 而實作 PasswordSync，請以下列旗標啓動配置應用程式：

```
Configure.exe -direct
```

若指定 `-direct` 旗標，配置應用程式會隨即顯示 [使用者] 標籤。

若您不使用 JMS 而實作 PasswordSync，則無需建立 JMS 偵聽程式介面。因此，請略過第 398 頁的「在應用程式伺服器上部署 PasswordSync」中所列的程序。若要設定通知，可能必須改變 [變更使用者密碼] 工作流程。

備註 如果您隨後在未指定 `-direct` 旗標的情況下執行配置應用程式，則必須在配置 JMS 後方可執行 PasswordSync。請使用 `-direct` 旗標重新啓動應用程式，以便再次略過 JMS。

PasswordSync 是否可以與其他用於強制自訂密碼策略的 Windows 密碼篩選器配合使用？

是的，您可以將 PasswordSync 與其他 _WINDOWS_ 密碼篩選器配合使用。然而，必須是 [通知套裝軟體] 登錄值中列出的最後一個密碼篩選器。

您必須使用以下登錄路徑：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification
Packages （類型 REG_MULTI_SZ 的值）
```

依預設，安裝程式將 Identity Manager 密碼截取置於清單結尾。但是，如果您在安裝該軟體後安裝自訂密碼篩選器，則需要將 `lhpwic` 移至 [通知套裝軟體] 清單的結尾。

您可以將 PasswordSync 與其他 Identity Manager 密碼策略配合使用。在 Identity Manager 伺服器端檢查策略時，必須傳送所有資源密碼策略，才可以將密碼同步化推出至其他資源。因此，您應使 Windows 本機密碼策略具有與 Identity Manager 中定義的大多數限制性密碼策略同等的限制性。

備註 密碼截取 DLL 不會強制執行任何密碼策略。

是否可以將 PasswordSync Servlet 安裝在 Identity Manager 以外的其他應用伺服器上？

可以。除了 JMS 應用程式需要的所有 JAR 檔案之外，PasswordSync Servlet 還需要 JAR 檔案 `spml.jar` 和 `idmcommon.jar`。

PasswordSync 服務是否將密碼以明文傳送至 lh 伺服器？

雖然我們建議透過 SSL 執行 PasswordSync，但是在傳送至 Identity Manager 伺服器之前，所有敏感資料都是加密的。

如需相關資訊，請參閱第 388 頁的 「配置 PasswordSync 使用 SSL」。

有時密碼變更會導致 com.waveset.exception.ItemNotLocked？

如果啓用 PasswordSync，密碼變更 (即使從使用者介面啓動) 會使資源的密碼發生變更，而這會導致資源與 Identity Manager 連絡。

如果正確配置 `passwordSyncThreshold` 工作流程變數，則 Identity Manager 將檢查使用者物件並確定該使用者物件已處理密碼變更。但是，如果使用者或管理員同時對同一使用者進行其他密碼變更，則使用者物件將被鎖定。

第 12 章

安全性

本章提供有關 Identity Manager 安全性功能的資訊，並詳細說明您可以採取以進一步降低安全性風險的步驟。

檢閱下列主題以瞭解有關使用 Identity Manager 管理系統安全性的詳細資訊。

安全性功能

Identity Manager 可透過提供以下功能來協助降低安全性風險：

- 即時停用帳號存取 - Identity Manager 讓您透過單一動作即可停用組織或個人的存取權限。
- 登入階段作業限制 - 您可以設定對同步運作之登入階段作業的限制。
- 使用中的風險分析 - Identity Manager 會經常掃描是否有非使用中的帳號及可疑密碼作業等安全性風險。
- 全面的密碼管理 - 完整且靈活的密碼管理權能可確保能夠實施完整的存取控制。
- 監視存取作業的稽核與報告 - 您可以執行各類報告來提供有關存取作業的有針對性的資訊 (請參閱第 8 章「報告」以取得有關報告功能的更多資訊)。
- 細化管理權限控制 - 您可以爲使用者指定單一權能，或指定一系列透過管理員角色定義的管理責任，從而在 Identity Manager 中授予管理控制並進行管理。
- 伺服器金鑰加密 ñ Identity Manager 可讓您透過 [作業] 區域建立與管理伺服器加密金鑰。

此外，系統架構也會儘可能地尋求降低安全性風險的機會。例如，登出後即無法透過瀏覽器的 [上一頁] 功能存取先前造訪過的頁面。

限制同步運作的登入階段作業

依預設，Identity Manager 使用者可以具有同步運作的登入階段作業。不過，您可以開啓系統配置物件進行修改 (第 197 頁) 並編輯 `security.authn.singleLoginSessionPerApp` 配置屬性的值，以將同步運作的階段作業限制爲每一個登入應用程式一個階段作業。該屬性是包含每個登入應用程式名稱 (例如，管理員介面、使用者介面或 Identity Manager IDE) 的一個屬性的物件。將此屬性的值變更爲 `true`，即可強制每個使用者採用單一登入階段作業。

如果已執行，則使用者可登入至多個階段作業；但只有最後的登入階段作業保持爲使用中且有效。如果使用者對無效的階段作業執行動作，則會自動被迫離開階段作業並終止階段作業。

密碼管理

Identity Manager 在多個層級提供密碼管理：

- **管理變更管理**
  - 從多個位置 (**[編輯使用者]**、**[尋找使用者]** 或 **[變更密碼]** 頁面) 變更使用者密碼
  - 在任何一個可進行細化資源選取的使用者資源上變更密碼
- **管理密碼重設**
  - 產生隨機密碼
  - 對一般使用者或管理員顯示密碼
- **使用者變更密碼**
  - 透過以下 URL 爲一般使用者提供密碼變更自助功能

    http://localhost:8080/idm/user
  - 您可以選擇自訂自助網頁，使其符合一般使用者的環境
- **使用者更新資料**
  - 設定一般使用者管理的任何使用者模式屬性
- **使用者存取回復**
  - 使用認證答案授與使用者變更其密碼的存取權限
  - 使用通過式認證授與使用者藉由使用幾個密碼之一進行存取的權限
- **密碼策略**
  - 使用規則定義密碼參數

通過式認證

使用通過式認證授予使用者和管理員透過一個或多個不同密碼進行存取的權限。Identity Manager 透過實作以下內容來管理認證：

- 登入應用程式 (登入模組群組的集合)
- 登入模組群組 (登入模組的有序集合)
- 登入模組 (爲每個指定的資源設定認證，並指定多個認證成功需求之一)

關於登入應用程式

登入應用程式定義登入模組群組的集合，登入模組群組進一步定義使用者登入 Identity Manager 時所使用之登入模組的集合和順序。每個登入應用程式均包括一個或多個登入模組群組。

登入時，登入應用程式會檢查登入模組群組集。如果只設定一個登入模組群組，則會使用該群組，且它所包含的登入模組會以群組定義的順序處理。如果登入應用程式中包含多個已定義的登入模組群組，則 Identity Manager 會檢查套用至每個登入模組群組的登入限制規則，以確定要處理哪個群組。

登入限制規則

登入限制規則會套用至登入模組群組。對於每一個在登入應用程式中登入的模組群組，只有一個群組是無法讓登入限制規則套用的。

Identity Manager 會計算第一個登入模組群組的限制規則，以決定要處理一個集合中的哪一個登入模組群組。如果成功，則會處理該登入模組群組。如果失敗，則它會輪流計算每個登入模組群組，直到某個限制規則成功或是已經計算發現某個不包含限制規則的登入模組群組 (並在隨後使用)。

備註 如果登入應用程式包含多個登入模組群組，則沒有登入限制規則的登入模組群組應放在模組集的最後一個位置。

登入限制規則範例

在下列位置型登入限制規則範例中，規則會從 HTTP 標頭中取得請求程式的 IP 位址，然後檢查它是否位於 192.168 網路上。如果在 IP 位址中找到 192.168.，則規則將傳回 true 值，並且會選取此登入模組群組。

編碼樣例 12-1 基於位置的登入限制規則

```
<Rule authType='LoginConstraintRule' name='Sample On Local Network'>
  <match>
    <ref>remoteAddr</ref>
    <s>192.168.</s>
  </match>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' name='All'/>
  </MemberObjectGroups>
</Rule>
```

編輯登入應用程式

從功能表列選取 **[安全性]**，然後選取 **[登入]** 以存取 [登入] 頁面。

登入應用程式清單顯示：

- 每一個定義的 Identity Manager 登入應用程式 (介面)
- 包含登入應用程式的登入模組群組
- 針對各登入應用程式所設定的 Identity Manager 階段作業逾時限制

從 [登入] 頁面中，您可以：

- 建立自訂登入應用程式
- 刪除自訂登入應用程式
- 管理登入模組群組

若要編輯某登入應用程式，請從清單中選取該應用程式。

設定 Identity Manager 階段作業限制

在 [修改登入應用程式] 頁面中，您可以爲每個 Identity Manager 登入階段作業設定逾時值 (限制)。選取時、分和秒數後，再按一下 **[儲存]**。您建立的限制會顯示在登入應用程式清單中。

您可以設定每個 Identity Manager 登入應用程式的階段作業逾時。當使用者登入 Identity Manager 應用程式時，即會使用目前配置的階段作業逾時值，計算使用者階段作業因未作業而將在未來哪個日期與時間逾時。接著，計算出來的日期會儲存在使用者的 Identity Manager 階段作業中，以便在每次提出請求時可供檢查。

若登入管理員變更了登入應用程式階段作業逾時值，則該值對未來所有的登入作業都將有效。現有階段作業的逾時值將取決於使用者登入時的有效值。

針對 HTTP 逾時所設定的值會影響所有 Identity Manager 應用程式，而且優先於登入應用程式階段作業的逾時值。

停用對應用程式的存取

從 [建立登入應用程式] 和 [修改登入應用程式] 頁面，您可以選取 [停用] 選項以停用登入應用程式，從而阻止使用者登入。若使用者嘗試登入已停用的應用程式，則會將使用者重新導向至替代頁面，說明應用程式目前已停用。您可以透過編輯自訂目錄來編輯顯示在此頁面上的訊息。

在您取消選取該選項之前，登入應用程式將保持停用狀態。爲安全起見，您無法停用管理員登入。

編輯登入模組群組

登入模組群組清單顯示：

- 每個登入模組群組
- 組成登入模組群組的個別登入模組
- 登入模組群組是否包含限制規則

在 [登入模組群組] 頁面中，您可以建立、編輯和刪除登入模組群組。請從清單中選取登入模組群組，以進行編輯。

編輯登入模組

如下輸入登入模組的詳細資訊或進行選取 (不是所有選項都可用於每個登入模組)。

- **登入成功條件** - 選取適用於此模組的需求。選項包括：
  - **必要** - 此登入模組爲成功認證的必要模組。無論認證是成功或失敗，認證程序都會進行清單中的下一個登入模組。如果僅有一個登入模組，則管理員可成功登入。
  - **必需** - 此登入模組爲成功認證的必要模組。如果認證成功，則認證程序會進行清單中的下一個登入模組。如果失敗，則認證將不會繼續進行。
  - **足夠** - 此登入模組不是成功認證的必要模組。如果認證成功，則認證程序並不會繼續進行下一個登入模組，但管理員可成功登入。如果認證失敗，則認證會繼續進行清單上的下一個登入模組。
  - **選擇性** - 此登入模組不是成功認證的必要模組。無論認證是成功或失敗，認證程序都會繼續清單中的下一個登入模組。
- **登入搜尋屬性** - (僅限 LDAP)。指定要在嘗試連結 (登入) 至相關聯的 LDAP 伺服器時，使用的已排序 LDAP 使用者屬性名稱清單。每一個指定的 LDAP 使用者屬性，連同使用者指定的登入名稱，可用於搜尋相符的 LDAP 使用者 (依序)。如此可在將 Identity Manager 配置爲傳遞至 LDAP 時，允許使用者使用 LDAP cn 或電子郵件地址登入 Identity Manager。

  例如，如果您指定：

  ```
  cn
  mail
  ```

  而使用者嘗試以 `gwilson` 登入，則 LDAP 資源將首先嘗試尋找 `cn=gwilson` 的 LDAP 使用者。如果成功，則會嘗試使用由使用者指定的密碼登入。如果不成功，則 LDAP 資源將搜尋 `mail=gwilson` 的 LDAP 使用者。如果還是失敗，則無法登入。

  如果未指定值，則預設 LDAP 搜尋屬性爲：

  ```
  uid
  cn
  ```

- **登入相互關聯規則** - 選取登入相互關聯規則，以用於將使用者所提供的登入資訊對映至 Identity Manager 使用者。使用規則中所指定的邏輯，可將此規則用於搜尋 Identity Manager 使用者。規則必須傳回一個或多個用於搜尋符合該規則的 Identity Manager 使用者的 AttributeConditions。選取的規則必須具有 `LoginCorrelationRule` authType。如需有關 Identity Manager 用以對映認證使用者 ID 與 Identity Manager 使用者之步驟的說明，請參閱第 429 頁的「登入模組處理邏輯」。
- **新的使用者名稱規則** - 選取在登入過程中自動建立新的 Identity Manager 使用者時，所使用的新使用者命名規則。

按一下 **[儲存]** 以儲存登入模組。儲存之後，就可以決定此模組與登入模組群組中所有其他模組的相對位置。

警告

如果將 Identity Manager 登入配置爲可透過認證登入多個系統，則爲 Identity Manager 認證目標的所有系統上，帳號的使用者 ID 和密碼皆需相同。

如果使用者 ID 和密碼的組合不同，則如果登入系統時的使用者 ID 和密碼與 Identity Manager [登入使用者] 表單中所輸入者不相符，登入將會失敗。

其中某些系統具有鎖住策略，可強制執行失敗登入嘗試次數策略，一旦超過即需鎖定帳號。在這些系統中，即便使用者透過 Identity Manager 登入持續成功，最終仍將鎖定使用者帳號。

登入模組處理邏輯

編碼樣例 12-2 包含虛擬程式碼，說明 Identity Manager 用以對映認證使用者 ID 與 Identity Manager 使用者的步驟。

編碼樣例 12-2 說明登入模組處理邏輯的虛擬程式碼

```
if an existing IDM user's ID is the same as the specified user ID

   if that IDM user has a linked resource whose resource name matches the
   resource that was authenticated and whose accountId matches the resource
   accountId returned by successful authentication (e.g. dn), then we have
   found the right IDM user

   otherwise if there is a LoginCorrelationRule associated with the
   configured login module

      evaluate it to see if it maps the login credentials to a single IDM
      user

      otherwise login fails

   otherwise login fails

if the specified userID does not match an existing IDM user's ID

   try to find an IDM user that has a linked resource whose resource name
   matches the resource accountID returned by successful authentication

      if found, then we have found the right IDM user

      otherwise if there is a LoginCorrelationRule associated with the
      configured login module

         evaluate it to see if it maps the login credentials to a single
         IDM user

         otherwise login fails

      otherwise login fails
```

在編碼樣例 12-2 中，系統會嘗試使用使用者的連結資源 (資源資訊)，尋找相符的 Identity Manager 使用者。然而，如果資源資訊方式失敗但已配置 loginCorrelationRule，則系統會嘗試使用 loginCorrelationRule 尋找相符的使用者。

配置共用資源的認證

若有多個邏輯上相同的資源 (例如共用信任關係的多部 Active Directory 網域伺服器)，或有多個位於相同實體主機上的資源，則可以指定這些資源是共用資源。

您應該宣告共用資源，讓 Identity Manager 知道它一次只應該嘗試驗證一組資源。否則，若使用者鍵入錯誤的密碼，則 Identity Manager 會嘗試針對每個資源使用相同的密碼。這樣即使使用者只鍵入一次錯誤的密碼，也會因多次登入失敗而鎖定使用者的帳號。

運用共用資源，使用者可以向一個共用資源進行認證，而 Identity Manager 會自動嘗試將使用者對映至共用資源群組中其餘的資源。例如，Identity Manager 使用者帳號可能會連結至資源 AD-1 的資源帳號。但登入模組群組可能會定義使用者必須向資源 AD-2 進行認證。

若 AD-1 和 AD-2 定義爲共用資源 (在此情況下，是位於相同的信任的網域中)，則若使用者向 AD-2 認證成功，Identity Manager 只要在資源 AD-1 上尋找相同的使用者帳號 ID，也可以將使用者對映至 AD-1。

備註 所有列在共用資源群組中的資源，也必須併入登入模組定義中。若完整的共用資源清單也未出現在登入模組定義中，則共用資源功能將無法正確運作。

您可以使用下列格式，將共用資源定義於 「系統配置」物件中 (第 197 頁)：

編碼樣例 12-3 配置共用資源的認證

```
<Attribute name=common resources>
    <Attribute name=Common Resource Group Name>
        <List>
            <String>Common Resource Name</String>
            <String>Common Resource Name</String>
        </List
    </Attribute>
</Attribute>
```

配置 X509 憑證認證

使用下列資訊和程序配置 Identity Manager 的 X509 憑證認證。

必要條件

若要在 Identity Manager 中支援基於 X509 憑證的認證，請確定已正確配置雙向 (用戶端與伺服器) SSL 認證。從用戶端的角度，這表示符合 X509 規範的使用者憑證應已匯入瀏覽器中 (或可透過智慧卡讀取器使用)，而用於簽署使用者憑證的可信任憑證應已匯入 Web 應用程式伺服器的可信任憑證金鑰存放區中。

此外，必須啓用所使用的用戶端憑證，進行用戶端認證。

若要確認是否已選取用戶端憑證的用戶端認證選項，請執行以下步驟：

1. 使用 Internet Explorer，選取 **[工具]**，然後選取 **[網際網路選項]**。
2. 選取 **[內容]** 標籤。
3. 在 [憑證] 區域中，按一下 **[憑證]**。
4. 選取用戶端憑證，然後按一下 **[進階]**。
5. 在 [憑證目的] 區域中，確認選取 [用戶端認證] 選項。

配置 Identity Manager 中 X509 憑證認證

若要配置 Identity Manager 進行 X509 憑證認證，請執行以下步驟：

1. 以 [配置人] 的身份 (或具同等權限的身份) 登入 [管理員介面]。
2. 選取 **[配置]**，然後選取 **[登入]**，以顯示 [登入] 頁面。
3. 按一下 **[管理登入模組群組]**，以顯示 [登入模組群組] 頁面。
4. 在清單中選取登入模組群組。
5. 在 [指定登入模組...] 清單中，選取 [識別系統 X509 憑證登入模組]。Identity Manager 會顯示 [修改登入模組] 頁面。
6. 設定登入成功需求。可接受的值如下：
   - **必要** - 此登入模組爲成功認證的必要模組。無論認證是成功或失敗，認證程序都會進行清單中的下一個登入模組。如果僅有一個登入模組，則管理員可成功登入。
   - **必需** - 此登入模組爲成功認證的必要模組。如果認證成功，則認證程序會進行清單中的下一個登入模組。如果失敗，則認證將不會繼續進行。
   - **足夠** - 此登入模組不是成功認證的必要模組。如果認證成功，則認證程序並不會繼續進行下一個登入模組，但管理員可成功登入。如果認證失敗，則認證會繼續進行清單上的下一個登入模組。
   - **選擇性** - 此登入模組不是成功認證的必要模組。無論認證是成功或失敗，認證程序都會繼續清單中的下一個登入模組。
7. 選取登入相互關聯規則。此規則可以是內建的規則或自訂相互關聯規則。(請參閱下節獲得有關建立自訂相互關聯規則的資訊)。
8. 按一下 **[儲存]** 返回 [修改登入模組群組] 頁面。
9. 或者，重新安排登入模組的順序 (如果登入模組群組中已指定多個登入模組)，然後按一下 **[儲存]**。
10. 如果尚未指定，則將登入模組群組指定給登入應用程式。在 [登入模組群組] 頁面上，按一下 [返回登入應用程式]，再選取登入應用程式。將登入模組群組指定給應用程式後，按一下 **[儲存]**。

備註 如果將 waveset.properties 檔案中的 allowLoginWithNoPreexistingUser 選項設定爲 true 值，則當配置 Identity Manager X509 憑證登入模組時，系統會提示您選取 [新的使用者名稱規則]。此規則用於確定如何命名相關的登入相互關聯規則找不到使用者時建立的新使用者。

[新的使用者名稱規則] 可用的輸入引數與 [登入相互關聯規則] 相同。它會傳回單一字串，此字串會成爲用於建立新 Identity Manager 使用者帳號的使用者名稱。

在 idm/sample/rules 中含有新使用者名稱規則的範例，名稱爲 NewUserNameRules.xml。

建立並匯入登入相互關聯規則

Identity Manager X509 憑證登入模組會使用登入相互關聯規則，決定如何將憑證資料對映至適當的 Identity Manager 使用者。Identity Manager 包含內建相互關聯規則，名稱爲 Correlate via X509 Certificate subjectDN。

您也可以增加您自己的關聯規則。請參閱位於 idm/sample/rules 目錄中的 LoginCorrelationRules.xml 當作範例。每一個相互關聯規則必須遵守這些指導原則：

- 其 authType 屬性必須設爲 LoginCorrelationRule。
- 預期傳回 AttributeConditions 清單的實例，登入模組會使用此實例找到相關的 Identity Manager 使用者。例如，登入相互關聯規則可能傳回 AttributeCondition，它會根據電子郵件地址搜尋相關的 Identity Manager 使用者。

傳遞至登入相互關聯規則的引數如下：

- 標準 X509 憑證欄位 (例如 subjectDN、issuerDN 和有效日期)
- 關鍵和非關鍵性的延伸特性

傳遞至登入相互關聯規則的憑證引數的命名慣例：

```
cert.field name.subfield name
```

以下爲規則可以使用的引數名稱範例：

- cert.subjectDN
- cert.issuerDN
- cert.notValidAfter
- cert.notValidBefore
- cert.serialNumber

使用傳入引數的登入相互關聯規則，會傳回一個或多個 AttributeConditions 的清單。[識別系統 X509 憑證登入模組] 會使用這些清單找到相關的 Identity Manager 使用者。

在 idm/sample/rules 中包含登入相互關聯規則的範例，名爲 LoginCorrelationRules.xml。

建立自訂相互關聯規則後，您必須將它匯入 Identity Manager。從 [管理員介面] 中選取 **[配置]**，然後選取 **[匯入交換檔案]**，以使用檔案匯入功能。

測試 SSL 連線

若要測試 SSL 連線，請透過 SSL 連線到配置的應用程式介面之 URL (例如 https://idm007:7002/idm/user/login.jsp)。您會被告知您將進入安全的網站，並提示您指定要傳送給 Web 伺服器的個人憑證。

診斷問題

透過 X509 憑證而發生的認證問題會在登入表單上以錯誤訊息的形式報告。如需完整的診斷，請在 Identity Manager 伺服器上對於以下類別和層級進行追蹤：

- `com.waveset.session.SessionFactory 1`
- `com.waveset.security.authn.WSX509CertLoginModule 1`
- `com.waveset.security.authn.LoginModule 1`

若用戶端憑證屬性在 HTTP 請求中的名稱不是 `javaxservlet.request.X509Certificate`，則會收到一則訊息，指出在 HTTP 請求中找不到此屬性。

若要更正這個問題：

1. 啓用 `SessionFactory` 的追蹤，以查看完整的 HTTP 屬性清單，並找出 X509 憑證的名稱。
2. 使用 Identity Manager 除錯設備 (第 59 頁) 編輯 `LoginConfig` 物件。
3. 將 Identity Manager X509 憑證登入模組之 `<LoginConfigEntry>` 中的 `<AuthnProperty>` 的名稱變更爲正確名稱。
4. 儲存，然後重試。

您可能還需要先移除，然後再重新增加登入應用程式中的 Identity Manager X509 憑證登入模組。

加密使用和管理

加密用於確保記憶體和儲存庫中伺服器資料以及在伺服器和閘道之間傳輸的所有資料的機密性和完整性。

以下各節提供了有關如何在 Identity Manager 伺服器和閘道中使用和管理加密的更多資訊，並闡述了有關伺服器和閘道加密金鑰的問題。

受加密保護的資料

下表顯示了在 Identity Manager 產品中受加密保護的資料類型，包括用於保護每種類型資料的密碼。

表 12-1 受加密保護的資料類型

資料類型	RSA MD5	NIST Triple DES 168 位元金鑰 (DESede/ECB/NoPadding)	PKCS#5 基於密碼的加密 56 位元金鑰 (PBEwithMD5andDES)
伺服器加密金鑰		預設	配置選項[1]
閘道加密金鑰		預設	配置選項 [1]
策略字典字詞	是		
使用者密碼		是	
使用者密碼歷程記錄		是	
使用者回覆		是	
資源密碼		是	
資源密碼歷程記錄	是		
伺服器和閘道之間的所有有效負載		是	

1. 透過系統配置物件 (第 197 頁) 的 pbeEncrypt 屬性或 [管理伺服器加密] 作業進行配置。

伺服器加密金鑰問題與回覆

請閱讀以下各節，以取得有關伺服器加密金鑰來源、位置、維護和使用的常見問題的回覆。

伺服器加密金鑰來自何處？

伺服器加密金鑰是對稱的 triple-DES 168 位元金鑰。伺服器支援兩種類型的金鑰：

- **預設金鑰** - 此金鑰已編譯爲伺服器代碼。
- **隨機產生的金鑰** - 此金鑰可以在伺服器初始啓動時、或在目前金鑰可能出現安全性問題時產生。

在何處維護伺服器加密金鑰？

伺服器加密金鑰是在儲存庫中維護的物件。在任何給定儲存庫中都會有許多資料加密金鑰。

伺服器如何知道使用哪個金鑰對已加密資料進行解密和重新加密？

儲存在儲存庫中的每一份加密資料都以伺服器加密金鑰 (用於加密該資料) 的 ID 爲前綴。將包含加密資料的物件讀入記憶體後，Identity Manager 會使用與加密資料的 ID 前綴關聯的伺服器加密金鑰進行解密，然後使用相同的金鑰重新加密 (如果資料已變更)。

如何更新伺服器加密金鑰？

Identity Manager 提供了名爲「管理伺服器加密」的作業。此作業允許經授權的安全管理員執行多項金鑰管理作業，包括：

- 產生新的「目前」伺服器金鑰
- 依類型重新加密包含帶有「目前」伺服器金鑰的已加密資料的現有物件

請參閱本章中的「管理伺服器加密」，以取得有關如何使用此作業的更多資訊。

如果變更「目前」伺服器金鑰，會對現有加密資料造成什麼影響？

沒有影響。仍將使用加密資料的 ID 前綴參照的金鑰對現有加密資料進行解密或重新加密。如果產生新的伺服器加密金鑰並設定爲「目前」金鑰，則任何要加密的新資料都將使用該伺服器金鑰。

爲避免發生多金鑰問題以及爲維護更高層級的資料完整性，請使用 [管理伺服器加密] 作業對所有具有「目前」伺服器加密金鑰的現有加密資料重新加密。

當您匯入的加密資料沒有加密金鑰可用時，會發生什麼狀況？

若您將含有加密資料的物件匯入至儲存庫，但加密該資料時所使用的金鑰並不在此儲存庫中，則資料仍可匯入，但無法進行解密。

如何保護伺服器金鑰？

如果伺服器未配置爲使用密碼加密 (PBE) - PKCS#5 加密 (透過 `pbeEncrypt` 屬性或 [管理伺服器加密] 作業在系統配置物件中設定)，則使用預設金鑰加密伺服器金鑰。對於安裝的所有 Identity Manager，預設金鑰都是相同的。

如果伺服器配置爲使用 PBE 加密，則每次啓動伺服器時都會產生一個 PBE 金鑰。透過提供一個密碼 (從伺服器特定的秘密產生) 作爲 PBEwithMD5andDES 密碼來產生 PBE 金鑰。PBE 金鑰僅在記憶體中維護，並且從不具有永久性。另外，PBE 金鑰對於共用一個共同儲存庫的所有伺服器都是相同的。

若要啓用伺服器金鑰的 PBE 加密，密碼 PBEwithMD5andDES 必須可用。依預設，Identity Manager 不包含此密碼，但此密碼採用 PKCS#5 標準，許多 JCE 提供者實作 (例如 Sun 和 IBM 提供的實作) 中都提供了該標準。

我可以匯出伺服器金鑰以安全地儲存在外部嗎？

可以。如果伺服器金鑰是 PBE 加密的，則在匯出之前，將使用預設金鑰對其進行解密和重新加密。這使得它們可以獨立於本機伺服器 PBE 金鑰而被稍後匯入相同或其他伺服器中。如果使用預設金鑰加密伺服器金鑰，則在匯出之前不需要任何預先處理。

將金鑰匯入伺服器後，如果該伺服器配置爲使用 PBE 金鑰，則將解密這些金鑰。然後，如果該伺服器配置爲使用 PBE 金鑰加密，則將使用本機伺服器的 PBE 金鑰重新加密這些金鑰。

哪些資料會在伺服器和閘道之間進行加密？

在伺服器和閘道之間傳輸的所有資料 (有效負載) 都由針對伺服器-閘道階段作業隨機產生的對稱 168 位元金鑰進行 triple-DES 加密。

閘道金鑰問題與回覆

請閱讀以下各節，以取得有關閘道來源、儲存、分發和保護的常見問題的回覆。

加密或解密資料的閘道金鑰來自何處？

每次 Identity Manager 伺服器連線至閘道時，初始訊號交換都將產生新的隨機 168 位元 triple-DES 階段作業金鑰。此金鑰將用於加密或解密所有在該伺服器和該閘道之間傳輸的後續資料。對於每個伺服器/閘道對，產生的階段作業金鑰都是唯一的。

如何將閘道金鑰分發至閘道？

階段作業金鑰由伺服器隨機產生，然後在伺服器和閘道之間安全地進行交換，方法是使用作爲初始伺服器至閘道訊號交換的一部分的共用秘密主金鑰對階段作業金鑰進行加密。

在初始訊號交換時，伺服器會查詢閘道以確定閘道支援的模式。閘道可以在兩種模式中作業

- **預設模式** -使用已編譯爲伺服器代碼的預設 168 位元 triple-DES 金鑰，對伺服器至閘道的初始協定訊號交換進行加密。
- **安全模式** -針對每個共用儲存庫產生一個隨機 168 位元 triple-DES 閘道金鑰，並作爲初始信號交換協定的一部分用於在伺服器和閘道之間進行通訊。此閘道金鑰像其他加密金鑰一樣儲存在伺服器儲存庫中，並儲存在閘道的本機登錄中。

  伺服器在安全模式中連絡閘道時，伺服器將使用閘道金鑰加密測試資料並將其傳送至閘道。然後，閘道將嘗試解密測試資料，將一些閘道唯一資料增加至測試資料，重新加密這些資料，並將資料傳回伺服器。如果伺服器可以成功解密測試資料和閘道唯一資料，則伺服器將產生伺服器-閘道唯一階段作業金鑰，使用閘道金鑰對其進行加密並將其傳送至閘道。收到之後，閘道將解密階段作業金鑰並將其保留，以供在伺服器至閘道階段作業中使用。如果伺服器無法成功解密測試資料和閘道唯一資料，則伺服器將使用預設金鑰加密閘道金鑰並將其傳送至閘道。閘道將使用在預設金鑰中編譯的閘道金鑰解密閘道金鑰，並將該閘道金鑰儲存在其登錄中。然後，伺服器將使用閘道金鑰加密伺服器-閘道唯一階段作業金鑰並將其傳送至閘道，以供在伺服器至閘道階段作業中使用。

  之後，閘道將僅接受來自已使用其閘道金鑰加密階段作業金鑰的伺服器的請求。啓動時，閘道將檢查登錄中是否有金鑰。如果有，則使用它。如果沒有，則使用預設金鑰。閘道在登錄中設定金鑰後，將不再允許使用預設金鑰建立階段作業。這將阻止某些人設定惡意伺服器和建立至閘道的連線。

我可以更新用於加密或解密伺服器至閘道有效負載的閘道金鑰嗎？

Identity Manager 提供了名爲「管理伺服器加密」的作業，其允許經授權的安全管理員執行多項金鑰管理作業，包括產生新的「目前」閘道金鑰和使用該「目前」閘道金鑰更新所有閘道。這是用於加密每個階段作業金鑰 (用於保護在伺服器和閘道之間傳輸的所有有效負載) 的金鑰。根據系統配置 (第 197 頁) 中的 `pbeEncrypt` 屬性值，使用預設金鑰或 PBE 金鑰來加密新產生的閘道金鑰。

閘道金鑰儲存在伺服器、閘道的什麼地方？

在伺服器上，閘道金鑰就像伺服器金鑰一樣儲存在儲存庫中。在閘道上，閘道金鑰儲存在本機登錄機碼中。

如何保護閘道金鑰？

保護閘道金鑰的方式與保護伺服器金鑰的方式相同。如果伺服器配置爲使用 PBE 加密，則將使用 PBE 產生的金鑰加密閘道金鑰。如果該選項爲 False，則將使用預設金鑰對其進行加密。請參閱前述標題爲「如何保護伺服器金鑰？」的章節，以取得更多資訊。

我可以匯出閘道金鑰以安全地儲存在外部嗎？

可以透過「管理伺服器加密」作業匯出閘道金鑰，就像匯出伺服器金鑰一樣。請參閱前述標題爲「我可以匯出伺服器金鑰以安全地儲存在外部嗎？」的章節，以取得更多資訊。

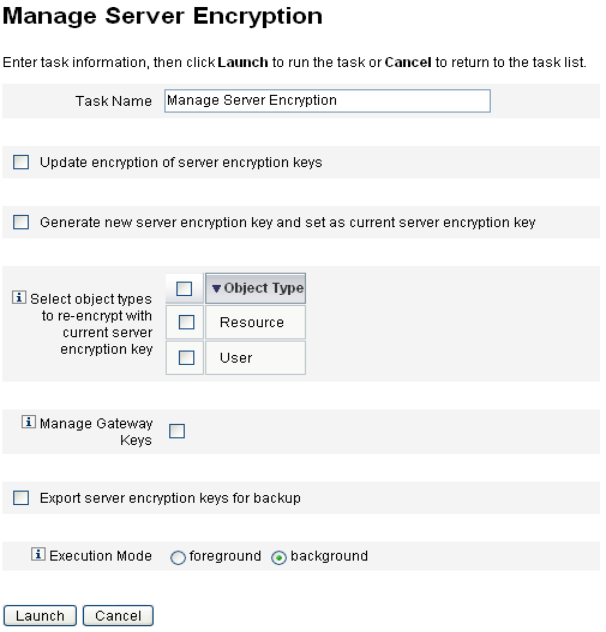
如何銷毀伺服器和閘道金鑰？

透過從伺服器儲存庫中刪除伺服器和閘道金鑰即可將其銷毀。請註意，只要仍在使用某金鑰加密伺服器資料或仍有閘道依賴於該金鑰，就不應該刪除該金鑰。使用「管理伺服器加密」作業重新加密所有具有目前伺服器金鑰的伺服器資料，並同步化目前的閘道金鑰與所有閘道，以確保在刪除任何舊的金鑰之前未在使用該舊金鑰。

管理伺服器加密

Identity Manager 伺服器加密功能可讓您建立新的 3DES 伺服器加密金鑰，然後使用 3DES 或 PKCS#5 加密對這些金鑰進行加密，如下圖所示。只有具有安全管理員權能的使用者才可以執行 [管理伺服器加密] 作業 (從 **[伺服器作業]** 標籤存取此作業)。

圖 12-1　管理伺服器加密作業



選取 **[執行作業]**，然後從清單中選取 [管理伺服器加密]，以爲此作業配置以下資訊：

- **更新伺服器加密金鑰的加密** - 選取此選項即可指定使用預設方法 (即 3DES) 加密，還是使用或 PKCS#5 加密對伺服器加密金鑰進行加密。當您選取此選項時，會出現兩個加密選項 (預設值和 PKCS#5)；請選擇其中之一。
- **產生新的伺服器加密金鑰，並將其設爲目前的伺服器加密金鑰** - 選取此選項可產生新的伺服器加密金鑰。在您選取此選項後所產生的每一部分加密資料，都將使用此金鑰進行加密。產生新的伺服器加密金鑰，並不會影響套用至現有加密資料的金鑰。
- **選取要以目前伺服器加密金鑰來重新加密的物件類型** - 選取一個或多個 Identity Manager 物件類型 (如資源或使用者)，以使用目前的加密金鑰重新加密。

- **管理閘道金鑰** - 選取此選項後，頁面會顯示下列閘道金鑰選項：
  - **產生新金鑰並同步化所有閘道**
    初始啓用安全閘道環境時選取此選項。此選項會產生新的閘道金鑰，並傳送給所有閘道。
  - **使用目前的閘道金鑰同步化所有閘道**
    選取此選項以同步化所有新閘道或尚未與新閘道金鑰通訊的閘道。如果所有閘道都已使用目前的閘道金鑰同步化，但是有一個閘道已關閉，或是您要強制新閘道更新金鑰時，請選取這個選項。
- **匯出伺服器加密金鑰作爲備份** - 選取此選項即可將現有的伺服器加密金鑰匯出爲 XML 格式的檔案。當您選取此選項時，Identity Manager 會顯示額外的欄位，以供您指定匯出金鑰的路徑和檔案名稱。

備註 如果您要使用 PKCS#5 加密，而且選擇產生和設定新的伺服器加密金鑰的話，您也應選取此選項。除此之外，您還應該將匯出的金鑰儲存在可移除的媒體上，並存放在安全的位置 (請勿放在網路上)。

- **執行模式** - 選取要在背景 (預設選項) 還是在前景執行此作業。如果您選擇以新產生的金鑰重新加密一個或多個物件類型，則此作業可能需要花費一點時間，並且最好在背景中執行。

使用授權類型保護物件安全

一般會使用 AdminGroup 權能中指定的權限，授予對 Identity Manager objectType (例如 [配置]、[規則] 或 TaskDefinition) 的存取權。不過，授予對一個或多個所控制的組織內 Identity Manager objectType 之所有物件的存取權，有時範圍仍然過大。

使用授權類型 (AuthType) 可讓您進一步設定範圍，或限制對指定 Identity Manager objectType 之物件子集的此存取權。例如，填入規則以從使用者表單中進行選取時，可能不想讓使用者能存取控制範圍內的所有規則。

若要定義新的授權類型，請編輯 Identity Manager 儲存庫中的 AuthorizationTypes 配置物件，並新增 <AuthType> 元素。此元素需要兩種特性：

- 新授權類型的名稱
- 新元素延伸或設定範圍的現有授權類型或 objectType

例如，若想要新增名稱爲 Marketing Rule 的新的規則授權類型以延伸 Rule，則請定義下列項目：

```
<AuthType name='Marketing Rule' extends='Rule'/>
```

接下來，若要啓用要使用的授權類型，則必須在兩個位置參照該授權類型。

- 位於將一個或多個權限授予新授權類型的自訂 AdminGroup 權能內
- 位於應該爲此類型的物件內

以下是這兩種參照的範例。

第一個範例顯示授予對 Marketing Rules 之存取權的 AdminGroup 權能定義。

編碼樣例 12-4

```
<AdminGroup name='Marketing Admin'>
  <Permissions>
    <Permission type='Marketing Rule' rights='View,List,Connect,Disconnect/>
  </Permissions>
  <AdminGroups>
    <ObjectRef type='AdminGroup' id='#ID#Account Administrator'/>
  </AdminGroups>
</AdminGroup>
```

下一個範例顯示 Rule 定義，此定義因爲已授予使用者對 Rule 或 Marketing Rule 的存取權，所以使用者可以存取物件。

```
<Rule name='Competitive Analysis Info' authType='Marketing Rule'>
 ...
</Rule>
```

備註 若授予任何使用者存取權，使其可存取父系授權類型或授權類型所延伸的靜態類型，則此使用者對所有子授權類型也擁有相同的權限。因此，使用上一個範例，所有已獲得對 Rule 之權限的使用者，也對 Marketing Rule 擁有相同的權限。但反之則不然。

安全性使用方案

身爲 Identity Manager 管理員，您只要在設定時或以後執行以下建議步驟，即可進一步減少受保護帳號和數據的安全性風險。

設定時

您應該：

- 使用 HTTPS 透過安全 Web 伺服器存取 Identity Manager。
- 重設預設 Identity Manager 管理員帳號 (管理員與 Configurator) 的密碼。若要進一步確保這些帳號的安全性，您可以將它們重新命名。
- 限制對 Configurator 帳號的存取。
- 將管理員的權能集限制爲只能執行爲實現其作業功能所需要的動作，可透過設定組織階層來限制管理員權能。
- 變更 Identity Manager 索引儲存庫的預設密碼。
- 開啓稽核以追蹤 Identity Manager 應用程式中的作業。
- 編輯對 Identity Manager 目錄中檔案的權限。
- 自訂工作流程以插入核准或其他檢查點。
- 開發回復程序來描述如何在緊急狀況下回復您的 Identity Manager 環境。

在使用期間

您應該：

- 定期變更預設 Identity Manager 管理員帳號 (管理員和 Configurator) 的密碼。
- 目前未使用系統時登出 Identity Manager。
- 設定或瞭解 Identity Manager 階段作業的預設逾時期間。因爲可針對每個登入應用程式以個別方式進行設定，因此階段作業逾時的值可能不同。

若應用程式伺服器與 Servlet 2.2 相容，則 Identity Manager 安裝程序會將 HTTP 階段作業逾時設爲預設值 30 分鐘。您可以編輯屬性來變更此值；但您應該將該值設定爲一個較低的值以增加安全性。不要將該值設定爲高於 30 分鐘。

若要變更階段作業逾時值，請執行以下步驟：

1. 編輯 `web.xml` 檔案，其位於您應用程式伺服器目錄樹中的 `idm/WEB-INF` 目錄。
2. 變更下列行中的數值：

```
<session-config>
  <session-timeout>30</session-timeout>
</session-config>
```

第 13 章

身份識別稽核：基本概念

本章介紹身份識別稽核及稽核控制背後的概念。稽核控制可用以監視及管理整個企業資訊系統及應用程式的稽核與規範遵循。

在本章中，將可瞭解以下概念與作業：

- 關於身份識別稽核
- 身份識別稽核的目標
- 瞭解身份識別稽核
- 在管理員介面中使用身份識別稽核
- 啓用稽核記錄
- 關於稽核策略

關於身份識別稽核

Identity Manager 將稽核定義爲在企業範圍內，對身份識別資料的系統化擷取、分析與回應，以確保遵循內部與外部的策略與規範。

要遵循會計與資料隱私權的法律規範並不容易。Identity Manager 的稽核功能提供了靈活的方法，可讓您實作適用於您的企業之規範遵循解決方案。

在大部分的環境中，會有不同的群組涉及到規範遵循：內部與外部稽核小組 (視稽核爲主要工作)；與非稽核工作人員 (稽核對他們而言可能是雜務)。IT 通常也與規範遵循有關，他們會協助將內部稽核小組的需求付諸於選定的解決方案實作。成功實作稽核解決方案的關鍵，在於精確擷取非稽核工作人員的知識、控制與程序，然後以自動化的方式應用這些資訊。

身份識別稽核的目標

身份識別稽核可改進稽核效能如下：

- 身份識別稽核會自動偵測規範遵循違規，透過即時通知實現迅速修正

  Identity Manager 稽核策略功能可讓您定義違規的規則 (亦即條件)。定義之後，系統便會掃描是否有違反既定策略的情況，例如未經授權的存取變更或錯誤的存取權限。如果偵測到這類情況，系統就會根據所定義的上報鏈通知適當的人員。接著，使用者呼叫的工作或自動由策略違規呼叫的工作流程便會修正 (更正) 該違規。

- 視需要提供有關內部稽核控制效用的關鍵資訊。

  Auditor 報告提供有關違規和異常之概括的狀態資訊，以便快速分析風險狀態。[報告] 標籤還提供違規的圖形化報告。您可依據資源、組織或策略檢視違規，並根據所定義的報告特性來自訂每個圖表。

- 自動化身份識別控制的認證檢閱作業，以降低操作風險

  工作流程功能可以啓用自動化的策略通知和存取違規給選取的使用者。

- 準備詳細描述使用者作業並符合法規要求的完整報告

  [報告] 區域可讓您定義詳細的報告及圖表，其中提供有關存取歷程記錄和權限，以及其他策略違規的資訊。透過報告功能，系統會保留安全與完整的身份稽核軌跡，以供擷取存取資料和使用者設定檔更新之用。

- 簡化定期檢閱程序以維護安全性和對法規的規範遵循

  您可以執行定期存取檢閱以收集使用者軟體權利文件記錄，並確定哪些軟體權利文件需要檢閱。接著該程序便會通知指定驗證者有擱置的請求需要其檢閱，並在驗證者對這些請求執行的動作完成後更新狀態或擱置的請求。

- 找出使用者帳號的潛在利益衝突權能

  Identity Manager 提供責任分離報告，其可識別具有特定權能或權限 (可能導致利益衝突) 的使用者。

瞭解身份識別稽核

Identity Manager 提供了一項功能可用於稽核使用者帳號權限和存取權限，另有功能可用以維護及認證規範遵循，即是**基於策略的規範遵循**和**定期存取檢閱**等功能。

基於策略的規範遵循

針對公司建立之適用於所有使用者帳號的需求，Identity Manager 透過稽核策略系統使管理員能夠維護對這些需求的規範遵循。

您可以使用稽核策略，透過以下兩種不同卻互補的方式確保規範遵循：**連續性規範遵循**和**定期規範遵循**。

在佈建作業可能於 Identity Manager 外部執行的環境中，這兩種技術更具互補性。只要帳號可能被不執行或不遵循現有稽核策略的程序所變更，就需要定期規範遵循。

連續規範遵循

連續規範遵循是指稽核策略會套用至所有佈建作業，如此便無法使用與目前策略不相容的方式修改帳號。

將稽核策略指定給組織和 (或) 使用者，即可啓用連續規範遵循。對使用者執行的所有佈建作業，都將導致使用者指定的策略受到計算。若此評估產生了任何策略失敗，都將中斷佈建作業。

組織型策略集會以階層方式定義。任一使用者都只有一個生效的組織策略集。所套用的是指定給最低層級組織的策略集。例如：

組織	直接指定的策略集	有效的策略
Austin	策略 A1、A2	策略 A1、A2
銷售		策略 A1、A2
開發	策略 B、C2	策略 B、C2
支援		策略 B、C2
測試	策略 D、E5	策略 D、E5
財務		策略 A1、A2
Houston		<無>

定期規範遵循

定期規範遵循是指 Identity Manager 會隨需求計算策略。任何不符合的情況都會擷取爲規範遵循違規。

執行定期規範遵循掃描時，您可以選取要在掃描中使用的策略。掃描程序會對直接指定的策略 (使用者指定的策略和組織指定的策略) 與任意一組所選取的策略進行調合。

具有 Auditor 管理員權能的 Identity Manager 使用者可以建立稽核策略，並透過定期執行策略掃描與檢閱是否有策略違規，以監視對這些策略的規範遵循。可透過修正和緩解程序管理違規。

如需有關 Auditor 管理員權能的更多資訊，請參閱第 215 頁的「瞭解與管理權能」。

Identity Manager 稽核可定期掃描使用者。這些掃描執行稽核策略，偵測已建立帳號限制中的偏差。一旦偵測到違規，便會啓動修正作業。這些規則可以是 Identity Manager 提供的標準稽核策略規則，也可以是使用者定義的自訂規則。

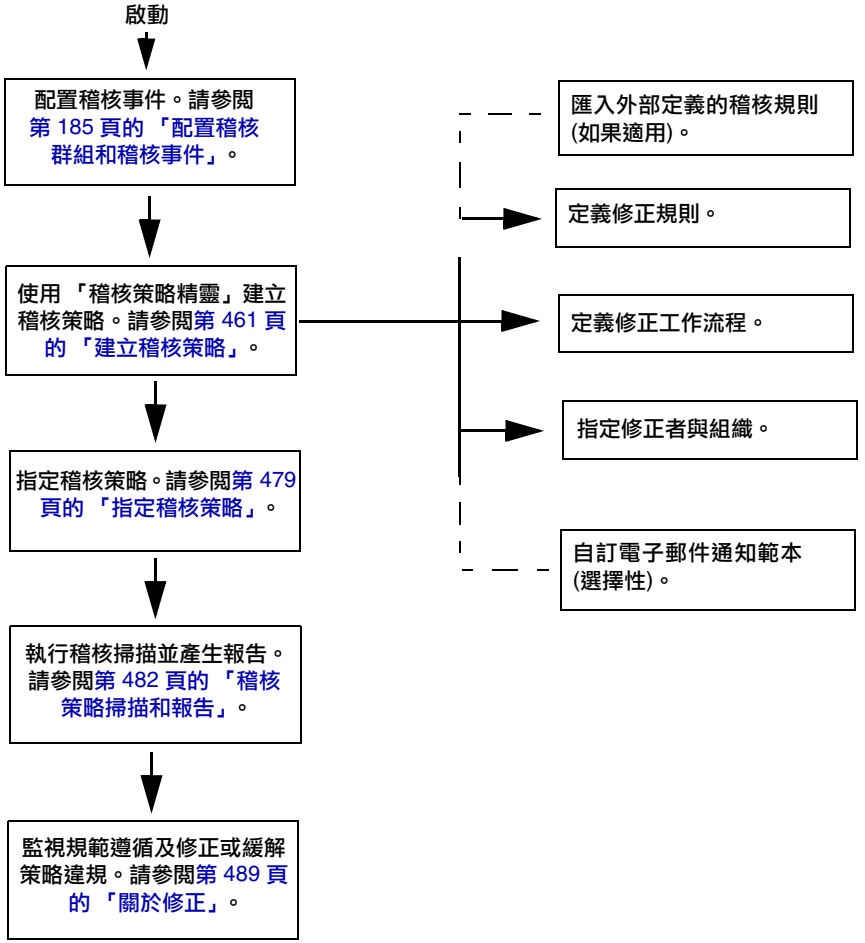
基於策略之規範遵循的邏輯作業流程

圖 13-1 (第 452 頁) 顯示建立策略性稽核控制的邏輯作業流程。

定期存取檢閱

Identity Manager 提供定期存取檢閱功能，可讓管理員與其他責任方臨時或定期檢閱和驗證使用者存取權限。如需有關此功能的更多資訊，請參閱第 500 頁的「定期存取檢閱與驗證」。

圖 13-1　建立策略性規範遵循的邏輯作業流程



在管理員介面中使用身份識別稽核

本節說明如何存取管理員介面中的「身份識別稽核」功能，也會討論用於身份識別稽核的電子郵件通知範本。

介面的 [規範遵循] 區段

若要建立並管理稽核策略，請使用 Identity Manager 管理員介面的 **[規範遵循]** 區段。

若要移至建立與管理稽核策略的 [規範遵循] 區段，請執行以下步驟：

1. 登入管理員介面 (第 56 頁)。
2. 按一下功能表列中的 **[規範遵循]**。

   [規範遵循] 區段有三個子標籤 (或功能表項目)：

   - 管理策略
   - 管理存取掃描
   - 存取檢閱

管理策略

[管理策略] 頁面會列出您有權檢視與編輯的策略。您還可以在此區域中管理存取掃描。

在 [管理策略] 頁面中，您可以使用稽核策略完成以下作業：

- 建立稽核策略
- 選取策略以進行檢視或編輯
- 刪除策略

第 457 頁的「下一節 「使用稽核策略」將說明如何使用稽核策略精靈，建立稽核策略。」一節中將提供有關這些作業的詳細資訊。

管理存取掃描

使用 **[管理存取掃描]** 標籤可建立、修改及刪除存取掃描。您可以在此區域中定義要執行或要排程爲定期存取檢閱的掃描。如需有關此功能的更多資訊，請參閱第 500 頁的「定期存取檢閱與驗證」。

存取檢閱

[存取檢閱] 標籤可讓您啓動、終止與刪除存取檢閱，以及監視存取檢閱的進度。其中顯示掃描結果的摘要報告並提供一些資訊連結，可讓您存取有關檢閱狀態和擱置作業的更多詳細資訊。

如需有關此功能的更多資訊，請參閱第 510 頁的「管理存取檢閱」。

身份識別稽核作業介面參照

若要查閱在管理員介面中執行其他身份識別稽核作業的方法，請參閱第 613 頁的附錄 C。此快速參照資料能告訴您該由何處著手各式稽核作業。

電子郵件範本

身份識別稽核在許多作業中都可使用電子郵件通知。其中每一則通知都會使用一個電子郵件範本物件。電子郵件範本可用於自訂電子郵件訊息的標頭與內文。

表 13-1 身份識別稽核電子郵件範本

範本名稱	用途
存取檢閱修正通知	在最初建立修正狀態的使用者軟體權利文件時，由存取檢閱傳送給修正者。
批次驗證通知	在驗證者有擱置的驗證時，由存取檢閱傳送給驗證者。
策略違規通知	在發生違規時，由稽核策略掃描傳送給修正者。
存取掃描開始通知	在存取檢閱啟動掃描時，傳送給該存取掃描的所有者。
存取掃描結束通知	在存取掃描完成時，傳送給該存取掃描的所有者。

啟用稽核記錄

您必須先啓用 Identity Manager 稽核記錄系統並將其配置爲收集稽核事件，才能開始管理規範遵循與存取檢閱。依預設，啓用稽核系統。具有「配置稽核」權能的 Identity Manager 管理員可配置稽核。

Identity Manager 提供規範遵循管理稽核配置群組。

若要檢視或修改「規範遵循管理」群組所儲存的事件，請執行下列動作：

1. 登入管理員介面 (第 56 頁)。
2. 從功能表列選取 **[配置]**，然後按一下 **[稽核]**。
3. 在 [稽核配置] 頁面中，選取 **[規範遵循管理]** 稽核群組名稱。

如需有關設定稽核配置群組的更多資訊，請參閱「配置」一章中第 185 頁的「配置稽核群組和稽核事件」。

如需有關稽核系統如何記錄事件的資訊，請參閱第 10 章「稽核記錄」。

關於稽核策略

稽核策略可針對一個或多個資源的一組使用者，定義其帳號限制。其中包括用於定義策略限制的規則，以及在發生違規後用於處理違規的工作流程。**稽核掃描**會使用在稽核策略中定義的條件，計算組織中是否發生違規狀況。

稽核策略包含以下元件：

- **策略規則**會定義特定的違規。策略規則可包含以 XPRESS、XML 物件或 JavaScript 語言所撰寫的函數。
- 當稽核掃描識別出策略規則的違規時，便會選擇性地啓動**修正工作流程**。
- **修正者**是獲授權可回應策略違規的指定使用者。修正者可以是個別使用者或使用者群組。

建立具有稽核策略規則的策略

在稽核策略中，規則會根據屬性來定義可能的衝突。稽核策略可能包含參照廣泛資源的上百個規則。在規則評估期間，該規則可存取一個或多個資源的使用者帳號資料。稽核策略可能會限定哪些資源可供規則使用。

規則可以僅檢查單一資源的單一屬性，也可以檢查多個資源的多項屬性。

利用修正工作流程處理策略違規

您在建立用於定義策略違規的規則之後，可選取當稽核掃描期間偵測到違規時將啓動的工作流程。Identity Manager 提供預設的標準修正工作流程，爲稽核策略掃描提供預設的修正處理。除了其他動作之外，這個預設修正工作流程還會產生通知電子郵件給每個指定的層級 1 修正者 (必要時也會寄給其他層級的修正者)。

備註 與 Identity Manager 工作流程程序不同，必須將修正工作流程指定爲 `AuthType=AuditorAdminTask` 和 `SUBTYPE_REMEDIATION_WORKFLOW` 子類型。若您匯入工作流程以便用於稽核掃描，您必須手動新增這個屬性。請參閱第 463 頁的「(選擇性) 將工作流程匯入 Identity Manager」，以取得更多資訊。

指定修正者

如果您指定修正工作流程，則必須至少指定一個修正者。您最多可以指定三個層級的稽核策略修正者。如需有關修正的更多資訊，請參閱第 489 頁的「修正與緩解規範遵循違規」。

您必須先指定修正工作流程，才能指定修正者。

稽核策略方案範例

假設您負責應付帳款及應收帳款，且必須實作某些程序以預防責任集中在會計部門員工身上的潛在風險。這個策略必須確保應付帳款的負責人員並未同時負責處理應收帳款。

此稽核策略中將包含：

- 一組規則。每項規則各指定一個構成策略違規的條件
- 啓動修正作業的工作流程
- 一組指定的管理員或修正者，他們有權檢視及回應前述規則所建立的策略違規

當規則識別出策略違規 (在此案例中爲使用者擁有太多授權) 之後，相關聯的工作流程就會啓動指定的相關修正作業，包括自動通知選定的修正者。

層級 1 的修正者是指當稽核掃描識別出策略違規時，所要連絡的第一批修正者。如果爲稽核策略指定了多個層級，則當超過此區域中所確定的上報期限時，Identity Manager 會通知下一層級的修正者。

下一節「使用稽核策略」將說明如何使用稽核策略精靈，建立稽核策略。

第 14 章

稽核：稽核策略

本章說明如何使用「稽核策略精靈」，以建立、編輯、刪除及指定「稽核策略」。

在本章中，將可瞭解以下概念與作業：

- 使用稽核策略
- 建立稽核策略
- 編輯稽核策略
- 刪除稽核策略
- 對稽核策略進行疑難排解
- 指定稽核策略

使用稽核策略

若要建立稽核策略，請使用 Identity Manager 的稽核策略精靈。定義稽核策略後，即可對策略執行各項動作，例如修改或刪除策略。

稽核策略規則

稽核策略規則可定義特定的違規。策略規則可包含以 XPRESS、XML 物件或 JavaScript 語言所撰寫的函數。

您可使用稽核策略精靈建立簡單的規則，或使用 Identity Manager IDE 或 XML 編輯器建立更強大的規則。

- 規則必須爲子類型 `SUBTYPE_AUDIT_POLICY_RULE`。稽核策略精靈所產生的規則會自動指定爲此子類型。
- 規則必須屬於 authType `AuditPolicyRule`。稽核策略精靈所產生的規則會自動指定爲此 authType 類型。

使用稽核策略精靈建立的規則會傳回 `true` 或 `false` 值。傳回 `true` 值的策略規則會導致策略違規。但使用 Identity Manager IDE 時，卻可建立在稽核掃描或存取檢閱期間，會略過使用者的規則。傳回 `ignore` 值的稽核策略規則，會停止該使用者的規則處理，並跳至下一位目標使用者。

如需有關建立稽核策略規則的資訊，請參閱「Identity Manager Deployment Tools」一書中的「使用規則」。

建立稽核策略

請使用稽核策略精靈，建立稽核策略。

開啟稽核策略精靈

稽核策略精靈會引導您完成建立稽核策略的程序。

若要存取稽核策略精靈，請執行以下步驟：

1. 登入管理員介面 (第 56 頁)。
2. 按一下 **[規範遵循]** 標籤。

   [管理策略] 子標籤或功能表會隨即開啓。
3. 若要建立新的稽核策略，請按一下 **[新增]**。

建立稽核策略：簡介

使用此精靈可執行以下作業以建立稽核策略：

- 選取或建立要用以定義策略限制的規則
- 指定核准人並建立上報限制
- 指定修正工作流程

完成每個精靈螢幕中顯示的工作後，按 **[下一步]** 移至下一個步驟。

開始之前

請先謹慎規劃，再建立稽核策略！ 開始之前，請先確認是否已完成下列作業：

- 找出您在稽核策略精靈中建立策略時會使用的規則。所選擇的規則由您所建立的策略類型，以及您要定義的特定限制決定。請參閱下一節的找出所需的規則，以取得更多資訊。
- 匯入要在新的策略中包含的所有修正工作流程或規則。請參閱 (選擇性) 將工作流程匯入 Identity Manager (下文)，以取得更多資訊。
- 請確定您具有建立稽核策略所需的權能。請參閱第 215 頁的「瞭解與管理權能」以瞭解必要權能。

找出所需的規則

您在策略中指定的限制將會實作在您所建立或匯入的規則集中。使用稽核策略精靈建立規則時，請執行下列步驟：

1. 找出正在使用的特定資源。
2. 從資源的有效屬性清單中選取帳號屬性。
3. 選取要強加在屬性上的條件。
4. 輸入用於比較的值。

如需不使用「稽核策略精靈」建立稽核策略規則的資訊，請參閱「Identity Manager Deployment Tools」一書。

(選擇性) 將權責區分規則匯入 Identity Manager

稽核策略精靈無法建立權責區分規則。必須在 Identity Manager 外部建構這些規則，並使用 **[配置]** 標籤中的 **[匯入交換檔案]** 選項匯入規則。

(選擇性) 將工作流程匯入 Identity Manager

若要使用 Identity Manager 目前並未提供的修正工作流程，請匯入外部工作流程。使用 XML 編輯器或 Identity Manager IDE 可以建立自訂的工作流程 (第 60 頁)。

若要匯入外部工作流程，請執行以下步驟：

1. 設定 `authType=AuditorAdminTask` 並增加 `subtype=SUBTYPE_REMEDIATION_WORKFLOW`。您可以選擇使用 Identity Manager IDE 或 XML 編輯器，設定這些配置物件。
2. 使用 [匯入交換檔案] 選項匯入工作流程。
   a. 登入管理員介面 (第 56 頁)。
   b. 按一下 **[配置]** 標籤，然後再按一下 **[匯入交換檔案]** 子標籤或功能表。

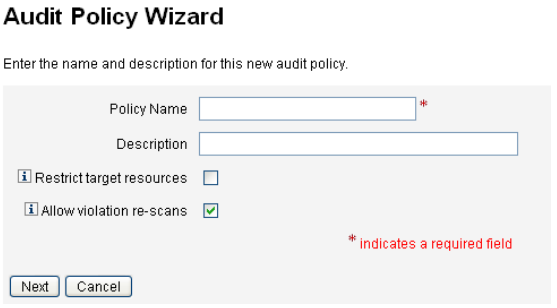
      [匯入交換檔案] 頁面會隨即開啓。
   c. 瀏覽至要上傳的工作流程檔案，然後按一下 **[匯入]**。

成功匯入工作流程後，它便會顯示在稽核策略精靈 (第 461 頁) 的 [修正工作流程] 選項清單中。

命名與說明稽核策略

在稽核策略精靈中輸入新策略的名稱及簡短說明，如圖 14-1 所示。

圖 14-1　稽核策略精靈：輸入名稱與描述螢幕



備註　稽核策略名稱不得包含以下字元：' (所有格符號)、. (小數點號)、| (管線符號)、[(左括號)、] (右括號)、, (逗號)、: (冒號)、$ (美元符號)、" (雙引號)、\ (反斜線) 或 = (等號)。

也應避免下列字元：_ (底線)、% (百分比符號)、^ (指數符號) 和 * (星號)。

若希望在執行掃描時僅存取所選取的資源，請選取 **[限制目標資源]** 選項。

若要在修正違規之後立即重新掃描使用者，請選取 **[允許違規重新掃描]** 選項。

備註　若稽核策略不限制資源，則掃描期間將會存取使用者具有帳號的所有資源。若規則僅使用某些資源，則將策略限定爲這些資源會更有效率。

按 **[下一步]** 繼續至下一頁。

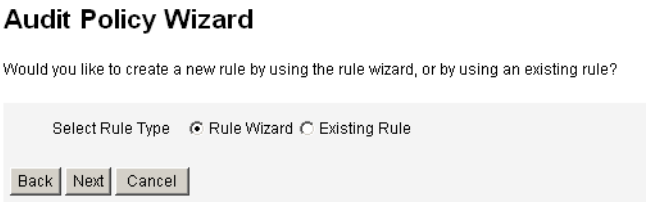
選取規則類型

使用此頁面可開始定義或包含策略中規則的程序 (建立策略的工作主要就是定義與建立規則)。

如圖 14-2 所示，您可以選擇使用 Identity Manager 規則精靈建立自己的規則，或結合使用現有規則。規則精靈僅允許在一項規則中使用一個資源。匯入的規則可依需要參照多個資源。

依預設會選取 **[規則精靈]** 選項。

圖 14-2　稽核策略精靈：選取規則類型螢幕



按一下 **[現有的規則]**，再按 **[下一步]** 選取使用 Identity Manager IDE 建立的規則 (第 60 頁)。執行下節 「選取現有的規則」步驟。

否則，請按一下 **[規則精靈]**，再按 **[下一步]**。執行下節中的步驟。

選取現有的規則

若要在新策略中包含現有的規則，請選取 [選取規則類型螢幕] 中的 **[現有的規則]** (圖 14-2)，再按 **[下一步]**。然後，從 **[選取現有的規則]** 下拉式功能表中選取現有的稽核策略規則。

備註　若看不到之前匯入 Identity Manager 的規則名稱，請確認您已將第 456 頁的 「建立具有稽核策略規則的策略」中所述的額外屬性增加至規則中。

按 **[下一步]**。

跳至第 469 頁的 「增加額外規則」一節。

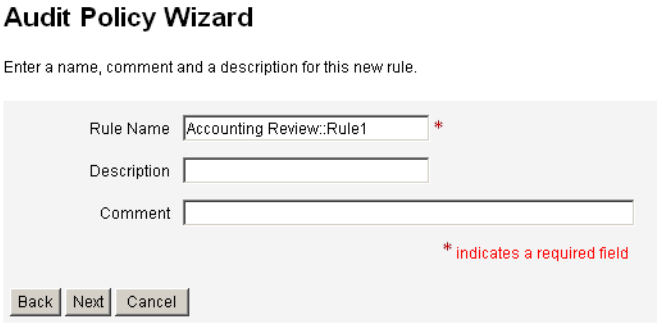
使用規則精靈建立新規則

若選擇使用稽核策略精靈中的 [規則精靈] 選項建立規則，請在以下各節說明的頁面中繼續輸入資訊。

命名與說明新規則

選擇性地爲新規則命名並加以說明。使用此頁面可輸入描述性文字，每次當 Identity Manager 顯示該規則時，描述性文字都會出現在規則名稱旁邊。請輸入簡潔清楚且能夠描述規則的說明。這段說明會顯示在 Identity Manager 內的 [檢閱策略違規] 頁面中。

圖 14-3　稽核策略精靈：輸入規則說明螢幕



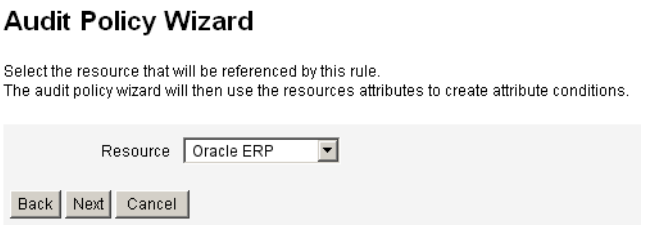
例如，若建立的規則可識別同時具有 Oracle ERP responsibilityKey 屬性值 `Payable User` 與 `Receivable User` 屬性值的使用者，則可以在 [描述] 欄位中輸入以下文字：**找出同時具有 `Payable User` 和 `Receivable User` 責任的使用者。**

使用 [註釋] 欄位可提供有關規則的額外資訊。

選取規則參照的資源

使用此頁面可選取規則將參照的資源。每個規則變數都必須對應到其資源的屬性。您具有檢視存取權限的所有資源都會顯示在此選項清單中。在此範例中，已選取 Oracle ERP。

圖 14-4　稽核策略精靈：選取資源螢幕



備註　支援每個可用資源介面的大多數 (但不是全部) 的屬性。如需有關可用之特定屬性的資訊，請參閱 「Identity Manager Resources Reference」。

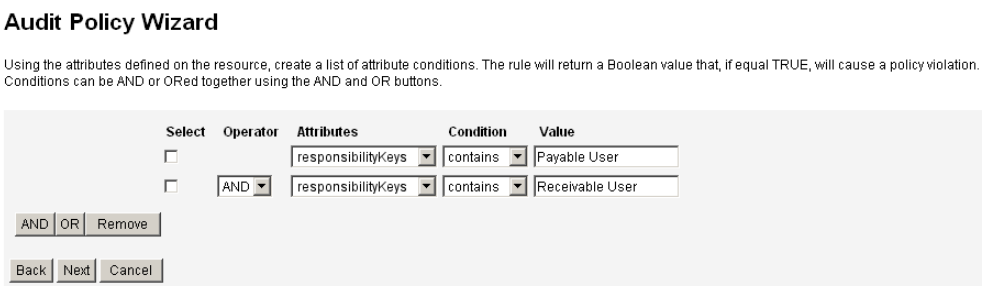
按 **[下一步]** 移至下一頁。

建立規則表示式

使用此螢幕可爲您的新規則輸入規則表示式。此範例所建立的規則不允許具有 Oracle ERP responsibilityKey 屬性值 `Payable User` 的使用者同時具有 `Receivable User` 屬性值。

1. 從可用屬性清單中選取使用者屬性。此屬性會直接對應到規則變數。
2. 從清單選取邏輯條件。有效的條件包括 = (等於)、!= (不等於)、< (小於)、<= (小於或等於)、> (大於)、>= (大於或等於)、爲 true、爲空、不爲空、爲空、包含。針對此範例的目的，您可以從可能的屬性條件清單中選取包含。
3. 輸入表示式的值。例如，若輸入 `Payable user`，則是在指定具有 responsibilityKeys 屬性值 `Payable user` 的 Oracle ERP 使用者。
4. (選擇性) 按一下 **[AND]** 或 **[OR]** 運算子以增加另一行並建立其他表示式。

圖 14-5 稽核策略精靈：選取規則表示式螢幕



此規則會傳回布林值。若兩個陳述式都爲 true，則策略規則會傳回 TRUE 值，進而引發策略違規。

備註 Identity Manager 不支援規則巢式控制。此外，使用稽核策略精靈建立的策略，如果在規則之間有不同的布林值運算子，會產生無法預期的結果，因爲未指定評估順序。

如果是複雜的規則表示式，請使用 XML 編輯器建立規則，勿用稽核策略精靈。使用 XML 編輯器可讓您在必要時只讓各規則間使用一個布林值運算子。

以下程式碼範例顯示了您已在此螢幕中建立之規則的 XML：

編碼樣例 14-1 新建立之規則的 XML 語法範例

```
<Description>Payable User/Receivable User</Description>
  <RuleArgument name='resource' value='Oracle ERP'>
    <Comments>Resource specified when  audit policy was created.</Comments>
    <String>Oracle ERP</String>
  </RuleArgument>
    <and>
      <contains>
        <ref>accounts[Oracle ERP].responsibilityKeys</ref>
        <s>Receivable User</s>
      </contains>
      <contains>
        <ref>accounts[Oracle ERP].responsibilityKeys</ref>
        <s>Payables User</s>
      </contains>
    </and>
    <MemberObjectGroups>
      <ObjectRef type='ObjectGroup' id='#ID#Top' name='Top'/>
    </MemberObjectGroups>
</Rule>
```

若要從規則中移除表示式，請選取屬性條件，然後按一下 **[移除]**。

按 **[下一步]** 以繼續執行「稽核策略精靈」。您會有機會增加更多的規則，可以利用增加現有的規則或再度使用精靈皆可。

增加額外規則

您可匯入現有的規則 (第 465 頁) 或使用精靈 (第 466 頁) 以建立其他規則。

請視需要按一下 **[AND]** 或 **[OR]** 以繼續增加規則。若要移除某規則，請選取該規則後按一下 **[移除]**。

只有在所有規則的布林表示式均計算爲 true 時，才會發生策略違規。使用 AND/OR 運算子分組規則後，即使所有規則均未計算爲 true，策略也可能會計算爲 true。Identity Manager 僅會針對計算爲 true 的規則建立違規 (僅當策略表示式評估爲 true 時)。稽核策略精靈無法明確控制布林表示式巢狀套疊，因此最好不要建立層級太深的表示式。

備註 Identity Manager 不支援規則巢式控制。此外，使用稽核策略精靈建立具有布林表示式巢式的策略，會產生無法預期的結果。

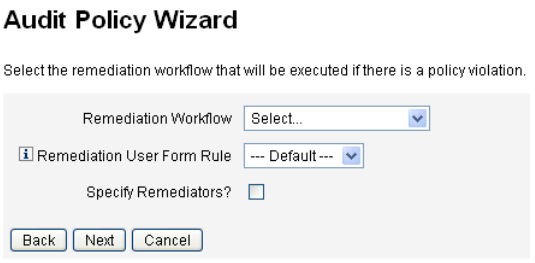
如需複雜的規則表示式，請使用 XML 編輯器建立參照需要使用的所有規則之獨立 XPRESS 規則。

選取修正工作流程

使用此螢幕可選取要與此策略相關聯的「修正工作流程」。此處所指定的工作流程會決定在偵測到稽核策略違規時，要在 Identity Manager 內採取的行動。

備註 針對每個失敗的稽核策略，各會啓動一個工作流程。針對每項規範遵循違規 (由特定策略的策略掃描所建立)，每個工作流程都會包含一個或多個工作項目。

圖 14-6 稽核策略精靈：選取修正工作流程螢幕



備註 如需有關匯入您使用 XML 編輯器或 Identity Manager Integrated Development Environment (IDE) 所建立之工作流程的資訊，請參閱第 463 頁的「(選擇性) 將工作流程匯入 Identity Manager」。

使用 **[修正使用者表單規則]** 下拉式功能表選取一項規則，以計算在透過修正作業編輯使用者時應套用的使用者表單。依預設，編輯使用者以回應修正工作項目的修正者，將使用指定給該修正者的使用者表單。若稽核策略指定了修正使用者表單，則會改用此表單。如此可在稽核策略指出特定的問題時，使用與之對應的專用表單。

若要指定與此修正工作流程相關聯的修正者，請選取 **[是否指定修正者？]** 核取方塊。若選取此選項，則按 **[下一步]** 便會顯示 [指定修正者] 頁面。若不選取此選項，則精靈會接著顯示 [稽核策略精靈指定組織] 畫面。

針對修正選取修正者及逾時

若指定修正者，則當偵測到針對此策略的違規時，指定給此稽核策略的修正者會收到通知。此外，預設的工作流程也會爲其指定修正工作項目。任何 Identity Manager 使用者皆可爲修正者。

您可以選擇指定至少一個層級 1 修正者或指定的使用者。偵測到策略違規時，修正工作流程首先會使用電子郵件連絡層級 1 修正者。若已達到指定的上報逾時期間但層級 1 修正者尚未回應，則 Identity Manager 接著會連絡您在此處指定的層級 2 修正者。只有在層級 1 和層級 2 修正者於上報期間結束之前均無回應時，Identity Manager 才會連絡層級 3 修正者。

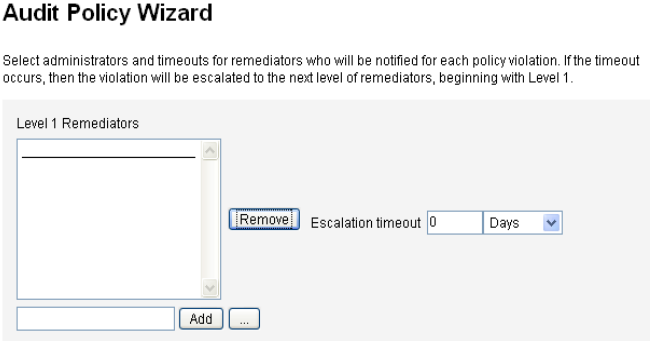
備註 若爲所選的最高層級修正者指定了上報逾時時間值，則在上報逾時後，即會從清單中移除工作項目。上報逾時時間的預設值爲 0。在此情況下，工作項目將不會過期，而會持續保留在修正者清單中。

[指定修正者] 是非必要選項。若選取此選項，請在指定設定後按 **[下一步]**，以繼續移至下一個螢幕。

若要將使用者增加至可用的修正者清單，請輸入使用者 ID，然後按一下 **[增加]**。或者，按一下 **[...** (更多)]，以搜尋使用者 ID。在 [開頭爲] 欄位中輸入一個或多個字元，然後按一下 **[尋找]**。從搜尋清單選取使用者後，按一下 **[增加]** 即可將該使用者增加至修正者清單。按一下 **[解除]** 以關閉搜尋區域。

若要從修正者清單移除使用者 ID，請從清單中進行選取，然後按一下 **[移除]**。

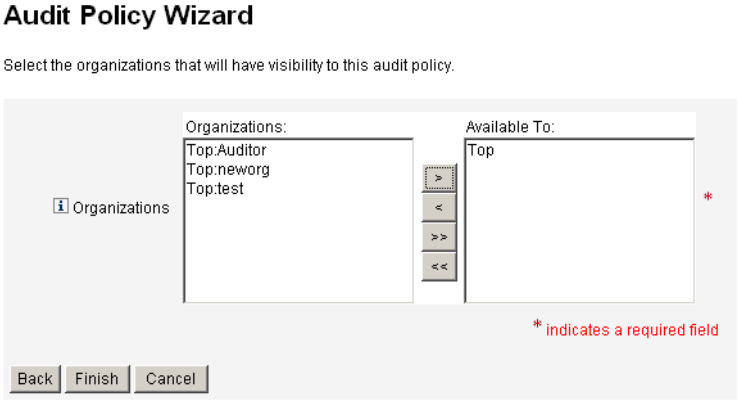
圖 14-7 稽核策略精靈：選取層級 1 修正者區域



選取可存取此策略的組織

使用圖 14-8 所示螢幕，可選取可以檢視及編輯此策略的組織。

圖 14-8　稽核策略精靈：指定組織可視性螢幕



選取組織後，按一下 **[完成]** 即可建立稽核策略並回到 [管理策略] 頁面。此時新建立的策略會顯示於此清單中。

編輯稽核策略

稽核策略的常見編輯工作包括：

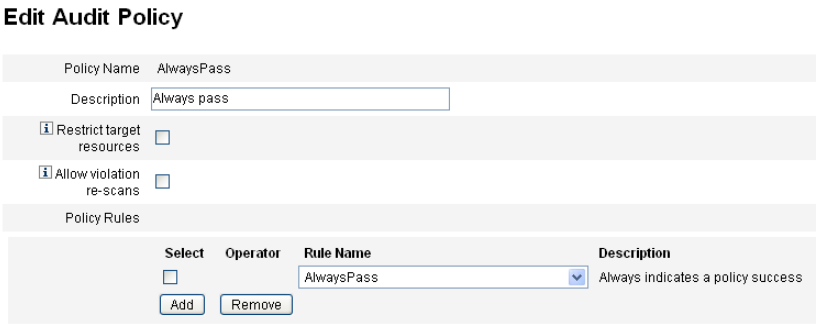
- 增加或刪除規則
- 變更目標資源
- 調整具有此策略存取權限的組織清單
- 變更與各個修正層級相關聯的上報逾時時間
- 變更與此策略相關聯的修正工作流程

編輯策略頁面

在 [稽核策略] 名稱欄中，按一下策略名稱即可開啓 [編輯稽核策略] 頁面。此頁面將稽核策略資訊歸類分組如下：

- 識別與規則區域
- 修正者與上報逾時時間區域
- 工作流程與組織區域

圖 14-9　編輯稽核策略頁面：識別與規則區域



使用此頁面區域可以：

- 編輯策略描述
- 增加或刪除規則

備註 您無法使用此產品直接編輯現有的規則。請使用 Identity Manager IDE 或 XML 編輯器編輯規則，然後將規則匯入 Identity Manager。然後可以移除舊版本，並加入新修改的版本。

編輯稽核策略描述

選取 [描述] 欄位中的文字並輸入新文字，以編輯稽核策略描述。

編輯選項

選擇性選取或取消選取 **[限制目標資源]** 或 **[允許違規重新掃描]** 選項。

從策略中刪除規則

若要從策略刪除規則，請按一下規則名稱前面的 **[選取]** 按鈕，然後按一下 **[移除]**。

增加規則到策略

按一下 **[增加]** 即可附加新的欄位，以供您用以選取要增加的規則。

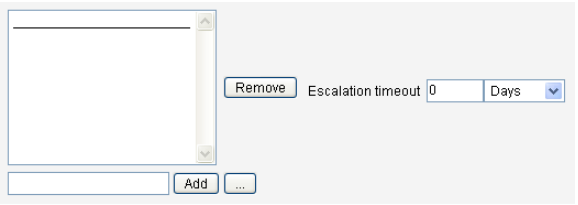
變更策略使用的規則

在 [規則名稱] 欄中，從選項清單中選取其他規則。

修正者區域

圖 14-10 中顯示 [修正] 區域的一部分，您可於此處指定層級 1、層級 2、層級 3 的策略修正者。

圖 14-10　編輯稽核策略頁面：指定修正者



使用此頁面區域可以：

- 爲策略移除或指定修正者
- 調整上報逾時時間

移除或指定修正者

輸入使用者 ID 以針對一個或多個修正層級選取修正者，然後按一下 **[增加]**。若要搜尋使用者 ID，請按一下 **[...** (更多)**]**。您必須至少選取一個修正者。

若要移除修正者，請選取清單中的使用者 ID，然後按一下 **[移除]**。

調整上報逾時時間

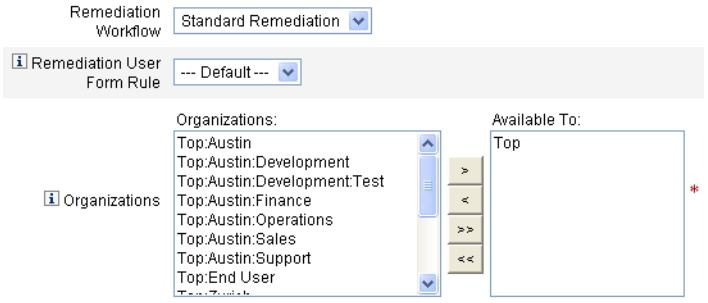
選取逾時值然後輸入新值。依預設將不會設定逾時值。

備註　若爲所選的最高層級修正者指定了上報逾時時間值，則在上報逾時後，即會從清單中移除工作項目。

修正工作流程與組織區域

圖 14-11 顯示了用於爲稽核策略指定修正工作流程和組織的區域。

圖 14-11　編輯稽核策略頁面：修正工作流程與組織



使用此頁面區域可以：

- 變更在發生策略違規時啓動的修正工作流程
- 選取修正使用者表單規則
- 調整具有此策略存取權限的組織

變更修正工作流程

若要變更指定給策略的工作流程，可以從選項清單選取替代的工作流程。依預設，不會爲稽核策略指定任何工作流程。

備註　若沒有爲稽核策略指定任何工作流程，則不會將違規指定給任何修正者。

從清單中選取修正工作流程，然後按一下 **[儲存]**。

選取修正使用者表單規則

選擇性地選取在透過修正作業編輯使用者時，計算所套用之使用者表單的規則。

指定或移除組織的可視性

調整可使用此稽核策略的組織，然後按一下 **[儲存]**。

策略範例

Identity Manager 提供下列可從 [稽核策略] 清單中存取的策略範例：

- IDM 角色比較策略
- IDM 帳號累積策略

IDM 角色比較策略

此策略範例可讓您對使用者目前的存取權與 Identity Manager 角色所指定的存取權進行比較。此策略可確保已爲使用者設定由角色所指定的所有資源屬性。

此策略在下列情況下將失敗：

- 使用者缺少角色所指定的任一資源屬性
- 使用者的資源屬性與角色所指定的屬性不同

IDM 帳號累積策略

此策略範例會驗證該使用者所擁有的所有帳號，是否至少由一個同樣由該使用者所擁有的角色所參照。

若指定給該使用者的角色並未明確參照某些資源，但此使用者此類資源擁有帳號，則此策略會失敗。

刪除稽核策略

從 Identity Manager 刪除稽核策略後，所有參照該策略的違規也將一併刪除。

按一下 [管理策略] 檢視策略後，可從介面的 [規範遵循] 區域刪除策略。若要刪除稽核策略，請在策略檢視中選取策略名稱，然後按一下 **[刪除]**。

對稽核策略進行疑難排解

對策略規則進行除錯通常是解決稽核策略問題的最佳辦法。

對規則進行除錯

若要對規則進行除錯，請將下列追蹤元素增加到規則程式碼中。

```
<block trace='true'>
<and>
    <contains>
        <ref>accounts[AD].firstname</ref>
        <s>Sam</s>
    </contains>
    <contains>
        <ref>accounts[AD].lastname</ref>
        <s>Smith</s>
    </contains>
</and>
</block>
```

問題

在 Identity Manager 介面中看不到我的工作流程。

解決方法

請確認：

- 您已將 `subtype='SUBTYPE_REMEDIATION_WORKFLOW'` 屬性增加至工作流程中。若沒有此子類型，便無法在 Identity Manager 管理員介面中看到工作流程。
- 您具有 authType `AuditorAdminTask` 的權能。
- 您所控制的組織就是工作流程所在的組織。

問題

我已匯入的規則未顯示在稽核策略精靈中。

解決方法

請確認：

- 每個規則皆屬於 `subtype=SUBTYPE_AUDIT_POLICY_RULE` 或 `subtype=SUBTYPE_AUDIT_POLICY_SOD_RULE`。
- 您具有 authType `AuditPolicyRule` 的權能。
- 您所控制的組織就是工作流程所在的組織。

指定稽核策略

若要將稽核策略指定給組織，使用者必須至少要具有「指定組織稽核策略」權能。若要將稽核策略指定給使用者，使用者必須具有「指定使用者稽核策略」權能。具有「指定稽核策略」權能的使用者同時具有此兩項權能。

若要指定組織層級的策略，請在 [帳號] 標籤中選取 [組織]，然後從 [指定的稽核策略] 清單中選取策略。

若要指定使用者層級的策略，請執行以下步驟：

1. 按一下 [帳號] 區域中的使用者。
2. 選取使用者表單中的 **[規範遵循]**。
3. 選取 [指定的稽核策略] 清單中之策略。

備註 在對使用者的違規進行修正時，將一律重新計算直接指定給該使用者的稽核策略 (亦即透過使用者帳號或組織指定所指定的策略)。

解決稽核員權能限制

依預設，頂層物件 (物件群組) 中會包含執行稽核作業所需的權能。因此，只有控制頂層的管理員可以指定這些權能給其他管理員。

您可以將權能增加至其他組織，藉此解決此項限制。Identity Manager 提供兩個公用程式 (位於 `sample/scripts` 目錄) 以協助執行此作業。

若要增加所需權能，對 [頂層] 以外的組織執行稽核作業，請執行以下步驟：

1. 執行以下指令列出所有權能 (AdminGroup) 及其相關組織 (物件群組)：

   ```
   beanshell objectGroupUpdate.bsh -type AdminGroup -action list -csv
   ```

   此指令會擷取輸出並匯出爲逗號分隔值 (CSV) 檔案。
2. 可視需要編輯此 CSV 檔案以調整權能的組織位置。
3. 執行此指令以更新 Identity Manager。

```
beanshell objectGroupUpdate.bsh -data CSVFileName -action add -groups NewObjectGroup
```

第 15 章

稽核：監視規範遵循

本章重點在於如何進行稽核檢閱並實作實務，協助您遵循聯邦法規規範。

在本章中，將可瞭解以下概念與作業：

- 稽核策略掃描和報告
- 修正與緩解規範遵循違規
- 定期存取檢閱與驗證
- 存取檢閱修正

稽核策略掃描和報告

此小節提供了有關稽核策略掃描的資訊，以及執行與管理稽核掃描的程序。

掃描使用者與組織

掃描會對個別使用者或組織執行選定的稽核策略。您可能要掃描使用者或組織以查看是否發生了特定違規，或執行未指定給使用者或組織的策略。請從介面的 **[帳號]** 區域中啓動掃描。

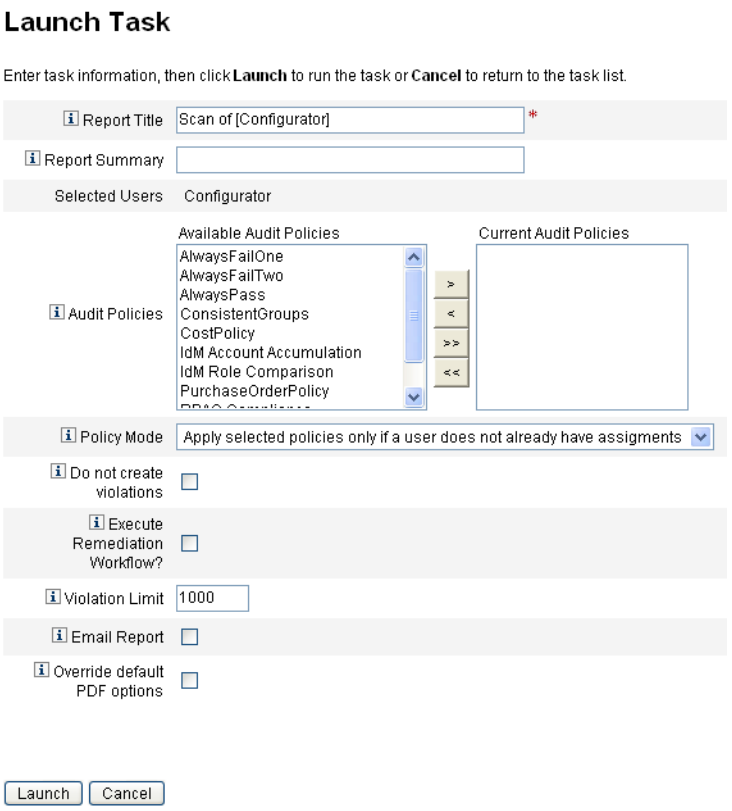
備註 您也可以從 [伺服器作業] 標籤啓動或排程稽核策略掃描。

若要從 [帳號] 區域啓動對使用者帳號或組織的掃描，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[帳號]**。
2. 在 [帳號] 清單中，執行以下任一動作：
   a. 選取一個或多個使用者，然後從 [使用者動作] 選項清單中選取 **[掃描]**。
   b. 選取一個或多個組織，然後從 [組織動作] 選項清單中選取 **[掃描]**。

   螢幕上將顯示 [啓動作業] 對話方塊。圖 15-1 是稽核策略使用者掃描的 [啓動作業] 頁面範例。

圖 15-1 [啓動作業] 對話方塊



3. 在 **[報告標題]** 欄位中指定掃描的標題。這是必填欄位。您可以選擇性地在 **[報告摘要]** 欄位中指定掃描的說明。
4. 選取一個或多個要執行的稽核策略。您必須至少指定一個策略。
5. 選取 **[策略模式]**。這會決定選取的策略將如何與已經具有策略指定的使用者互動。指定可以直接來自使用者或來自使用者被指定到的組織。
6. 選擇性選取 **[不建立違規]** 選項。當您啓用此選項時，將會計算稽核策略並報告違規，但不會建立或更新規範遵循違規，也不會執行修正工作流程。但是，由掃描而產生的作業會顯示應該建立的違規，這樣在測試稽核策略時，此選項會有所幫助。
7. 核取 **[是否執行修正工作流程？]** 以執行稽核策略中指定的修正工作流程。如果稽核策略並未定義修正工作流程，此時便不會執行修正工作流程。

8. 編輯 **[違規限制]** 值，以設定掃描在中斷前可發出之規範遵循違規的最大數目。此值是一種保護機制，可減少因執行在檢查時攻擊性過強的稽核策略所帶來的風險。空值表示不設定限制。
9. 核取 **[電子郵件報告]** 來指定報告的收件者。您也可以讓 Identity Manager 附加包含 CSV (逗號分隔值) 格式的報告的檔案。
10. 如果您想要置換預設的 PDF 選項，請啓用 **[置換預設 PDF 選項]** 選項。
11. 按一下 **[啓動]** 開始掃描。

    若要檢視稽核掃描的結果報告，請檢視 Auditor 報告。

使用 Auditor 報告

Identity Manager 提供了許多 Auditor 報告。下表說明了這些報告。

表 15-1 Auditor 報告說明

Auditor 報告類型	描述
存取檢閱範圍	顯示選取的存取檢閱所意指的各使用者間有何重疊或差異。因為大部分存取檢閱的使用者範圍都是透過查詢或某項成員身份作業進行指定，所以確切的使用者集會隨時間而有所不同。此報告可顯示兩個不同存取檢閱所指定的使用者之間有何重疊和 (或) 差異 (以便查看檢閱在作業中是否有效)；兩個不同存取檢閱所產生的軟體權利文件之間有何重疊和 (或) 差異 (以便查看範圍是否隨時間而變更)；或使用者與軟體權利文件之間有何重疊和 (或) 差異 (以便查看是否已為檢閱範圍內的所有使用者都產生了軟體權利文件)。
存取檢閱的詳細資訊	顯示所有使用者軟體權利文件記錄的目前狀態。可依使用者的組織、存取檢閱與存取檢閱實例、軟體權利文件記錄的狀態和驗證者來篩選此報告。
存取檢閱摘要	提供有關所有存取檢閱的摘要資訊。其概述了所列的每個存取檢閱掃描之已掃描使用者、已掃描策略和驗證作業的狀態。
存取掃描使用者範圍	比較選取的掃描，以判斷哪些使用者包含於掃描範圍內。其將顯示重疊 (包含於所有掃描中的使用者) 或差異 (並未包含於所有掃描中，但包含於多個掃描中的使用者)。嘗試組織多個存取掃描以涵蓋相同或不同使用者時 (視是否需要掃描而定)，此報告很有用。
稽核策略摘要	概述了所有稽核策略的關鍵元素，包括每個策略的規則、修正者和工作流程。
已稽核的屬性	顯示所有指示特定資源帳號屬性變更的稽核記錄。 此報告發掘已儲存之所有可稽核屬性的稽核資料。此報告會找出以任何擴充屬性為基礎的資料，您可以從 WorkflowServices 或標記為可稽核的資源屬性來指定它們。如需有關配置此報告的資訊，請參閱第 488 頁的 「配置已稽核的屬性報告」。
稽核策略違規歷程記錄	在指定時間段內建立的每個策略之所有規範遵循違規的圖形化檢視。可依策略篩選此報告，並依天、週、月或季進行分組。
使用者存取	顯示指定使用者的稽核記錄與使用者屬性。
組織違規歷程記錄	在指定時間段內建立的每個資源之所有規範遵循違規的圖形化檢視。可依組織篩選，並依天、週、月或季進行分組。
資源違規歷程記錄	在指定時間範圍內建立的每個資源之所有規範遵循違規的圖形化檢視。
權責區分	顯示安排在衝突表中的責任分離違規。使用網路型介面，您可以按一下連結來存取額外資訊。 您可依組織篩選此報告，並且可按天、週、月或季對其進行分組。
違規摘要	顯示目前的所有規範遵循違規。您可依修正者、資源、規則、使用者或策略篩選此報告。

您可從 Identity Manager 介面的 [報告] 標籤中取得這些報告。

備註 RULE_EVAL_COUNT 值等於在策略掃描期間計算的規則數目。此值有時會包含在報告中。

Identity Manager 會如下計算 RULE_EVAL_COUNT 值：

掃描的使用者數目 x（策略中的規則數目 + 1）

因爲 Identity Manager 也會計算策略規則 (實際決定是否違反策略的規則)，所以計算中會包含 +1。策略規則會檢查稽核規則結果，並執行布林邏輯以找出策略結果。

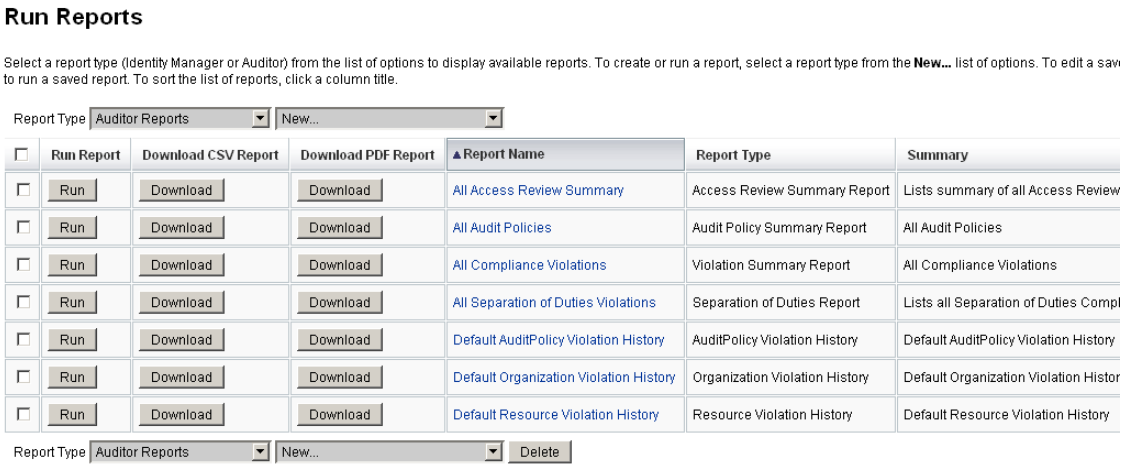
例如，若策略 A 有三個規則，而策略 B 有兩個規則，而且已掃描十位使用者，則 RULE_EVAL_COUNT 值等於 70，原因是 10 位使用者 x (3 + 1 + 2 + 1 個規則)

建立 Auditor 報告

若要執行報告，您必須先建立報告範本。您可爲報告指定各種條件，包括指定接收報告結果的電子郵件收件者。報告範本在建立並儲存後，將顯示在 [執行報告] 頁面中。

圖 15-2 顯示了包含已定義之 Auditor 報告清單的 [執行報告] 頁面範例。

圖 15-2　執行報告頁面選擇



若要建立 Auditor 報告，請執行以下程序：

1. 在管理員介面中，按一下主功能表的 **[報告]**。

   [執行報告] 頁面會隨即開啓。

2. 選取 **[稽核員報告]** 爲報告類型。

3. 在報告的 **[新增]** 清單中，選取一個報告。

[定義報告] 頁面會隨即出現。報告對話方塊的欄位與版面配置會因各種報告類型而異。請參閱 Identity Manager 說明，以取得有關指定報告條件的資訊。

輸入並選取報告條件之後，您可以：

- 執行報告但不儲存 - 按一下 **[執行]** 即可開始執行報告。Identity Manager 不會儲存報告 (如果您已定義新報告) 或變更的報告條件 (如果您已編輯現有報告)。

- 儲存報告 - 按一下 **[儲存]** 以儲存報告。儲存報告後，您可以從 [執行報告] 頁面 (報告清單) 執行此報告。

從 [執行報告] 頁面執行報告後，您可以立即或稍後從 [檢視報告] 標籤中檢視輸出。

- 如需有關排定報告的資訊，請參閱第 271 頁的「排定報告」。

配置已稽核的屬性報告

[已稽核的屬性報告] (請參閱表 15-1 (第 485 頁)) 可報告 Identity Manager 使用者和帳號的屬性層級變更。不過，標準稽核記錄產生的稽核記錄資料，不足以支援完整的查詢表示式。

標準稽核記錄確實會將變更的屬性寫入稽核記錄的 `acctAttrChanges` 欄位中，但寫入已變更屬性的方式，僅能讓報告查詢根據變更的屬性名稱比對記錄。報告查詢無法正確比對屬性值。

您可以指定下列參數，將此報告配置爲比對包含 `lastname` 屬性變更的記錄：

```
Attribute Name = 'acctAttrChanges'

Condition = 'contains'

Value = 'lastname'
```

備註 由於 `acctAttrChanges` 欄位中儲存資料的方式，所以 `Condition='contains'` 爲必要。此欄位不能有多個值。此值基本上就是資料結構，包含所有變更屬性的 `before/after` 值，並使用 `attrname=value` 格式的資料結構。因此，上述設定可讓報告查詢比對 `lastname=`*`xxx`* 的任何實例。

也可以只擷取具有特定屬性 (內含特定值) 的稽核記錄。若要執行此動作，請遵循第 329 頁之「配置 [稽核] 標籤」一節中的程序進行。請選取 **[稽核整個工作流程]** 核取方塊，並按一下 **[增加屬性]** 按鈕，選取您想要記錄的屬性以進行報告，然後按一下 **[儲存]**。

接著，請啓用作業範本配置 (若尚未啓用)。若要執行此動作，請遵循第 300 頁之「啓用作業範本」一節中的程序進行。請勿變更 **[已選取的程序類型]** 清單中之預設值，只要按一下 **[儲存]**。

工作流程現在可提供適合同時比對屬性名稱及其值的稽核記錄。雖然啓動此稽核層級會提供更多資訊，但是請注意這會使效能大幅下滑，且工作流程執行起來會較慢。

修正與緩解規範遵循違規

本小節說明了如何使用 Identity Manager 修正來保護您的重要資產。以下主題討論了 Identity Manager 修正程序的元素：

關於修正

Identity Manager 偵測到未解決 (未緩解) 的稽核策略規範遵循違規時，會建立修正請求，此修正請求必須由修正者 (可以計算和回應稽核策略違規的指定使用者) 加以處理。

修正者上報

Identity Manager 可讓您定義三個層級的修正者上報。修正請求最初會傳送給層級 1 的修正者。如果層級 1 的修正者在逾時期限到期前沒有對修正請求採取任何行動，Identity Manager 會將違規上報至層級 2 的修正者，並開始新的逾時期限。如果第層級 2 的修正者在逾時期限到期前並未回應，則該請求會再次上報至層級 3 的修正者。

若要執行修正，您必須在企業中至少指定一位修正者。您可以選擇是否要爲每個層級指定多位修正者，但是建議您最好這麼做。多位修正者將有助於確保工作流程不會延誤或停滯。

修正安全性存取

這些授權選項適用於 authType `RemediationWorkItem` 類型的工作項目。

- 修正工作項目所有者
- 修正工作項目所有者的直接或間接管理員
- 對修正工作項目所有者所屬組織進行控制的管理員

依預設，授權檢查的運作方式如下：

- 所有者是嘗試執行動作的使用者，或
- 所有者屬於由嘗試執行動作之使用者所控制的組織，或
- 所有者是嘗試執行動作之使用者的從屬

可透過修改以下選項獨立配置第二次和第三次檢查：

- **controlOrg** - 有效值爲 true 或 false。
- **subordinate** - 有效值爲 true 或 false。
- **lastLevel** - 要包括在結果中的最後一個從屬層級；-1 表示所有層級。lastLevel 的整數值預設爲 -1，表示直接與間接的從屬。

可透過以下方法增加或修改這些選項：

`UserForm:Remediation List`

修正工作流程程序

Identity Manager 提供標準修正工作流程，以針對稽核策略掃描提供修正處理。

標準修正工作流程會產生修正請求 (檢閱類型的工作項目，其中包含有關規範遵循違規的資訊)，並向稽核策略中任命的每個層級 1 修正者傳送電子郵件通知。當修正者緩解違規時，工作流程會變更現有規範遵循違規物件的狀態，並爲其指定過期時間。

規範遵循違規僅可透過使用者、策略名稱和規則名稱的組合進行識別。當稽核策略計算爲 true 時，則將爲每個使用者/策略/規則組合建立新的規範遵循違規 (如果目前該組合尚無違規)。如果該組合確實有違規，且該違規處於已緩解狀態，則工作流程程序不會採取任何動作。如果未緩解現有違規，則其重複計數將遞增。

如需有關修正工作流程的更多資訊，請參閱第 456 頁的 「關於稽核策略」。

修正回應

依預設，會爲每位修正者提供三個回應選項：

- **修正 -** 修正者指出已採取行動來修復資源上的問題。

  修改過遵循性違規後，Identity Manager 會建立稽核事件來記錄修正。此外，Identity Manager 還會儲存修正者名稱和所提供的所有註釋。

備註 修正後，直到執行下一次稽核掃描才會刪除違規。若稽核策略配置爲允許重新掃描，則會在修正違規完成時立即重新掃描使用者。

- **緩解 -** 修正者允許違規，並授予使用者在特定期間對此違規免責。

  如果違規是有目的的 (例如，需要兩個群組的商業案例)，您可以長期緩解違規。您也可以短期緩解違規 (例如，當資源的系統管理員在休假中，而您不知道如何修復問題)。

  Identity Manager 會儲存已緩解違規的修正者名稱，並儲存指定給免責的過期日期以及所提供的所有註釋。

備註 當 Identity Manager 偵測到過期的免責時，就會將違規從緩解狀態恢復成擱置狀態。

- **轉寄** - 修正者將解決違規的責任重新指定給另一位人員。

修正範例

您的企業建立了一條規則，規定使用者不能同時負責「應付帳款」與「應收帳款」，而您收到有使用者違反這一規則的通知。

- 如果在公司雇用其他人擔任該職位之前，該使用者是負責這兩種角色的主管，那麼您可以緩解違規，並核發最多六個月的免責。
- 如果使用者違反規定，您可以要求您的 Oracle ERP 管理員來修正衝突，然後在該資源的問題解決後，緩解違規。此外，您可以將修正請求轉寄給 Oracle ERP 管理員。

修正電子郵件範本

Identity Manager 提供「策略違規通知」電子郵件範本 (啓用方法是選取 **[配置]** 標籤，然後選取 **[電子郵件範本]** 子標籤)。您可以將此範本配置爲向修正者通知擱置違規。如需更多資訊，請參閱第 181 頁的「自訂電子郵件範本」。

使用 [修正] 頁面

選取 **[工作項目]**，然後選取 **[修正]** 即可存取 [修正] 頁面。

您可使用此頁面執行以下作業：

- 檢視擱置的違規
- 排定策略違規的優先權
- 緩解一個或多個策略違規
- 修正一個或多個策略違規
- 轉寄一個或多個違規
- 從修正工作項目編輯使用者

檢視策略違規

採取行動之前，您可以先使用 [修正] 頁面檢視有關違規的詳細資訊。

根據您的權能或在 Identity Manager 權能階層中的位置，可能可以檢視其他修正者的違規，並對這些違規採取行動。

以下主題與檢視違規有關：

- 第 493 頁的「檢視擱置請求」
- 第 494 頁的「檢視已完成的請求」
- 第 494 頁的「更新表格」

檢視擱置請求

依預設，指定給您的擱置請求會顯示在 [修正] 表格中。您可以使用 **[列出修正對象]** 選項來檢視其他修正者的擱置修正請求：

- 選取 **[我的直接報告]** 即可檢視組織中直接對您報告之使用者的擱置請求。
- 選取 **[搜尋使用者]**，以輸入或找出您要檢視其擱置請求的一個或多個使用者。輸入使用者 ID，再按一下 **[套用]** 即可檢視該使用者的擱置請求。或者，按一下 **[...](更多)]** 以搜尋使用者。找出使用者並選取該使用者後，請按一下 **[解除]** 以關閉 [搜尋] 區域。

產生的表格會提供以下有關各個請求的資訊：

- **修正者** - 所指定修正者的名稱。只有在您檢視其他修正者的修正請求時，才會顯示此欄。
- **使用者** - 提出請求的使用者。
- **稽核策略/請求** - 請求修正者執行的動作。
- **稽核規則/描述** - 請求的修正註釋。
- **違規狀態** - 違規的目前狀態。
- **嚴重性** - 指定給請求的嚴重性 ([無]、[低]、[中]、[高] 或 [嚴重])
- **優先權** - 指定給請求的優先權 ([無]、[低]、[中]、[高] 或 [緊急])
- **請求日期**：發出修正請求的日期與時間。

備註 每個使用者均可選擇自訂表單，以顯示與該特定修正者相關的修正資料。若要指定自訂表單，請選取使用者表單上的 **[規範遵循]** 標籤。

檢視已完成的請求

若要檢視已完成的修正請求，請按一下 **[我的工作項目]** 標籤，然後按一下 **[歷程記錄]** 標籤。將顯示先前已修正之工作項目的清單。

產生的表格 (由 AuditLog 報告產生) 提供有關每個修正請求的以下資訊：

- **時間戳記 -** 對請求進行修正時的日期與時間
- **主旨 -** 處理請求之修正者的名稱
- **動作 -** 修正者是否已緩解或已修正 請求
- **類型 -** ComplianceViolation 或 UserEntitlement
- **物件名稱 -** 所違反的稽核策略之名稱
- **資源 -** 提供修正者的帳號 ID (或可能顯示爲 [不適用])
- **ID** - 與策略違規相關的帳號 ID。
- **結果 -** 一律顯示爲 [成功]

按一下表格中的時間戳記可開啓 [稽核事件細節] 頁面。

[稽核事件詳細資訊] 頁面提供已完成請求的相關資訊，包括有關修正或緩解、事件參數 (如果適用) 與可稽核的屬性之資訊。

更新表格

若要更新 [修正] 表中提供的資訊，請按一下 **[重新整理]**。[修正] 頁面會使用新的修正請求更新表格。

排定策略違規的優先權

您可以爲策略違規指定優先權與 (或) 嚴重性，以排定其優先權。從 [修正] 頁面爲違規排定優先權。

若要編輯違規的優先權或嚴重性，請執行以下步驟：

1. 從清單中選取一個或多個違規。
2. 按一下 **[排定優先權]**。

   [排定策略違規優先權] 頁面會隨即開啓。
3. 選擇性爲違規設定嚴重性。其選項包括 [無]、[低]、[中]、[高] 或 [嚴重]。
4. 選擇性爲違規設定優先權。其選項包括 [無]、[低]、[中]、[高] 或 [緊急]。
5. 完成選取後，按一下 [確定]。Identity Manager 即可返回修正清單。

備註 只有 CV (規範遵循違規) 類型的修正可設定嚴重性與優先權值。

緩解策略違規

您可以從 [修正] 與 [檢閱策略違規] 頁面緩解策略違規。

從 [修正] 頁面

若要從 [修正] 頁面緩解擱置策略違規，請執行以下步驟：

1. 在表格中選取列以指定要緩解的請求。
   - 啓用一個或多個個別的選項，以指定要緩解的請求。
   - 啓用表格標頭中的選項，以緩解表格中列出的所有請求。

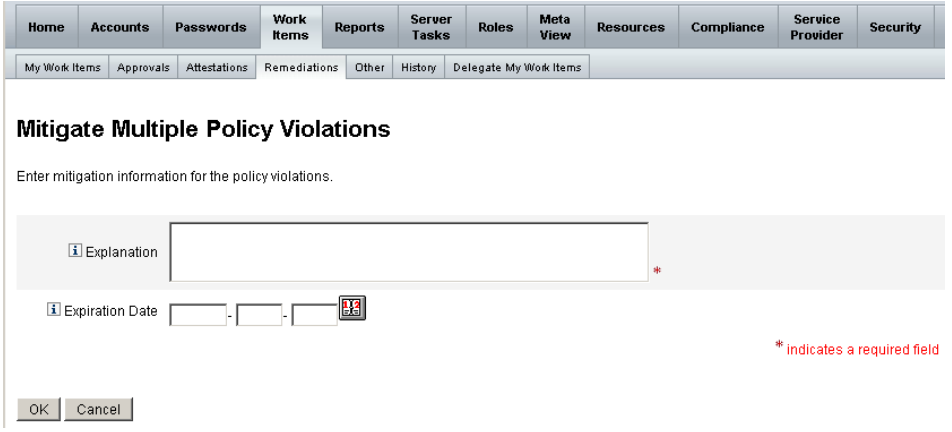
備註 Identity Manager 僅允許您輸入一組說明緩解動作的註釋。除非所有違規都有關聯，而且單一註釋便已足夠，否則您可能不會想要執行批次緩解。

您只能緩解含有規範遵循違規的請求。無法緩解其他修正請求。

2. 按一下 **[緩解]**。

   [緩解策略違規] 頁面 (或 [緩解多項策略違規] 頁面) 會隨即出現：

圖 15-3 [緩解策略違規] 頁面



3. 在 [說明] 欄位中輸入有關緩解的註釋。(這是必填欄位。)

   您的註釋可爲此動作提供稽核線索，因此請務必輸入完整、有用的資訊。例如，說明您緩解策略違規的原因、日期，以及選擇免責期限的原因。

4. 提供免責的過期日期，方法是在 [過期日期] 欄位中直接鍵入日期 (格式爲 **YYYY-MM-DD**)，或按一下日期 按鈕，並從行事曆選取日期。

備註 若未提供日期，免責就會無限期有效。

5. 按一下 **[確定]**，儲存您的變更並回到 [修正] 頁面。

修正策略違規

若要修正一個或多個策略違規，請執行以下步驟：

1. 使用表格中的核取方塊來指定要修正的請求。
   - 啓用表格中的一個或多個個別核取方塊，以指定要修正的請求。
   - 啓用表格標頭中的核取方塊，以修正表格中列出的所有請求。

     如果選取多個請求，請記住 Identity Manager 僅允許輸入一組註釋來說明修正動作。除非所有違規都有關聯，而且單一註釋便已足夠，否則您可能不會想要執行批次修正。

2. 按一下 **[修正]**。
3. 螢幕上將顯示 [修正策略違規] 頁面 (或 [修正多項策略違規] 頁面)。
4. 在 [註釋] 欄位中輸入您有關修正的註釋。
5. 按一下 **[確定]**，儲存您的變更並回到 [修正] 頁面。

備註 在對使用者的違規進行修正時，將一律重新計算直接指定給該使用者的稽核策略 (亦即透過使用者帳號或組織指定所指定的策略)。

轉寄修正請求

您可以將一個或多個修正請求轉寄給另一位修正者。

若要轉寄修正請求，請執行以下步驟：

1. 使用表格中的核取方塊來指定要轉寄的請求。
   - 啓用表格標頭中的核取方塊，以轉寄表格中列出的所有請求。
   - 啓用表格中的個別核取方塊，以轉寄一個或多個請求。
2. 按一下 **[轉寄]**。

   [選取並確認轉寄] 頁面會隨即出現。

   圖 15-4 [選取並確認轉寄] 頁面

3. 在 [轉寄給] 欄位中輸入修正者名稱，然後按一下 **[確定]**。或者，您也可以按一下 **[...]** (更多)] 以搜尋修正者名稱。從搜尋清單中選取名稱，然後按一下 **[設定]** 即可在 [轉寄給] 欄位中輸入該名稱。按一下 **[解除]** 以關閉 [搜尋] 區域。

再次顯示 [修正] 頁面時，新修正者的名稱即會顯示在表格的 [修正者] 欄中。

從修正工作項目編輯使用者

從修正工作項目中，您可以 (需具有適當的使用者編輯權能) 編輯使用者以修正問題，如相關軟體權利文件歷程記錄所說明。

若要編輯使用者，請從 [檢閱修正請求] 頁面按一下 **[編輯使用者]**。[編輯使用者] 頁面會隨即出現，其中顯示：

- 適用於此工作項目並與使用者相關聯的軟體權利文件歷程記錄
- 使用者的屬性。此處所出現的選項，與 [帳號] 區域中所提供的 [編輯使用者] 表單上所顯示的選項相同。

對使用者進行變更後，請按一下 **[儲存]**。

備註 儲存使用者編輯項目後，將使得 [更新使用者] 工作流程開始執行。因爲此工作流程可能需要經過核准，所以在儲存使用者帳號的變更之後，可能有一段時間這些變更無法生效。若稽核策略允許重新掃描，而 [更新使用者] 工作流程尚未完成，則後續的策略掃描可能會偵測到相同的違規。

定期存取檢閱與驗證

Identity Manager 提供執行存取檢閱的程序，存取檢閱可讓管理員或其他責任方檢閱和驗證使用者存取權限。此程序有助於識別與管理隨時間積累的使用者權限，還有助於維護對「沙賓法案 (SOX)」、「美國金融服務現代化法案 (GLBA)」與其他聯邦法規的規範遵循。

存取檢閱可在您需求時執行，或排程爲定期進行 (例如每個行事曆季度執行一次)，從而讓您可以執行定期存取檢閱來維護使用者權限的正確層級。存取檢閱可選擇性包括稽核策略掃描。

關於定期存取檢閱

定期存取檢閱是定期執行的程序，用於驗證一組員工在指定的時間對相應資源是否具有相應的權限。

定期存取檢閱涉及以下作業：

- 存取檢閱掃描 - 執行使用者軟體權利文件之規則型評估的掃描，可決定是否需要驗證。
- 驗證 - 透過核准或拒絕使用者軟體權利文件回應驗證請求的程序。

使用者軟體權利文件是一組特定資源上使用者帳號的詳細記錄。

存取檢閱掃描

若要啓動定期存取檢閱，您必須至少先定義一個存取掃描。

存取掃描可定義要掃描的對象、掃描中所包括的資源、掃描期間要計算的所有選用性稽核策略，以及用於確定要手動驗證哪些軟體權利文件記錄和由誰執行驗證的規則。

存取檢閱工作流程程序

一般而言，Identity Manager 存取檢閱工作流程會執行下列作業：

- 建構使用者清單、取得每個使用者的帳號資訊，以及計算選用性稽核策略
- 建立使用者軟體權利文件記錄
- 確定是否需要驗證每個使用者軟體權利文件記錄
- 爲每個驗證者指定工作項目
- 等待所有驗證者核准，或等待首次拒絕
- 如果在指定逾時期限內未收到對請求的任何回應，則上報至下一個驗證者
- 使用解決方案更新使用者軟體權利文件記錄

如需修正權能的描述，請參閱第 519 頁的 「存取檢閱修正」。

必要的管理員權能

若要執行定期存取檢閱並管理檢閱程序，則使用者必須具有「稽核員定期存取檢閱管理員」權能。具有 Auditor 存取掃描管理員權能的使用者可以建立並管理存取掃描。

若要指定這些權能，請編輯使用者帳號並修改安全性屬性。如需有關這些權能和其他權能的更多資訊，請參閱第 215 頁的 「瞭解與管理權能」。

驗證

驗證是由一個或多個指定驗證者執行的認證程序，可確認在特定日期使用者軟體權利文件是否存在。存取檢閱期間，驗證者會透過電子郵件通知接收存取檢閱驗證請求的通知。驗證者必須是 Identity Manager 使用者，但無需是 Identity Manager 管理員。

驗證工作流程

Identity Manager 使用在存取掃描識別到需要檢閱之軟體權利文件記錄時啓動的驗證工作流程。存取掃描會根據該存取掃描中所定義的規則做出此決定。

存取掃描計算的規則可確定是否需要手動驗證使用者軟體權利文件記錄，或是否可以自動核准或拒絕該記錄。如果需要手動驗證使用者軟體權利文件記錄，則存取掃描將使用第二個規則來確定誰是適當的驗證者。

每個要手動驗證的使用者軟體權利文件記錄都將指定給工作流程，每位驗證者負責一個工作項目。可使用 ScanNotification 工作流程將這些工作項目的通知傳送給驗證者，該工作流程會針對每個掃描、每個驗證者將項目隨附在一個通知中。除非已選取 ScanNotification 工作流程，否則通知將針對使用者軟體權利文件。這表示驗證者可針對每個掃描收到多份通知，並且其數目可能很大，這取決於掃描的使用者數目。

驗證安全性存取

這些授權選項適用於 authType `AttestationWorkItem` 類型的工作項目。

- 工作項目所有者
- 工作項目所有者的直接或間接管理員
- 控制工作項目所有者所屬組織的管理員
- 已透過認證檢查進行驗證的使用者

依預設，授權檢查的運作方式如下：

- 所有者是嘗試動作的使用者，或
- 所有者屬於嘗試動作之使用者所控制的組織，或
- 所有者是嘗試動作之使用者的從屬。

可透過修改以下表單特性獨立配置第二次和第三次檢查：

- `controlOrg` - 有效值爲 true 或 false
- `subordinate` - 有效值爲 true 或 false
- `lastLevel` - 要包括在結果中的最後一個從屬層級；-1 表示所有層級

`lastLevel` 的整數值預設爲 1，表示直接與間接的從屬。

可透過以下方法增加或修改這些選項：

`UserForm:AccessApprovalList`

備註 若將驗證作業的安全性設爲由組織進行控制，則還需要「稽核員驗證者」權能，才可以修改其他使用者的驗證。

委託驗證

依預設，存取掃描工作流程會優先處理使用者針對驗證工作項目與通知所建立的 [存取檢閱驗證作業] 與 [存取檢閱修正] 等類型的工作項目委派。存取掃描管理員可取消選取 [遵循委派] 選項來忽略委派設定。如果驗證者已將所有工作項目委託給其他使用者，但是沒有針對存取檢閱掃描設定 [遵循委派] 選項，則驗證者 (而非負責處理該委派的指定使用者) 將收到驗證請求通知和工作項目。

計劃定期存取檢閱

對於任何企業來說，存取檢閱可能都是費時費力的程序。Identity Manager 定期存取檢閱程序可自動執行存取檢閱程序的許多部分，從而有助於將涉及的成本與時間降至最低。然而，某些程序仍很耗費時間。例如，從許多位置中擷取成千上萬使用者之使用者帳號資料的程序就可能需要相當長的時間。手動驗證記錄的動作也將很耗費時間。合理的計劃可提昇程序效率，從而大大降低投入。

計劃定期存取檢閱時請考慮以下注意事項：

- 根據所涉及使用者和資源數量的不同，掃描時間可能會有很大差異。

  一個大型組織執行單一定期存取檢閱時，可能要花費一天或幾天的時間進行掃描，而且完成手動驗證可能還要花費一週或幾週的時間。

  例如，根據以下計算，對於一個具有 50,000 名使用者與十個資源的組織，完成存取掃描可能需要大約一天的時間：

  1 秒/資源 * 50K 名使用者 * 10 個資源 / 5 個同步運作執行緒 = 28 小時

  如果資源分散在各地，則可能因網路延時而增加處理時間。

- 使用多個 Identity Manager 伺服器進行並列處理可加快存取檢閱程序的速度。

  當各掃描的資源不同時，執行並列掃描最有效。定義存取檢閱時，請建立多個掃描並將資源限制爲特定資源集，以對每個掃描使用不同的資源。然後在啓動作業時，選取多個掃描並將其排定爲立即執行。

- 自訂驗證工作流程與規則可讓您獲得更好的控制力，並可提高效率：

  例如，自訂驗證者規則可將驗證責任分配給多個驗證者。驗證程序據此指定工作項目並傳送通知。

- 使用驗證者上報規則可協助縮短對驗證請求的回應時間。

  設定預設上報驗證者規則，或使用自訂的規則可設定驗證者上報鏈。還可指定上報逾時時間值。

- 瞭解如何使用檢閱確定規則自動確定哪些軟體權利文件記錄需手動檢閱，以節省時間。

- 透過指定掃描層級通知工作流程來隨附掃描的驗證請求通知。

調校掃描作業

在掃描程序期間，有多個執行緒會存取使用者的檢視，而可能存取使用者具有帳號的資源。在完成存取檢閱後，會計算多個稽核策略與規則，這可能導致發生規範遵循違規。

爲防止兩個執行緒同時更新同一個使用者檢視，該程序會針對此使用者名稱建立常駐記憶體鎖定。若無法在 5 秒 (預設值) 內建立此鎖定，即會在掃描作業中寫入錯誤，並且會略過使用者，藉以防止同一組使用者同時進行掃描處理。

您可以編輯數個「可調校參數」的值，這些參數可作爲掃描作業的作業引數：

- `clearUserLocks` (布林值) - 若爲 true，則所有目前的使用者鎖定都會在掃描啓動前解除。
- `userLock` (整數值) - 嘗試鎖定使用者時所等候的時間 (以毫秒爲單位)。預設值爲 5 秒。負數值會停用對該掃描的鎖定。
- `scanDelay` (整數值) - 派送掃描執行緒之間所暫停的時間 (以毫秒爲單位)。預設值爲 0 (無延遲)。若您爲此引數設定了值，掃描即會變慢，但系統對其他作業的回應能力將變強。
- `maxThreads` (整數值) - 用於處理掃描之同步運作執行緒的數目。預設值爲 5。若資源的回應速度非常慢，則增加此數值或許可上報掃描流量。

若要變更這些參數值，請編輯對應的 [作業定義] 表單。如需有關此作業的更多資訊，請參閱「Identity Manager Workflows, Forms, and Views」。

建立存取掃描

若要定義存取檢閱掃描，請執行以下步驟：

1. 選取 **[規範遵循]**，然後選取 **[管理存取掃描]**。
2. 按一下 **[新增]**，以顯示 [建立新的存取掃描] 頁面。
3. 爲存取掃描指定名稱。

備註 存取掃描名稱不能包含以下字元：

' (所有格符號)、. (點號)、| (管線符號)、[(左括號)、] (右括號)、, (逗號)、: (冒號)、$ (美元符號)、" (雙引號)、\ (反斜線) 或 = (等號)。

也應避免下列字元：_ (底線)、% (百分比符號)、^ (指數符號) 和 * (星號)。

4. 選擇性增加有助於識別掃描的描述。
5. 選擇性啓用 **[動態軟體權利文件]** 選項。若啓用此選項，則會爲驗證者提供以下額外選項：
   - 可立即重新掃描擱置的驗證，以重新整理軟體權利文件資料並重新計算驗證需求。
   - 可將擱置的驗證路由至另一位使用者以進行修正。在修正後會重新整理並重新計算軟體權利文件資料，以判斷是否需要進行此驗證。
6. 從以下選項中選取 **[使用者範圍類型]**：(這是必填欄位。)
   - **根據屬性條件規則 -** 選擇此選項即可根據所選 [使用者範圍類型] 掃描使用者。Identity Manager 提供下列預設規則：
     - 全部管理員
     - 我的所有報告
     - 所有非管理員
     - 我的直接報告
     - 無管理員的使用者

備註 您可以使用 Identity Manager Integrated Development Environment (IDE) 增加使用者範圍設定規則。如需有關 IDE 的資訊，請參閱第 60 頁的「Identity Manager IDE」。

- **已指定給資源 -** 選擇此選項可以掃描所有在一個或多個所選取資源上具有帳號的使用者。當您選擇此選項時，此頁面會顯示 [使用者範圍資源]，讓您指定資源。
- **根據特定角色** - 選擇此選項可掃描所有成員，這些成員至少擁有您指定的一個角色，或擁有您指定的所有角色。
- **組織成員** - 選擇此選項即可掃描一個或多個所選組織的所有成員。
- **給管理員的報告** - 選擇此選項即可掃描向所選管理員報告的所有使用者。管理員階層由使用者的 Lighthouse 帳號之 Identity Manager 屬性決定。

如果使用者範圍是組織或管理員，則 [是否爲遞迴範圍] 選項可用。此選項允許透過受控制成員鏈遞迴選取使用者。

7. 如果您還選擇在存取檢閱掃描期間掃描稽核策略以偵測違規，請將您選取的項目從 [可用稽核策略] 移至 [目前的稽核策略] 清單，以選取要套用至此掃描的稽核策略。

   將稽核策略增加至存取掃描會導致對同一使用者集採用與執行稽核掃描相同的運作方式。但是，除此之外，稽核策略偵測到的所有違規還會儲存在使用者軟體權利文件記錄中。此資訊可使自動核准或拒絕更簡便，因爲此規則可將使用者軟體權利文件記錄中違規的存在與否作爲其邏輯的一部分。

8. 如果已掃描前述步驟中的稽核策略，則可以使用 **[策略模式]** 選項，指定存取掃描如何確定要針對指定使用者所執行的稽核策略。可同時爲使用者指定使用者層級和/或組織層級的策略。預設存取掃描運作方式爲，僅當使用者尚未具有任何指定的策略時才套用爲存取掃描指定的策略。

   a. 套用選取的策略並忽略其他指定的策略

   b. 僅在使用者尚未具有指定的策略時才套用已選取的策略

   c. 同時套用選取的策略和爲使用者指定的策略

9. (選擇性) 指定**[檢視程序所有者]**。使用此選項可指定定義之存取檢閱作業的所有者。如果已指定檢閱程序所有者，則回應驗證請求時可能遇到衝突的使用者在核准或拒絕使用者軟體權利文件時可棄權，從而將驗證請求轉寄給檢閱程序所有者。按一下選取 (省略號) 方塊可搜尋使用者帳號並進行選取。

10. **遵循委派** - 選取此選項即可爲存取掃描啓用委派。如果已核取此選項，則存取掃描將僅遵循委派設定。依預設，啓用 [遵循委派]。

11. **限制目標資源** - 選取此選項即可限制要掃描的目標資源。

    此設定可直接影響存取掃描的效率。如果未限制目標資源，則每個使用者軟體權利文件記錄都將包含使用者連結之每個資源的帳號資訊。這表示在掃描期間，將查詢每個使用者的每個指定資源。透過使用此選項指定資源子集，您可以大大縮短 Identity Manager 建立使用者軟體權利文件記錄所需的處理時間。

12. **執行違規修正** - 選取此選項即可在偵測到違規時，啓用稽核策略的修正工作流程。

    選取此選項後，如果針對任何指定的稽核策略偵測到違規，都將導致執行相應的稽核策略修正工作流程。

    此選項通常不應選取，除非情況較爲複雜。

13. **存取核准工作流程** - 選取預設的標準驗證作業工作流程，或選取自訂的工作流程 (如果適用)。

    此工作流程用於將要檢閱的使用者軟體權利文件記錄顯示給適當的驗證者 (由驗證者規則確定)。預設的標準驗證工作流程將爲每個驗證者建立一個工作項目。若存取掃描指定上報，則此工作流程會負責上報休止時間太久的工作項目。若未指定工作流程，則使用者驗證會無限期地保持在擱置狀態。

備註 「Identity Manager Deployment Tools」一書包含 Identity Auditor 規則、自訂它們的方式以及原因的詳細資訊。請參閱「Working with Rules」一章之「Customizing Default Rules and Rule Libraries」小節的「Auditor Rules」主題。

14. **驗證者規則** - 選取預設驗證者規則，或選取自訂驗證者規則 (如果適用)。

    將使用者軟體權利文件記錄作爲輸入提供給驗證者規則，該規則將傳回驗證者名稱清單。如果選取 [遵循委派]，則存取掃描會遵循原始名稱清單中每個使用者配置的委派資訊，將名稱清單轉送給適當的使用者。如果 Identity Manager 使用者的委派導致路由循環，則會捨棄委派資訊，並將工作項目傳送至最初的驗證者。預設驗證者規則指出驗證者應是軟體權利文件記錄所表示之使用者的管理員 (idmManager)，或是配置程式帳號 (如果該使用者的 `idmManager` 爲空)。如果驗證需涉及資源所有者與管理員，則必須使用自訂規則。如需有關自訂驗證者規則的資訊，請參閱「Identity Manager Deployment Tools」一書。

15. **驗證者上報規則** - 使用此選項，可指定預設上報驗證者規則，或選取自訂規則 (如果適用)。您還可以指定規則的上報逾時時間值。預設的上報逾時時間值爲 0 天。

    此規則可指定已超過上報逾時期間之工作項目的上報鏈。預設上報驗證者規則會上報指定至驗證者的管理員 (`idmManager`) 或配置程式 (如果驗證者的 `idmManager` 值爲空)。

    您可以分鐘、小時或天指定上報逾時時間值。

    「Identity Manager Deployment Tools」一書包含有關「驗證者上報規則」的額外資訊。

16. **檢閱確定規則** - 選取以下任一規則，以指定掃描程序如何確定軟體權利文件記錄的處理方式：(這是必填欄位。)

    - **拒絕已變更的使用者** - 如果某個使用者軟體權利文件記錄與同一存取掃描定義中的上一個使用者軟體權利文件不同，且已核准上一個使用者軟體權利文件，則自動拒絕該記錄。否則，強制執行手動驗證，並核准與先前已核准之使用者軟體權利文件相同的所有使用者軟體權利文件。依預設，此規則只會比較使用者檢視的「帳號」部分。
    - **檢閱已變更的使用者** - 如果任何使用者軟體權利文件記錄與同一存取掃描定義中的上一個使用者軟體權利文件不同，且已核准上一個使用者軟體權利文件，則對該記錄強制執行手動驗證。核准與先前已核准之使用者軟體權利文件相同的所有使用者軟體權利文件。依預設，此規則只會比較使用者檢視的「帳號」部分。
    - **檢閱全部** - 對所有使用者軟體權利文件記錄強制執行手動驗證。

備註 拒絕變更的使用者和檢閱變更的使用者規則將使用者軟體權利文件與核准軟體權利文件記錄之相同存取掃描的上一個實例相比較。

您可以透過複製和修改規則來變更該運作方式，將比較限定在任何選取的使用者檢視部分。請參閱「Identity Manager Deployment Tools」以取得有關自訂規則的資訊。

此規則可能傳回的值包括：

- -1 - 不需要驗證
- 0 - 自動拒絕驗證
- 1 - 必須手動驗證
- 2 - 自動核准驗證
- 3 - 自動修正驗證 (自動修正)

「Identity Manager Deployment Tools」一書包含有關 「檢閱決定規則」的額外資訊。

17. **修正者規則** - 選取規則以用於決定在執行自動修正時，誰應修正特定使用者的軟體權利文件。該規則可檢查使用者目前的使用者軟體權利文件與違規，且必須傳回應執行修正作業之使用者的清單。如果未指定規則，則不會進行修正。此規則經常用於軟體權利文件發生規範遵循違規的情況。

    「Identity Manager Deployment Tools」一書包含有關 「修正者規則」的額外資訊。

18. **修正使用者表單規則 -** 選取規則以用於在編輯使用者時，選取要用來驗證修正者的適當表單。修正者可設定其自己的表單，而置換此表單。若掃描收集要與自訂表單相符的特定資料，請設定此表單規則。

    「Identity Manager Deployment Tools」一書包含有關「檢閱決定規則」的額外資訊。

19. **通知工作流程** - 選取以下任一選項即可指定每個工作項目的通知運作方式。

    - **無** - 此爲預設選項。此選項可讓驗證者收到針對其必須驗證之每個個別使用者軟體權利文件的電子郵件通知。
    - **ScanNotification** - 此選項可將所有驗證請求隨附在單一通知中。通知可指示爲收件者指定了多少驗證請求。

      如果存取掃描中指定了檢閱程序所有者，則當掃描開始和結束時，ScanNotification 工作流程還將向檢閱程序所有者傳送通知。請參閱步驟 9。

      ScanNotification 工作流程使用以下電子郵件範本

      - 存取掃描開始通知
      - 存取掃描結束通知
      - 批次驗證通知

      您可以自訂 ScanNotification 工作流程。

20. **違規限制** - 使用此選項，可指定掃描在中斷前可發出之規範遵循違規的最大數目。預設限制爲 1000。欄位爲空則表示無限制。

    儘管在稽核掃描或存取掃描期間，策略違規數通常會比使用者數少很多，但設定此值可防止會導致違規數大量增加之不完善策略所帶來的不良影響。例如，考慮以下情況：

    如果存取掃描涉及 50,000 名使用者，並針對每個使用者產生兩到三個違規，則每個規範遵循違規的修正成本將對 Identity Manager 系統產生不良影響。

21. **組織** - 選取可使用該存取掃描物件的組織。這是必填欄位。

按一下 **[儲存]**，以儲存掃描定義。

刪除存取掃描

您可以刪除一個或多個存取掃描。若要刪除存取掃描，請從 **[規範遵循]** 標籤中選取 **[管理存取掃描]**，再選取掃描的名稱，然後按一下 **[刪除]**。

管理存取檢閱

定義存取掃描後，即可將其作爲存取檢閱的一部分使用或進行排程。啓動存取檢閱後，將有多個選項可用於管理檢閱程序。如需相關資訊，請參閱以下各節：

- 啓動存取檢閱
- 排程存取檢閱作業
- 管理存取檢閱進度
- 修改掃描屬性
- 取消存取檢閱

啟動存取檢閱

若要從管理員介面啓動存取檢閱，請使用下列其中一種方法：

- 從 **[規範遵循] > [存取檢閱]** 頁面，按一下 **[啓動檢閱]**。
- 在 **[伺服器作業] > [執行作業]** 頁面中，選取 [存取檢閱] 作業。

在所顯示的 [啓動作業] 頁面中，指定存取檢閱的名稱。從 [可用的存取掃描] 清單中選取掃描，然後將其移至 [已選取] 清單。如果您選取多個掃描，則可以選擇以下任一啓動選項：

- **立即** - 若選取此選項，則會在您按一下 [啓動] 按鈕後立即開始執行掃描。如果您在 [啓動作業] 中爲多個掃描選取該選項，則掃描將並列執行。
- **需等待** - 此選項可讓您指定啓動掃描前要等待的時間，該時間與存取檢閱作業的啓動有關。

備註 您可以在存取檢閱階段作業期間啓動多個掃描。但是，由於每個掃描可能都涉及大量使用者，因此掃描程序可能需要好幾個小時才能完成。最佳實踐表明您應分別管理掃描。例如，您可以啓動一個掃描以使其立即執行，而交錯排定其他掃描。

按一下 **[啓動]**，以啓動存取檢閱程序。

備註 您爲存取檢閱指定的名稱很重要。某些報告可以對具有相同名稱之定期執行的存取檢閱進行比較。

當您啓動存取檢閱時，螢幕上將顯示工作流程程序圖以說明該程序的步驟。

排程存取檢閱作業

您可從 [伺服器作業] 區域排定存取檢閱作業。例如，若要設定需定期執行的存取檢閱，請選取 **[管理排程]**，然後定義排程。您可以將作業排定爲每月或每季發生一次。

若要定義排程，請在 [排程作業] 頁面中選取 [存取檢閱] 作業，然後在 [建立作業排程] 頁面中填入資訊。

按一下 **[儲存]** 儲存已排定的作業。

備註 依預設，Identity Manager 可將存取檢閱作業的結果保留一週。如果您選擇將某個檢閱排程爲一週執行多次，請將 [結果選項] 設定爲 [刪除]。如果未將 [結果選項] 設定爲 [刪除]，則不會執行新檢閱，因爲先前作業的結果仍然存在。

管理存取檢閱進度

使用 **[存取檢閱]** 標籤即可監視存取檢閱的進度。透過 **[規範遵循]** 標籤存取該功能。

您可以透過 **[存取檢閱]** 標籤，檢閱所有使用中的和先前已處理的存取檢閱之摘要。提供了所列之每個存取檢閱的以下資訊：

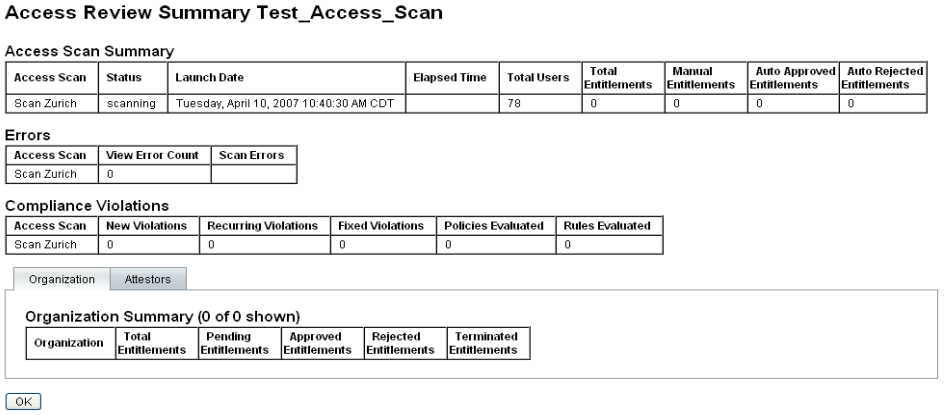
- **狀態** - 檢閱程序的目前狀態：正在啓動、正在終止、已終止、正在執行數個掃描、已排定數個掃描、正在等待驗證或已完成。
- **啓動日期** - 啓動存取檢閱作業的日期 (時間戳記)。
- **使用者總數** - 要掃描的使用者之總數。
- **軟體權利文件詳細資訊** - 表格中附加的一些欄，依狀態提供軟體權利文件總數。其中包括擱置、已核准、已拒絕、已終止與已修正的軟體權利文件之詳細資訊，以及軟體權利文件總數。

  [已修正] 欄可指出目前處於「正在修正」狀態的軟體權利文件數目。軟體權利文件經修正後會成爲「擱置」狀態，因此在存取檢閱結束時，此欄的值將變爲零。

若要檢視有關檢閱的更詳細資訊，請選取該檢閱以開啓摘要報告。

圖 15-5 顯示了存取檢閱摘要的範例報告。

圖 15-5 存取檢閱摘要報告頁面



按一下 **[組織]** 或 **[驗證者]** 表單標籤，以檢視依這些物件分類的掃描資訊。

您還可以執行存取檢閱摘要報告，以檢閱和下載報告中的此資訊。

修改掃描屬性

設定存取掃描後，您可以編輯掃描以指定新選項，例如指定在執行存取掃描時要掃描的目標資源，或要針對其掃描違規的稽核策略。

若要編輯掃描定義，請從 [存取掃描] 清單中選取該掃描，然後在 [編輯存取檢閱掃描] 頁面中修改屬性。

您必須按一下 **[儲存]** 才能儲存對掃描定義所做的所有變更。

備註 變更存取掃描的範圍可能會變更最新取得之使用者軟體權利文件記錄中的資訊，因爲此項變更會影響[檢閱確定規則] (如果此規則對使用者軟體權利文件與舊的使用者軟體權利文件記錄進行比較)。

取消存取檢閱

在 **[存取檢閱]** 頁面中按一下 **[終止]**，即可停止進行中的所選檢閱。終止檢閱將導致執行以下動作：

- 取消排定所有已排定的掃描
- 停止所有正在執行的掃描
- 刪除所有擱置的工作流程和工作項目
- 所有擱置驗證者都會標記爲已取消
- 將使用者完成的所有驗證保留不變

刪除存取檢閱

在 [存取檢閱] 頁面中按一下 **[刪除]**，即可刪除所選檢閱。

如果存取檢閱作業的狀態爲已終止或已完成，則您可以刪除該作業。您必須先終止進行中的存取檢閱作業，才能將其刪除。

刪除存取檢閱作業將刪除該檢閱產生的所有使用者軟體權利文件記錄。刪除動作將記錄在稽核記錄中。

若要刪除存取檢閱，請在 [存取檢閱] 頁面中按一下 **[刪除]**。

備註 取消及刪除存取檢閱將導致更新大量 Identity Manager 物件與作業，這可能需要數分鐘才能完成。您可以在 **[伺服器作業] > [全部作業]** 中檢視作業結果，以檢查作業進度。

管理驗證責任

您可以透過 Identity Manager 管理員或使用者介面管理驗證請求。本小節提供有關回應驗證請求以及驗證中所涉及之責任的資訊。

存取檢閱通知

如果驗證請求需要驗證者的核准，則在掃描期間 Identity Manager 會向驗證者傳送通知。如果已委託驗證者責任，則請求會被傳送給受委託人。如果定義了多個驗證者，則每個驗證者都將收到一份電子郵件通知。

請求將在 Identity Manager 介面中顯示爲 **[驗證]** 工作項目。當指定的驗證者登入 Identity Manager 時，將顯示擱置的驗證工作項目。

檢視擱置請求

從介面的 [工作項目] 區域檢視驗證工作項目。選取 [工作項目] 區域中的 **[驗證]** 標籤，可列出所有需要核准的軟體權利文件記錄。在 [驗證作業] 頁面中，您還可以針對所有直接給您的報告和您可直接或間接控制的特定使用者，列出其軟體權利文件記錄。

根據軟體權利文件記錄執行動作

驗證工作項目包含需要檢閱的使用者軟體權利文件記錄。軟體權利文件記錄提供有關使用者存取權限、指定的資源及策略違規的資訊。

以下是對驗證請求的可能回應：

- **核准** - 驗證自軟體權利文件記錄中所記錄的日期開始，軟體權利文件是適用的。
- **拒絕** - 軟體權利文件記錄指出目前無法驗證或修正的可能差異。
- **重新掃描** - 請求重新掃描，以重新計算使用者的軟體權利文件。
- **轉寄** - 可讓您爲檢閱指定其他收件者。
- **棄權** - 對此記錄的驗證不適用，並且尚未發現更適當的驗證者。驗證工作項目將轉寄至檢閱程序所有者。僅當存取檢閱作業中已定義檢閱程序所有者時，才可使用此選項。

如果在指定的上報逾時期間之前，驗證者未採取以上任一動作來回應請求，則會將通知傳送至上報鏈中的下一個驗證者。直到記錄回應後通知程序才會停止。

您可以透過 **[規範遵循] > [存取檢視]** 標籤監視驗證狀態。

封閉迴圈修正

您可以透過下列方式避免拒絕使用者軟體權利文件：

- 將軟體權利文件標記爲必須請求其他使用者進行更正 (即「請求修正」)。在此情況下，會建立新的修正工作項目，並將其指定給一個或多個指定的修正者。

  接著，新的修正者可選擇編輯使用者 (使用 Identity Manager 或獨立編輯)，然後在工作項目達到要求後將其標記爲已修正。屆時會重新掃描並再次計算使用者的軟體權利文件。

- 請求對軟體權利文件進行重新評估 (重新掃描)。在此情況下，會重新掃描並重新計算使用者軟體權利文件。原始驗證工作項目會結束。若根據存取掃描中所定義的規則仍需要驗證軟體權利文件，則會建立新的驗證工作項目。

請求修正

您可以將擱置的驗證路由至其他使用者以進行修正 (如果存取掃描已定義此作業)。

備註 [建立存取掃描] 或 [編輯存取掃描] 頁面上的 [動態軟體權利文件] 選項可啓用此功能。

若要請求其他使用者進行修正，請執行以下步驟：

1. 從驗證清單中選取一個或多個軟體權利文件，然後按一下 **[請求修正]**。

   [選取並確認請求修正] 頁面會隨即出現。

2. 輸入使用者名稱，然後按一下 **[增加]** 即可將該使用者增加至 [轉寄給] 欄位中。或者，您也可以按一下 **[...]**(更多) 以搜尋使用者。選取搜尋清單中的使用者，然後按一下 **[增加]**，將該使用者增加至 [轉寄給] 清單中。按一下 **[解除]** 以關閉 [搜尋] 區域。

3. 在 [註釋] 欄位中輸入註釋，然後按一下 **[繼續]**。

   Identity Manager 會返回至驗證清單。

備註 修正請求的詳細資訊會出現在個別使用者軟體權利文件的 [歷程記錄] 區域中。

重新掃描驗證

您可以對擱置的驗證進行重新掃描與重新計算 (如果存取掃描已定義此作業)。

備註 [建立存取掃描] 或 [編輯存取掃描] 頁面上的 [動態軟體權利文件] 選項可啓用此功能。

若要重新掃描擱置的驗證，請執行以下步驟：

1. 從驗證清單中選取一個或多個軟體權利文件，然後按一下 **[重新掃描]**。

   [重新掃描使用者軟體權利文件] 頁面會隨即出現。

2. 在 [註釋] 區域中輸入重新掃描動作的相關註釋，然後按一下 **[繼續]**。

轉寄驗證工作項目

您可以將一個或多個驗證工作項目轉寄給其他使用者。

若要轉寄驗證作業，請執行以下步驟：

1. 在驗證清單中選取一個或多個工作項目，然後按一下 **[轉寄]**。

   [選取並確認轉寄] 頁面會隨即出現。

2. 在 [轉寄給] 欄位中輸入使用者名稱。或者，您也可以按一下 **[...]**(更多) 以搜尋使用者名稱。

3. 在 [註釋] 欄位中輸入轉寄動作的相關註釋。

4. 按一下 **[繼續]**。

   Identity Manager 會返回至驗證清單。

備註 轉寄動作的詳細資訊會出現在個別使用者軟體權利文件的 [歷程記錄] 區域中。

以數位方式簽署存取檢閱動作

您可以設定數位簽署以處理存取檢閱動作。如需有關配置數位簽署的資訊，請參閱第 235 頁的「簽署核准」。該小節討論的主題說明了將憑證和 CRL 增加至 Identity Manager 以取得簽署的核准所需之伺服器端配置和用戶端配置。

存取檢閱報告

Identity Manager 提供以下報告，可讓您計算存取檢閱的結果：

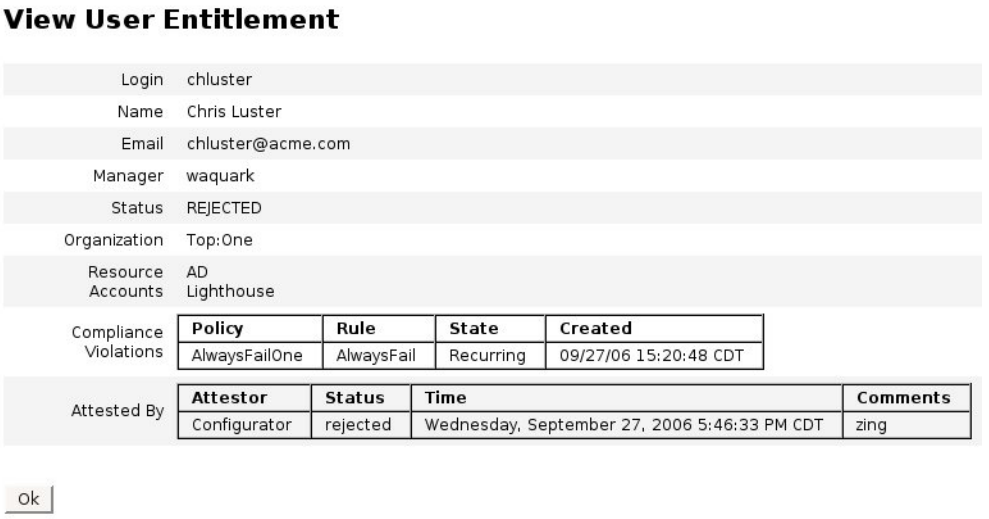
- **存取檢閱範圍報告** - 此報告可以視報告的定義方式，使用表格格式提供下列資訊：
  - **名稱** - 使用者軟體權利文件有所重疊及 (或) 差異的使用者清單

  此報告也可能會包含附加欄，以顯示包含重疊及 (或) 差異的存取檢閱。

- **存取檢閱詳細資訊報告** - 該報告以表格的格式提供以下資訊：
  - **名稱** - 使用者軟體權利文件記錄的名稱
  - **狀態** - 檢閱程序的目前狀態：正在啓動、正在終止、已終止、正在執行數個掃描、已排定數個掃描、正在等待驗證或已完成
  - **驗證者** - 指定作爲記錄之驗證者的 Identity Manager 使用者
  - **掃描日期** - 記錄掃描何時發生的時間戳記
  - **處理日期** - 驗證軟體權利文件記錄時的日期 (時間戳記)
  - **組織** - 軟體權利文件記錄中使用者的組織
  - **管理員** - 已掃描之使用者的管理員
  - **資源** - 使用者在其上具有帳號的資源，已擷取至該使用者軟體權利文件中
  - **違規** - 檢閱期間所偵測到的違規數目

按一下該報告中的名稱可開啓使用者軟體權利文件記錄。圖 15-6 顯示使用者軟體權利文件記錄檢視中提供的資訊範例。

圖 15-6 使用者軟體權利文件記錄



- **[存取檢閱摘要報告]** - 此報告也已在第 511 頁的「管理存取檢閱進度」中討論並在圖 15-5 中說明，其中會顯示以下有關您爲報告選取之存取掃描的摘要資訊：
  - **檢閱名稱** - 存取掃描的名稱
  - **日期** - 檢閱於何時啓動的時間戳記
  - **使用者計數** - 該檢閱中已掃描的使用者數目
  - **軟體權利文件計數** - 所產生的軟體權利文件記錄數目
  - **已核准** - 已核准的軟體權利文件記錄數目
  - **已拒絕** - 已拒絕的軟體權利文件記錄數目
  - **擱置** - 仍處於擱置狀態的軟體權利文件記錄數目
  - **已取消** - 已取消的軟體權利文件記錄數目

這些報告均可從 [執行報告] 頁面，以可移植文件格式 (PDF) 或逗號分隔值 (CSV) 格式下載。

存取檢閱修正

規範遵循違規修正與緩解以及存取檢閱修正，均可從 [工作項目] 標籤的 [修正] 區域中加以管理。但這兩種修正類型有其不同之處。本節說明存取檢閱修正的獨特運作方式，以及它與第 489 頁的「修正與緩解規範遵循違規」中說明的修正作業與資訊有何不同。

關於存取檢閱修正

當驗證者請求對使用者軟體權利文件進行修正時，標準修正工作流程會建立修正請求，而此請求必須由修正者 (可計算及回應修正請求的指定使用者) 加以處理。

只能修正問題，而無法緩解問題。必須在問題解決後，驗證才能繼續。

從存取檢閱產生修正後，[存取檢閱] 面板會追蹤所有涉及該檢閱的驗證者與修正者。

修正者上報

存取檢閱修正請求不會上報至除初始修正者以外的修正者。

修正工作流程程序

存取檢閱修正的邏輯定義於標準修正工作流程中。

當驗證者請求對使用者軟體權利文件進行修正時，標準修正工作流程會執行下列作業：

- 產生修正請求 (類型爲 accessReviewRemediation)，其中包含需修正之使用者軟體權利文件的相關資訊。
- 傳送電子郵件給請求的修正者。

接著，新的修正者可選擇編輯使用者 (使用 Identity Manager 或獨立編輯)，然後在工作項目達到要求後將其標記爲已修正。屆時會重新掃描並再次計算使用者的軟體權利文件。

修正回應

依預設，會爲存取檢閱修正者提供三個回應選項：

- **修正** - 修正者指出已採取行動以修復問題。

  接著會重新掃描並再次計算使用者的軟體權利文件。若使用者軟體權利文件再次標記爲需要驗證，則原始驗證者將再次於 [驗證] 工作項目清單中看見該使用者軟體權利文件。

  修正請求動作的詳細資訊會出現在個別使用者軟體權利文件的 [歷程記錄] 區域中。

- **轉寄** - 修正者將解決修正請求的責任重新指定給另一位人員。

  轉寄動作的詳細資訊會出現在個別使用者軟體權利文件的 [歷程記錄] 區域中。

- **編輯使用者** - 修正者選擇直接編輯使用者以修正問題。

  只有在修正者具有修改使用者的權限時，此按鈕才會顯示。對使用者進行變更後按一下 **[儲存]**，修正者即會進入 [修正確認] 頁面，以提供可說明對使用者所做變更的註釋。

  接著會重新掃描並再次計算使用者的軟體權利文件。若使用者軟體權利文件再次標記爲需要驗證，則原始驗證者將再次於 [驗證] 工作項目清單中看見該使用者軟體權利文件。

  編輯的詳細資訊會作爲修正請求動作，出現在個別使用者軟體權利文件的 [歷程記錄] 區域中。

使用修正頁面

針對所有屬於存取檢閱修正工作項目的修正工作項目，[類型] 欄會顯示爲 UE (使用者軟體權利文件)。

不支援的存取檢閱修正動作

存取檢閱修正不支援優先權排定與緩解功能。

第 16 章

資料匯出程式

資料匯出程式功能可讓您將有關使用者、角色及其他物件類型的資訊寫入外部資料倉儲。

請閱讀本章以獲得協助您設定與維護資料匯出程式的資訊和程序。如需有關規劃與實作資料匯出程式的完整詳細資訊，請參閱「Identity Manager Technical Deployment Overview」。

本章包含以下主題：

何謂資料匯出程式？

Identity Manager 包含及處理與分散式系統及應用程式之間管理身份識別相關的資料。爲了改善整體效能，Identity Manager 不會保留其在一般佈建與其他日常作業期間產生的所有資料。例如，Identity Manager 預設不會保留中間狀態工作流程作業與作業實例。如果需要擷取 Identity Manager 通常捨棄的所有或部分資料，請啓用資料匯出程式功能。

啓用資料匯出程式之後，Identity Manager 會將偵測到對指定物件 (資料類型) 所做的每項變更，在儲存庫表格中儲存爲一筆記錄。在作業將其寫入外部資料倉儲之前，這些事件會排入佇列 (您可以配置匯出每種資料類型的頻率)。匯出的資料可進一步處理，或在使用商業轉換、報告及分析工具查詢與轉換時做爲依據。

將資料匯出至資料倉儲對 Identity Manager 伺服器的效能會造成不良影響，除非有匯出資料的業務需求，否則不應啓用此功能。

Identity Manager 也可讓您建立及執行鑑識查詢。鑑識查詢會搜尋資料倉儲，並識別符合您指定條件的 [使用者] 或 [角色] 物件。詳細資訊請參閱第 536 頁的「配置鑑識查詢」。

規劃實作資料匯出程式

由於預設會停用資料匯出程式，因此必須加以配置才能運作。資料匯出程式的配置需要決定下列事項，配置才可開始。

- 要匯出的資料類型爲何？
- 擷取各種資料類型的資料所使用的技術爲何？
- 各種類型的資料匯出頻率爲何？
- 各種類型的匯出模式內容爲何？
- 是否需要自訂倉儲介面程式碼 (WIC) 工廠類別？

啓用資料匯出程式之後，預設配置會匯出所有資料類型的所有屬性。如此會耗用永遠不會用到的倉儲儲存，而可能導致 Identity Manager 與倉儲不必要的處理負擔。對於稍後有機會用到的資料，資料倉儲會以保守謹慎的態度擷取資料。您不需要匯出所有可匯出的資料。您可以配置要匯出的資料類型，並禁止匯出某些事件。

一旦決定上述事項，請使用下列步驟實作資料匯出程式：

1. (選擇性) 爲選取的類型自訂匯出模式，然後重新產生倉儲 DDL。詳細資訊請參閱「Identity Manager Technical Deployment Overview」。
2. 在倉儲 RDBMS 上建立使用者帳號，然後在此系統上載入倉儲 DDL。詳細資訊請參閱「Identity Manager Technical Deployment Overview」。
3. 如第 526 頁的「配置資料匯出程式」所述配置資料匯出程式。
4. 測試資料匯出程式以確保其配置正確。詳細資訊請參閱第 535 頁的「測試資料匯出程式」。
5. (選擇性) 建立可搜尋寫入至資料倉儲之資料的鑑識查詢。詳細資訊請參閱第 536 頁的「配置鑑識查詢」。
6. 使用 JMX 並監視記錄檔以維護資料匯出程式。詳細資訊請參閱第 541 頁的「維護資料匯出程式」。

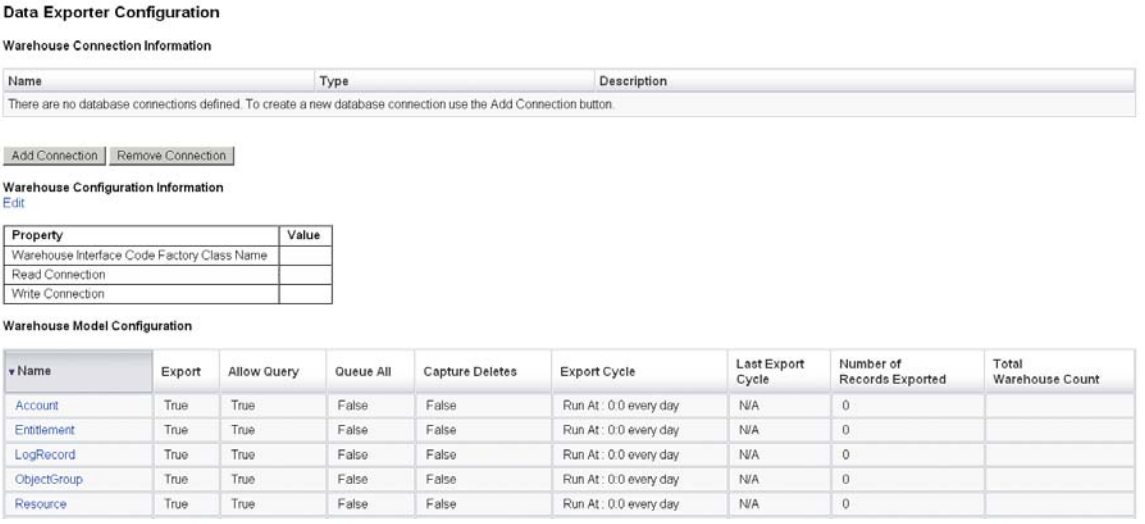
配置資料匯出程式

[資料匯出程式配置] 頁面可讓您定義要保留的資料類型、指定要匯出的屬性，以及排程何時匯出資料。每種資料類型皆可獨立配置。

若要配置資料匯出程式，請執行以下步驟：

1. 在管理員介面的主功能表中，按一下 **[配置]**。然後按一下 **[倉儲]** 輔助標籤。[資料匯出程式配置] 頁面隨即開啓。

圖 16-1 資料匯出程式配置



2. 若要定義讀取與寫入連線，請按一下 **[增加連線]** 按鈕。[編輯資料庫連線] 頁面會隨即開啓。

   完成此頁面上的所有欄位，然後按一下 **[儲存]** 以返回 [資料匯出程式配置] 頁面。詳細資訊請參閱第 528 頁的 「定義讀取與寫入連線」。

3. 若要指定 WIC 類別及資料庫連線，請在 [倉儲配置資訊] 區段中，按一下 **[編輯]** 連結。[資料匯出程式倉儲配置] 頁面隨即開啓。

   完成此頁面上的所有欄位，然後按一下 **[儲存]** 以返回 [資料匯出程式配置] 頁面。詳細資訊請參閱第 530 頁的 「定義倉儲配置資訊」。

4. 在 [倉儲模型配置] 表格中，按一下資料類型連結。[資料匯出程式類型配置] 頁面隨即開啓。

   完成此頁面上的 **[匯出]**、**[屬性]** 與 **[排程]** 標籤，然後按一下 **[儲存]** 以返回 [資料匯出程式配置] 頁面。詳細資訊請參閱第 531 頁的「配置倉儲模型」。

   每個資料類型均重複此步驟。

5. 若要配置匯出作業常駐程式，請在 [倉儲作業配置] 區段中，按一下 **[編輯]** 連結。[資料匯出程式倉儲配置] 頁面隨即開啓。

   完成此頁面上的所有欄位，然後按一下 **[儲存]** 以返回 [資料匯出程式配置] 頁面。詳細資訊請參閱第 533 頁的「配置倉儲作業」。

備註 一旦完成這些步驟，匯出作業便可完整運作。啓用匯出之後，資料記錄即會開始排入佇列等候匯出。若未啓用匯出作業，佇列表格會填滿，接著佇列會暫停。匯出較小的批次 (較常匯出) 一般而言比匯出較大的批次還要有效率，但是匯出還受限於倉儲本身的寫入可用性，這就會受到其他因素限制。

6. 您也可以設定最大佇列大小。詳細資訊請參閱第 534 頁的「修改配置物件」。

定義讀取與寫入連線

Identity Manager 在匯入週期期間使用寫入連線。讀取連線則用於表示目前在倉儲中的記錄數目 (在倉儲配置期間)，以及處理鑑識查詢介面。

倉儲連線可定義爲應用程式伺服器的資料來源、JDBC 連線或資料庫資源的參照。若定義了 JDBC 連線或資料庫資源，則資料匯出在寫入作業期間會大量使用少數連線，然後再關閉所有連線。資料匯出程式僅在倉儲配置期間及執行鑑識查詢期間使用讀取連線，作業完成後即會關閉這些連線。

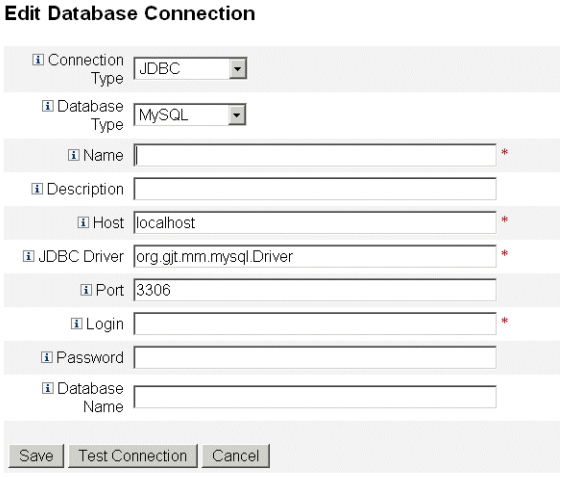
匯出程式針對寫入連線與讀取連線使用相同的模式，且兩者可使用相同的連線資訊。但是，若您有獨立的連線，部署會寫入一組倉儲分段備份表格，將該表轉換爲實際倉儲，然後再將倉儲表格轉換爲供 Identity Manager 讀取的資料超市。

您可以編輯 [資料匯出程式配置] 表單，以避免 Identity Manager 讀取倉儲。此表單包含 `includeWarehouseCount` 特性，可使 Identity Manager 查詢倉儲並顯示每種資料類型的記錄筆數。若要停用此功能，請複製 [資料匯出程式配置] 表單，將 `includeWarehouseCount` 特性的值變更爲 `true`，再匯入您的自訂表單。

若要定義讀取與寫入連線，請執行以下步驟：

1. 從 [資料匯出程式配置] 頁面按一下 **[增加連線]** 按鈕。

圖 16-2 資料匯出程式配置



2. 指定 Identity Manager 如何透過選取 **[連線類型]** 下拉式功能表中的選項，以建立資料倉儲的讀取或寫入連線。

   - **JDBC** - 使用 Java 資料庫連結 (JDBC) 應用程式設計介面連線至資料庫。連線池儲存是由倉儲介面程式碼所提供。
   - **資源** - 使用在資源中定義的連線資訊。連線池儲存是由倉儲介面程式碼所提供。
   - **資料來源** - 使用基礎應用程式伺服器於連線管理與連線池。此連線類型是向應用程式伺服器請求連線。

   頁面上所顯示的欄位，會因您從 **[連線類型]** 下拉式功能表中選取的選項而有所不同。請參閱線上說明，以取得有關配置資料庫連線的詳細資訊。

3. 按一下 **[儲存]** 以儲存配置變更並返回 [資料匯出程式配置] 頁面。

若要使用獨立的讀取與寫入連線，請重複此程序。

定義倉儲配置資訊

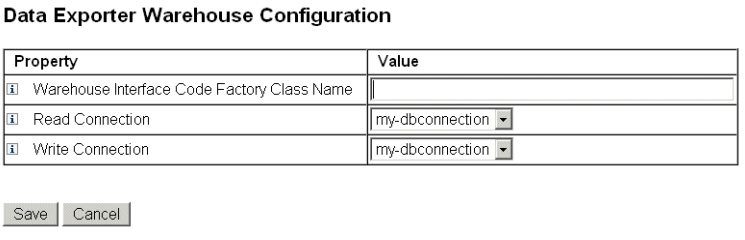
若要配置倉儲，您必須選取讀取連線、寫入連線，並指定倉儲介面程式碼工廠類別。WIC 工廠類別提供 Identity Manager 與倉儲之間的介面。Identity Manager 提供預設的程式碼實作，但您也可以建立自己的程式碼實作。如需有關建立自訂工廠類別的資訊，請參閱「Identity Manager Technical Deployment Overview」。

`$WSHOME/exporter` 目錄中必須有內含工廠類別的 JAR 檔案和所有支援的 JAR 檔案，且該目錄需位在執行匯出作業的 Identity Manager 伺服器上，以及所有配置資料匯出程式的伺服器上。任何指定時間內僅一部 Identity Manager 伺服器可匯出資料。

若要定義倉儲配置資訊，請執行以下步驟：

1. 從 [資料匯出程式配置] 頁面，按一下 [倉儲配置資訊] 區段中的 **[編輯]** 連結。

圖 16-3 資料匯出程式配置



2. 在 **[倉儲介面程式碼工廠類別名稱]** 欄位中指定一個值。若您的整合者尚未建立自訂類別，請輸入值 `com.sun.idm.warehouse.base.Factory`。
3. 從 **[讀取連線]** 與 **[寫入連線]** 下拉式功能表中選取一個選項，以指定連線。
4. 按一下 **[儲存]** 以儲存配置變更並返回 [資料匯出程式配置] 頁面。

配置倉儲模型

可匯出的資料類型各有一組選項，用於控制是否要匯出類型，以及類型的匯出方式與時機。由於匯出資料會增加 Identity Manager 伺服器的負載，因此僅有業務需求的資料類型才應啓用匯出。

下表描述可匯出的所有資料類型。

表 16-1　支援的資料類型

資料類型	說明
Account	包含 「使用者」與 「資源帳號」之間連結的記錄
Entitlement	包含特定使用者之驗證作業清單的記錄
LogRecord	包含單筆稽核記錄的記錄
ObjectGroup	模型化為組織的安全性容器
Resource	佈建帳號所在的系統/應用程式
ResourceAccount	包含於特定資源之帳號的屬性集
Role	存取的邏輯容器
Rule	Identity Manager 可執行的一組邏輯
TaskInstance	表示程序正在執行或已完成的記錄
User	沒有帳號或有多個帳號的邏輯使用者
WorkflowActivity	Identity Manager 工作流程的單一作業
WorkItem	Identity Manager 工作流程的手動操作

若要配置倉儲模型，請執行以下步驟：

1. 從 [資料匯出程式配置] 頁面按一下資料類型連結。
2. 在 [匯出] 標籤中，指定是否要匯出資料類型。若不要匯出此資料類型，請取消選取 **[匯出]** 核取方塊，並按一下 **[儲存]**。否則，請視需要選取此 [匯出] 標籤中的剩餘選項。
   - **允許查詢** - 控制是否可查詢模型。
   - **全部納入佇列** - 擷取對此類型的物件所做的全部變更。核取此選項可能會大量增加匯出程式的處理負擔，故請謹慎使用此選項。
   - **擷取刪除** - 記錄所有已刪除的此類型物件。核取此選項可能會大量增加匯出程式的處理負擔，故請謹慎使用此選項。
3. [屬性] 標籤可讓您選取要指定做爲鑑識查詢一部分的屬性，以及希望顯示於查詢結果的屬性。您無法刪除管理員介面的預設屬性。如需有關變更預設屬性的資訊，請參閱「Identity Manager Technical Deployment Overview」。

   新的屬性名稱具有下列特性：
   - attrName - 此屬性爲頂層且純量屬性。
   - attrName[] - 此屬性爲列出值的頂層屬性，且清單中的元素爲純量。
   - attrName['key'] - 此屬性包含對映值，需要具有指定鍵值的對映值。
   - attrName[].name2 - 此屬性爲列出值的頂層屬性，其中清單中的元素爲結構。name2 爲所存取結構中的屬性。
4. 在 [排程] 標籤中，指定資料類型相關聯之資訊的匯出頻率。週期是從伺服器上的午夜起算。每隔 20 分鐘的週期會整點執行，接著是整點後的 20 分鐘及 40 分鐘。若嘗試匯出的時間較排程的週期長，則會略過下一個週期。例如，若將週期定義爲 20 分鐘並自午夜開始，而完成匯出需要 25 分鐘，則下一個匯出會在 12:40 開始。原始排程的 12:20 不會發生匯出。

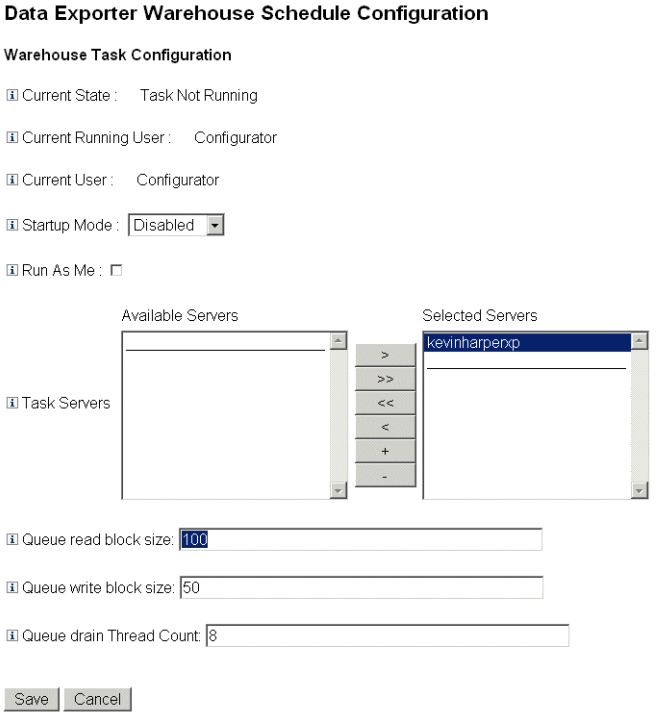
配置倉儲作業

您不需要在專屬伺服器上執行匯出作業，但若要匯出大量資料，可考慮如此執行。匯出作業在從 Identity Manager 傳送資料至倉儲時的效率極高，而且在匯出作業期間會儘量消耗 CPU。若不使用專屬伺服器，則應限制伺服器處理互動流量，因爲大量匯出時，回應時間會明顯地拉長。

若要配置倉儲配置資訊，請執行以下步驟：

1. 從 [資料匯出程式配置] 頁面，按一下 [倉儲作業配置] 區段中的 **[編輯]** 連結。

圖 16-4 資料倉儲排程配置



2. 從 **[啓動模式]** 下拉式功能表中選取選項，以決定在 Identity Manager 啓動時，是否要自動啓動倉儲作業。選取 [已停用] 表示必須手動啓動作業。
3. 核取 **[以本人身份執行]** 核取方塊可使用您的管理帳號執行匯出程式作業。

4. 選取可執行作業的伺服器。您可以指定多部伺服器，但一次只能執行一項倉儲作業。若執行作業的伺服器停止，排程程式會從清單 (如果有) 上的其他伺服器上自動重新啓動作業。
5. 在寫入 **[佇列讀取區塊大小]** 欄位前，指定從佇列讀入記憶體緩衝區的記錄筆數。此欄位的預設值適用於大部分的匯出作業。若 Identity Manager 儲存庫伺服器較倉儲伺服器慢，請增加此值。
6. 在 **[佇列寫入區塊大小]** 欄位中，指定單一作業事件中，寫入倉儲的記錄筆數。
7. 在 **[佇列清空執行緒計數]** 欄位中，指定用以讀取已排入佇列之記錄的 Identity Manager 執行緒數目。若佇列表格存有大量不同類型的記錄，請增加此數值。若佇列表格的資料類型數量很少，請減少此數值。
8. 按一下 **[儲存]** 以儲存配置變更並返回 [資料匯出程式配置] 頁面。

修改配置物件

配置並執行資料匯出程式之後，即會從內部佇列表格中擷取所有配置要排入佇列的資料類型。依預設，此表格沒有上限，但可透過編輯 〔資料倉儲配置〕 配置物件來配置上限。此物件具有名爲 `warehouseConfig` 的巢式物件。將下列內容增加至 `warehouseConfig` 物件：

```
<Attribute name='maxQueueSize' value='YourValue'/>
```

`maxQueueSize` 的值可爲小於 2^{31} 的任何正整數。達到上限後，資料匯出程式將停用佇列。在清空佇列之前，無法匯出產生的資料。

一般的 Identity Manager 作業每小時可產生數千筆已變更的記錄，因此佇列表格的大小增加極快。由於佇列表格位於 Identity Manager 儲存庫中，此增加會消耗 RDBMS 的表格空間，故而可能會用盡表格空間。若表格空間有限，則可能必須設定佇列上限。

使用 Data Queue JMX MBean 以監視佇列表格的大小。詳細資訊請參閱第 541 頁的「監視資料匯出程式」。

測試資料匯出程式

正確配置資料匯出程式之後，將會以背景程序運作，並依配置的間隔將資料傳送至倉儲。若需執行匯出程式，請使用 [資料倉儲匯出程式啓動程式] 作業。

若要啓動資料倉儲匯出程式啓動程式，請執行以下步驟：

1. 停用倉儲作業。詳細資訊請參閱第 533 頁的「配置倉儲作業」。
2. 按一下主功能表中的 **[伺服器作業]**。然後按一下 **[執行作業]** 輔助標籤。[可用的作業] 頁面會隨即開啓。
3. 按一下 **[資料倉儲匯出程式啓動程式]** 連結。[啓動作業] 頁面隨即開啓。
4. 選取 **[除錯選項]** 核取方塊以顯示其他選項。
5. 選取 **[忽略初始的 LastMod]** 核取方塊，會讓匯出程式忽略「上次輪詢」的時間戳記，而匯出程式會使用此時間戳記判定已從 Identity Manager 儲存庫中匯出的記錄。選取此選項時，將匯出 Identity Manager 儲存庫中所選類型的全部記錄。
6. 選擇要從 **[匯出一次]** 清單中匯出的資料類型。若未在 [匯出一次] 清單中選擇任何類型，匯出作業會以常駐程式來執行，並根據之前定義的排程進行匯出。若選取一或多種資料類型，Identity Manager 會立即匯出這些類型，然後結束匯出作業。
7. 視需要設定頁面上其他欄位的值。
8. 按一下 **[啓動]** 開始作業。

配置鑑識查詢

鑑識查詢可讓 Identity Manager 讀取資料倉儲中已儲存的資料，並且可根據使用者、角色或相關資料類型目前或之前的值，識別使用者或角色。鑑識查詢類似於「尋找使用者」或「尋找角色」報告，但不同之處在於符合條件可根據之前的資料來計算，而除了正在查詢的使用者或角色之外，還可搜尋資料類型不同的屬性。

鑑識查詢的目的在對使用 Identity Manager 的結果採取行動。鑑識查詢不是一般用途的報告工具。

鑑識查詢可詢問類似下列的問題：

- 在時間 A 至 B 之間，曾經存取系統 X 者爲何？該存取之核准者爲何？
- 在過去 48 小時內，已處理之佈建請求數量爲何，且每項請求所佔用時間多長？

鑑識查詢的結果無法儲存。若要執行一般倉儲資料報告，請使用商業報告工具。

建立查詢

鑑識查詢可搜尋「使用者」或「角色」物件。查詢可以很複雜，讓作者得以針對相關資料類型選取一個或多個屬性條件。使用者鑑識查詢可搜尋下列資料類型的屬性：使用者、帳號、資源帳號、角色、軟體權利文件和工作項目。角色鑑識查詢可搜尋下列資料類型的屬性：角色、使用者和工作項目。

在單一資料類型中，所有屬性條件邏輯上皆使用 AND，因此必須符合所有條件才會出現相符項目。依預設，相符項目與所有資料類型之關係爲 AND，但若選取 **[使用 OR]** 核取方塊，則相符項目與所有資料類型之關係邏輯上使用 OR。

倉儲可在單一「使用者」或「角色」物件中包含多筆記錄，且對該同一使用者或角色的單一查詢可傳回多個相符項目。爲協助區分這些相符項目，可限定每種資料類型的日期範圍，如此一來，僅指定日期範圍內的記錄才會視爲相符項目。也可限定每種相關資料類型的日期範圍，因此可以發出下列形式的查詢：

```
find all Users with Resource Account on ERP1 between May and July 2005 who
were attested by Fred Jones between June and August 2005 (尋找 Fred Jones 在
2005 年 6 月到 8 月間驗證，且從 2005 年 5 月到 7 月間在 ERP1 上具有資源帳號的所有使
用者)
```

日期範圍是從午夜至午夜爲基礎。例如，2007 年 5 月 3 日到 2007 年 5 月 5 日的範圍爲 48 小時。不會包括自 2007 年 5 月 5 日起的任何記錄。

查詢定義中必須指定每個屬性條件的運算元 (要加以比較的值)。此模式限制某些屬性必須有幾組可能值，但其他屬性則沒有限制。例如，大部分日期欄位的輸入必須使用 YYYY-MM-DD HH:mm:ss 格式。

備註 由於倉儲中的資料量可能很大，且查詢很複雜，因此從查詢到產生結果可能需要很長的時間。若您在鑑識查詢執行期間離開查詢頁面，將無法看到查詢的結果。

若要建立鑑識查詢，請執行以下步驟：

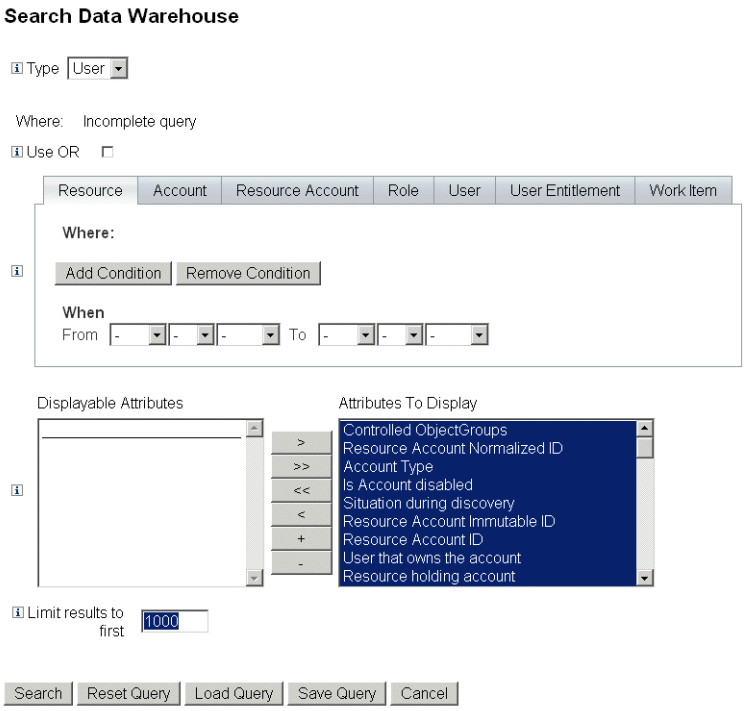
1. 在管理員介面的主功能表中，按一下 **[規範遵循]**。

   [稽核策略] 頁面 ([管理策略] 標籤) 隨即開啓。

2. 按一下 **[鑑識查詢]** 輔助標籤。

   [搜尋資料倉儲] 頁面隨即開啓。

圖 16-5　　搜尋資料倉儲



3. 從 **[類型]** 下拉式功能表中，選取是否搜尋使用者或角色記錄。
4. 選取 **[使用 OR]** 核取方塊，使 Identity Manager 對查詢的每種資料類型結果執行邏輯 OR。依預設，系統會對結果執行邏輯 AND。
5. 選取將在鑑識查詢中出現之代表資料類型的標籤。
   a. 按一下 **[增加條件]**。一組下拉式功能表隨即顯示。
   b. 從左側下拉式功能表中選取運算元 (要檢查的條件)，並在右側下拉式功能表中選取比較類型。然後輸入要搜尋的字串或整數。可能的運算元清單會定義於外部模式中。請參閱線上說明，以取得每個運算元的描述。
   c. 您也可以選取日期範圍，以縮小查詢範圍。

   視需要將更多條件增加至目前選取的資料類型。針對鑑識查詢定義中的所有資料類型重複此步驟。
6. 在可用的屬性中，挑選您想在鑑識查詢結果中顯示的屬性。
7. 指定 **[只返回前]** 欄位中的值。使用多個資料類型的條件時，該限制會將套用至每個類型的子查詢，而最後的結果爲所有子查詢的交集。因此，最後結果可能會因爲對子查詢的限制之故，而排除部分的記錄。
8. 按一下 **[搜尋]** 立即執行鑑識查詢，或按一下 **[儲存查詢]** 以重複使用查詢。如需有關重複使用鑑識查詢的資訊，請參閱第 540 頁的「儲存鑑識查詢」。

儲存鑑識查詢

配置查詢之後 (也可選擇執行查詢以確保查詢後產生所需的結果)，您可以儲存查詢以供稍後執行。

若要儲存鑑識查詢，請執行以下步驟：

1. 從 [搜尋資料倉儲] 頁面按一下 **[儲存查詢]**。[儲存鑑識查詢] 頁面隨即開啓。
2. 指定查詢的名稱與描述。
3. 選取 **[儲存條件值]** 核取方塊可儲存您在 [搜尋資料倉儲] 頁面中輸入的條件值 (字串與整數)。若未選取此核取方塊，則會以已儲存的鑑識查詢做爲範本，且必須在每次執行查詢時輸入值。
4. 任何人皆可執行已儲存的查詢，但預設只有查詢作者可修改查詢。若要允許其他使用者修改您的查詢，請選取 **[允許其他人變更此查詢]** 核取方塊。
5. 由於查詢傳回「使用者」或「角色」物件，因此您可以選擇要顯示在結果中的物件屬性。若您要顯示的屬性不在 **[要顯示的屬性]** 清單中，則可移至 [資料匯出程式配置] 頁面，並將可顯示的屬性新增至「使用者」或「角色」類型。

載入查詢

您可以載入任何使用者儲存的查詢，但僅可變更自己建立的查詢，或其他人標記爲任何人皆可修改的查詢。

若要載入鑑識查詢，請執行以下步驟：

1. 從 [搜尋資料倉儲] 頁面按一下 **[載入查詢]**。[載入鑑識查詢] 頁面隨即開啓。若查詢已儲存爲範本，[查詢摘要] 欄會顯示 **[查詢不完整]**。
2. 選取查詢左側的核取方塊，然後按一下 **[載入查詢]**。

維護資料匯出程式

本節說明您可以追蹤資料匯出程式狀態的方式：

- 監視資料匯出程式
- 監視記錄

監視資料匯出程式

配置並執行匯出程式之後，可選擇監視匯出程式以確保其持續運作。匯出程式有數個 JMX Bean，可用於決定匯出程式的運作方式。JMX Bean 包含下列統計資料：匯出程式的平均讀取/寫入速率、內部記憶體佇列的目前/最大大小，以及永久性佇列的大小。匯出程式在匯出期間還會產生稽核記錄，每種資類類型的每個週期各一個記錄。稽核記錄包含已匯出類型的記錄筆數，以及匯出所需的時間。

資料匯出程式提供下列 JMX 管理 Bean，可用於監視匯出程式。

表 16-2 JMX 管理 Bean

Bean 名稱	說明
DataExporter	包含目前已排入佇列的匯出數目，以及佇列的上限。
DataQueue	包含目前已快取的已排入佇列匯出作業數目，以及快取的資料取得率。
ExporterTask	包含匯出的讀取數 (從 Identity Manager)、寫入數 (至倉儲)、讀取與寫入的速率 (記錄筆數/秒)，以及錯誤數。

資料匯出程式可配置爲在一般的 Identity Manager 作業期間，將匯出記錄排入佇列至佇列表格中。由於佇列可能需要擴充到能容納大量記錄，且需要在伺服器重新啓動之後仍能保留，因此會以 Identity Manager 儲存庫的表格支援佇列。寫入至儲存庫通常會使一般的 Identity Manager 作業速度變慢，因此在記錄可在儲存庫中保留之前，佇列會使用少量的記憶體快取來作爲記錄緩衝區。

DataQueue MBean 屬性可設定爲顯示佇列在記憶體中的記錄上限 (在單一 Identity Manager 伺服器上)。在平衡的系統上，記憶體快取的記錄筆數應很小且會很快歸零。若您觀察到此數目變大 (千位數) 或在幾秒內未歸零，則應調查儲存庫的寫入效能。

ExportTask MBean 包含兩個錯誤數，其中一個是讀取的錯誤數，另一個是寫入的錯誤數。這些計數應爲零，但有幾個可能發生錯誤的原因，特別是在寫入期間。最常見的寫入錯誤是由於匯出的資料不符合倉儲表格欄所致，通常是字串溢位。某些匯出的字串資料沒有限制，但匯出表格欄必須有上限。

監視記錄

Identity Manager 有兩個沒有增長限制的物件集：稽核記錄和系統記錄檔。資料匯出程式可藉此解決與這些與記錄檔表格相關的維護問題。

稽核記錄

Identity Manager 將不可變的稽核記錄寫入稽核記錄，以做爲其所執行作業的歷程稽核軌跡。Identity Manager 在特定報告中使用這些記錄，並可能在管理員介面中顯示記錄的資料。但是，由於稽核記錄會無限制地並以適中的速率增長，因此部署人員必須判斷何時截斷稽核記錄。在資料匯出程式出現之前，若要保留截斷前的記錄，必須強制從儲存庫傾印表格。若啓用資料匯出程式並將其配置成匯出記錄檔記錄，則會在倉儲中保留舊記錄，且 Identity Manager 可視需要截斷稽核表格。

系統記錄檔

系統記錄檔和稽核記錄一樣，皆具有不可變的特性，但一般而言系統記錄檔的產生較不頻繁。資料匯出程式無法匯出系統記錄檔。若要截斷系統記錄檔並保留舊記錄，您必須在儲存庫中傾印表格。

第 17 章

服務提供者管理

本章提供管理 Sun Identity Manager 中服務提供者功能所需瞭解的資訊。若要使用此資訊，瞭解簡易目錄存取協定 (LDAP) 目錄和聯合管理會很有幫助。如需有關服務提供者實作的更深入說明，請參閱「Identity Manager Service Provider Deployment」。

本章包含以下主題：

服務提供者功能簡介

在服務提供者環境中，您需要能夠管理所有一般使用者 (即企業外部網路使用者以及企業內部網路使用者) 的使用者佈建。Identity Manager 服務提供者功能可讓公司管理員將身份識別帳號，分類爲兩種不同的類型：Identity Manager 使用者和服務提供者使用者。Identity Manager 中的服務提供者使用者是已配置爲 [服務提供者使用者] 類型的使用者帳號。

Identity Manager 使用者佈建和稽核功能透過提供以下功能延伸至服務提供者實作：

增強的一般使用者頁面

提供了增強的一般使用者頁面，您可以自訂這些頁面以進行服務提供者實作。

密碼與帳號 ID 策略

您可以定義服務提供者使用者以及資源帳號的帳號 ID 和密碼策略，如其他 Identity Manager 使用者一樣。

可使用**服務提供者系統帳號策略** (已增加至主 [策略] 表格)，爲服務提供者使用者啓動策略檢查代碼。

Identity Manager 和服務提供者同步化

可以將 Identity Manager 和服務提供者帳號的同步化配置爲在任何 Identity Manager 伺服器上執行或僅限於在選取的伺服器上執行。

可以輕鬆地透過 [資源] 頁面上的 [資源動作] 選項停止和啓動服務提供者同步化，如 Identity Manager 同步化一樣。請參閱第 587 頁的「啓動和停止同步化」。

Identity Manager 使用者同步化的輸入表單與服務提供者使用者同步化的輸入表單不同。請參閱第 582 頁的「一般使用者介面」。

Access Manager 整合

您可以使用 Sun Access Manager 7 2005Q4，在服務提供者一般使用者頁面上進行認證。如果配置了與 Access Manager 的整合，則 Access Manager 可確保僅經過認證的使用者才可以存取一般使用者頁面。

服務提供者需要使用者名稱，以用於稽核。更新 `AMAgent.properties` 檔案，以便將使用者 ID 增加至 HTTP 標頭，例如：

```
com.sun.identity.agents.config.response.attribute.mapping[uid] =
HEADER_speuid
```

一般使用者頁面認證篩選器將 HTTP 標頭值置入代碼其餘部分期望其處於的 HTTP 階段作業中。

初始配置

若要配置服務提供者功能，請使用以下程序編輯目錄伺服器的 Identity Manager 配置物件：

- 編輯主配置
- 編輯使用者搜尋配置

備註 在繼續之前，請確保您已經：

- 定義 LDAP 資源。依預設，會匯入名稱爲「服務提供者一般使用者目錄」的資源範例。如果要將使用者資訊和配置資訊儲存在不同目錄中，您可以配置多個資源。
  - 此模式必須包含 XML 物件的對映。
  - 爲目錄資源配置的基底環境僅適用於儲存在該目錄中的使用者。
- 如果需要，請配置您的服務提供者帳號策略。

編輯主配置

若要編輯服務提供者實作的配置物件，請執行以下步驟：

1. 在管理員介面中，按一下功能表的 **[服務提供者]**。
2. 按一下 **[編輯主配置]**。

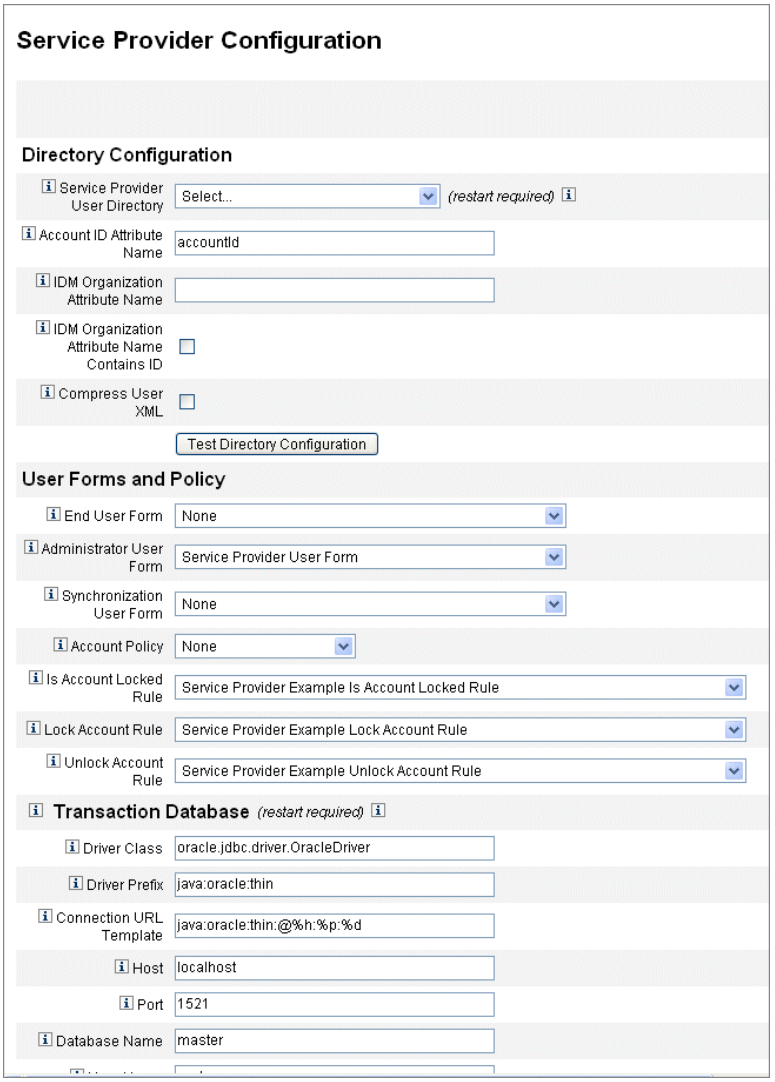
   [服務提供者配置] 頁面會隨即開啓。
3. 適當地完成 [服務提供者配置] 表單：
   - 目錄配置
   - 使用者表單策略
   - 作業事件資料庫
   - 追蹤的事件配置
   - 同步化帳號索引
   - 圖說文字配置

目錄配置

在 [目錄配置] 區段中，提供有關配置 LDAP 目錄的資訊並指定服務提供者使用者的 Identity Manager 屬性。

圖 17-1 顯示 [服務提供者配置] 頁面的此區域，以及下一節所討論的 [使用者表單和策略] 區域。

圖 17-1　　服務提供者配置 (目錄、使用者表單與策略)



若要完成目錄配置表單，請執行以下步驟：

1. 從清單中選取 **[服務提供者一般使用者目錄]**。

   選取儲存所有服務提供者使用者資料的 LDAP 目錄資源。

2. 輸入 **[帳號 ID 屬性名稱]**。

   此爲包含 LDAP 帳號之唯一短識別碼的 LDAP 帳號屬性名稱。該名稱被認爲是透過 API 進行認證和存取帳號的使用者名稱。該屬性名稱必須在模式對映中定義。

3. 指定 **[IDM 組織屬性名稱]。**

   此選項可指定 LDAP 帳號屬性的名稱，該 LDAP 帳號屬性包含 LDAP 帳號在 Identity Manager 中所屬組織的名稱或 ID。其用於 LDAP 帳號的託管。屬性名稱必須存在於 LDAP 資源模式對映中，並且是 Identity Manager 系統屬性名稱 (模式對映左側的名稱)。

備註 如果要透過組織授權啓用託管，請指定 [Identity Manager 組織屬性名稱]，並且如有需要，還應指定 [IDM 組織屬性名稱包含 ID]。

4. 如果您選擇選取 **[IDM 組織屬性名稱包含 ID]**，請啓用此選項。

   如果參照 LDAP 帳號所屬 Identity Manager 組織的 LDAP 資源屬性包含 Identity Manager 組織的 ID，而不包含組織名稱，請選取此選項。

5. 如果您選擇選取 **[壓縮使用者 XML]**，請啓用此選項。

   如果您選擇壓縮儲存在目錄中的使用者 XML，請選取此選項。

6. 按一下 **[測試目錄配置]** 以驗證配置項目。

備註 您可以依需要測試**目錄**、**作業事件**和**稽核配置**。若要完全測試所有這三項，請按一下所有三個測試配置按鈕。

使用者表單策略

在 [使用者表單和策略] 區域 (如上面的圖 17-1 所示) 中，指定要用於服務提供者使用者管理的表單與策略。

若要指定用於服務提供者使用者管理的表單和策略，請執行以下步驟：

1. 從清單中選取 **[一般使用者表單]**。

   此表單用於任何地方，[委託管理員] 頁面和同步化期間除外。如果選取 **[無]**，則不使用任何預設使用者表單。

2. 從清單中選取 **[管理員使用者表單]**。

   這是用於管理員環境中的預設使用者表單。其包含服務提供者帳號編輯頁面。如果選取 **[無]**，則不使用任何預設使用者表單。

備註 如果您不選擇管理員使用者表單，則管理員將無法從 Identity Manager 中建立或編輯服務提供者使用者。

3. 從清單中選取 **[同步使用者表單]**。

   若沒有針對資源執行服務提供者同步化指定表單，則會使用預設的 [同步使用者表單]。如果在資源同步策略上已指定輸入表單，則會改用該表單。資源通常需要不同的同步輸入表單。在此情況下，您應在每個資源上設定同步使用者表單，而非從清單中選取表單。

4. 從清單中選取 **[帳號策略]**。

   選項包括透過 [配置] > [策略] 定義的任何身份識別帳號策略。

5. 從清單中選取 **[帳號是否鎖定規則]**。

   選取要針對服務提供者使用者檢視執行的規則，該規則可確定帳號是否已鎖定。

6. 選取 **[鎖定帳號規則]**。

   選取要針對服務提供者使用者檢視執行的規則，該規則可在檢視中設定能鎖定帳號的屬性。

7. 選取 **[解除鎖定帳號規則]**。

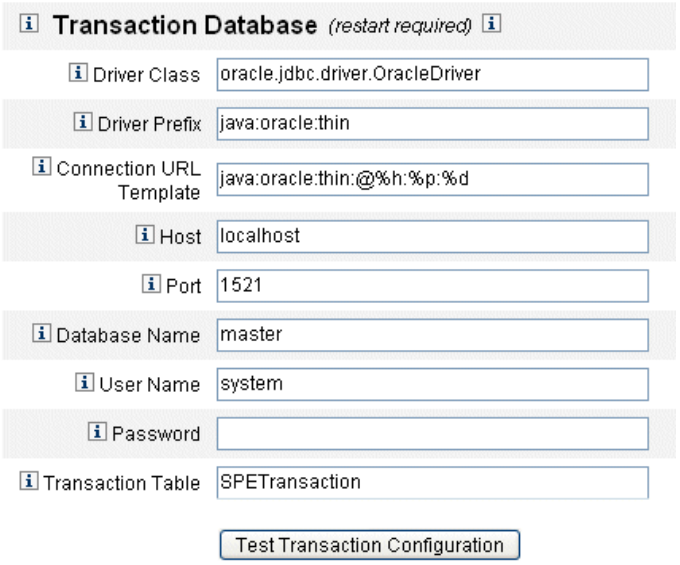
   選取要針對服務提供者使用者檢視執行的規則，該規則可在檢視中設定能解除鎖定帳號的屬性。

作業事件資料庫

使用 [服務提供者配置] 頁面的此區段 (如圖 17-2 所示)，可以配置作業事件資料庫。僅當使用 JDBC 作業事件永久存放區時才需要這些選項。變更其中的任何值均需要重新啓動伺服器以將其套用。

作業事件的資料庫表格必須根據 `create_spe_tables` DDL 程序檔 (位於 Identity Manager 安裝的 `sample` 目錄) 中所示的模式進行設定。您可能必須爲目標環境自訂適用的程序檔。

圖 17-2　服務提供者配置 (作業事件資料庫)



若要配置作業事件資料庫，請執行以下步驟：

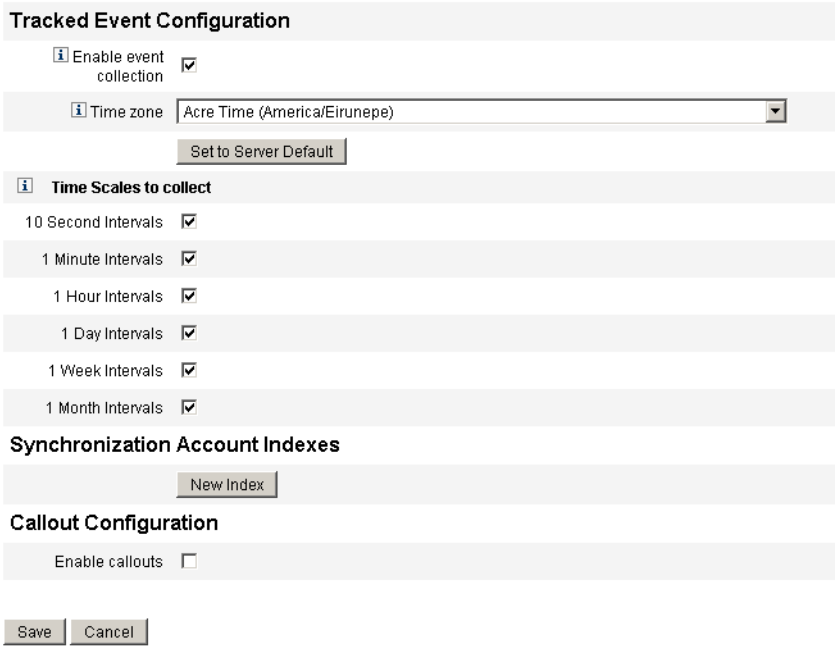
1. 輸入以下資料庫資訊：
   - **[驅動程式類別]** - 指定 JDBC 驅動程式類別名稱。
   - **[驅動程式前綴]** - 此欄位爲可選擇欄位。如果指定，則會在註冊新的驅動程式之前查詢 JDBC DriverManager。
   - **[連線 URL 範本]** - 此欄位爲可選擇欄位。如果指定，則會在註冊新的驅動程式之前查詢 JDBC DriverManager。
   - **[主機]** - 輸入正在執行資料庫的主機名稱。
   - **[連接埠]** - 輸入資料庫伺服器正在偵聽的連接埠號。
   - **[資料庫名稱]** - 輸入要使用的資料庫名稱。
   - **[使用者名稱]** - 輸入具有讀取、更新和刪除所選取資料庫中作業事件和稽核表中列之權限的資料庫使用者 ID。
   - **[密碼]** - 輸入資料庫使用者密碼。
   - **[作業事件表]** - 輸入要用於儲存擱置作業事件的所選取資料庫中的表格名稱。
2. 按一下 **[測試目錄配置]** 以驗證項目 (如果適用)。

繼續至 [服務提供者配置] 頁面的下一個區段，以配置追蹤的事件。

追蹤的事件配置

啓用事件收集後，您便可以即時追蹤統計資料，從而協助維護預期或商定層級的服務。依預設啓用事件收集，如圖 17-3 所示。清除 **[啓用事件收集]** 核取方塊可停用收集。

圖 17-3　服務提供者配置 ([追蹤的事件]、[帳號索引] 和 [圖說文字配置])



若要設定時區並指定服務提供者追蹤的事件之收集間隔，請執行以下步驟：

1. 從清單中選取 **[時區]**。

   選取記錄追蹤事件時要使用的時區，或選取 **[設定爲伺服器預設]** 以使用伺服器上設定的時區。

2. 選取 **[要收集的時間範圍]** 中的選項。

   按以下時間間隔總計收集結果：每 10 秒鐘、每分鐘、每小時、每天、每週和每月。停用您不希望按其進行收集的任何間隔。

同步化帳號索引

在服務提供者實作中同步化資源時，可能需要定義**帳號索引**，以正確地將資源所傳送的事件與服務提供者目錄中的使用者產生相互關聯。

依預設，資源事件需要包含符合目錄中 accountId 屬性的屬性 accountId 值。在某些資源中，不一定都會傳送 accountId。例如，ActiveDirectory 的刪除事件只包含 ActiveDirectory 產生的帳號 GUID。

不包含 accountId 屬性的資源必須包含以下任一屬性的值。

- **guid** - 此屬性通常包含系統產生的唯一識別碼。
- **identity** - 此屬性通常與除 LDAP 資源之外的所有資源之 accountId 相同 (在 LDAP 資源中，identity 包含物件的完整 DN)。

如果您需要使用 guid 或 identity 進行關聯，則必須爲這些屬性定義帳號索引。索引僅是一個或多個可用於儲存資源特定身份識別之目錄使用者屬性的選取。身份識別儲存在目錄中後，便可將其用於搜尋篩選，以關聯同步化事件。

若要定義帳號索引，請首先確定要用於同步化的資源以及其中哪些資源需要索引。然後編輯服務提供者目錄的資源定義，並在每個 Active Sync 資源之 GUID 或身份識別屬性的模式對映中增加屬性。例如，如果您從 ActiveDirectory 進行同步化，則可能要定義對映至未使用的目錄屬性 (如管理員) 之名爲 AD-GUID 的屬性。

定義服務提供者資源中的所有索引屬性之後，請執行以下步驟：

1. 在配置頁面的 [同步化帳號索引] 區域中，按一下 **[新索引]** 按鈕。

   表單擴展爲包含資源選取欄位，之後是兩個屬性選取欄位。在選取資源之前，屬性選取欄位保持空白

2. 從清單中選取 **[資源]**。

   現在，屬性欄位包含在所選資源之模式對映中定義的值。

3. 爲 **[GUID 屬性]** 或 **[完整的 Indentity 屬性]** 選取適當的索引屬性。

   通常不必同時設定二者。如果同時設定二者，則軟體會首先嘗試使用 GUID 進行關聯，然後使用完整 identity。

4. 您可以再次按一下 **[新索引]**，以定義其他資源的索引屬性。

5. 若要刪除索引，請按一下 **[資源]** 選取欄位右側的 **[刪除]** 按鈕。

刪除索引僅會從配置中移除索引，而不會修改目前可能在索引屬性中儲存值的所有現有目錄使用者。

備註 刪除索引僅會從配置中移除索引，而不會修改目前可能在索引屬性中儲存值的所有現有目錄使用者。

圖說文字配置

選取 [圖說文字配置] 區段中的此選項可以啓用圖說文字。啓用圖說文字後，會顯示圖說文字對映，可讓您爲每個列出的作業事件類型選取作業前與作業後選項。

依預設，作業前與作業後選項都設定爲 [無]。

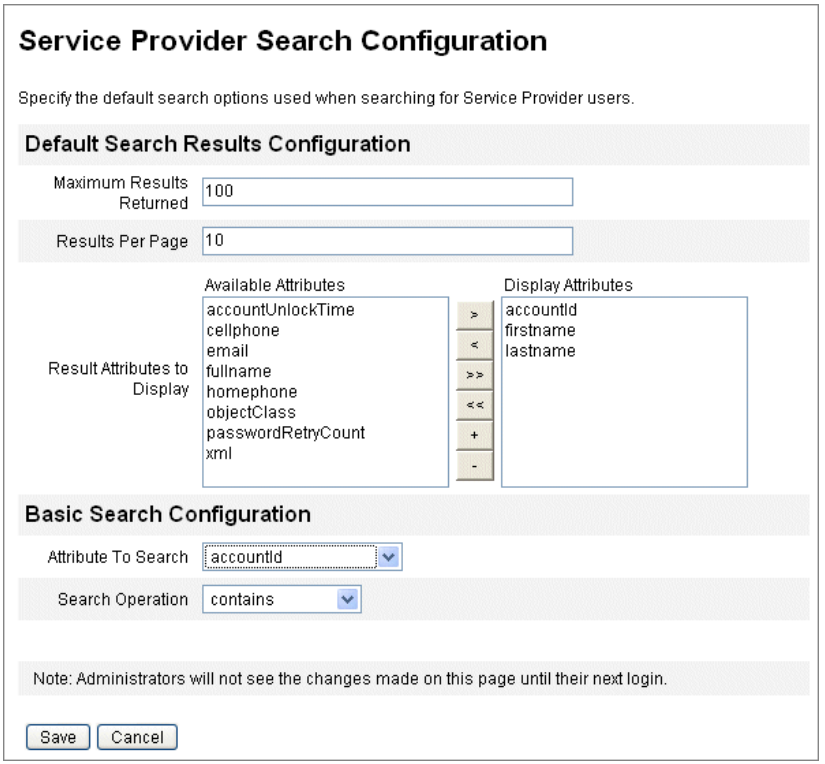
如果您指定作業後圖說文字，請使用 **[等待作業後圖說文字]** 選項指定作業事件必須等待作業後圖說文字處理完成後才能完成。如此可確保僅在作業後圖說文字成功完成後執行任何附屬作業事件。

備註 在 [服務提供者配置] 頁面的所有區段中完成選取之後，請按一下 **[儲存]** 以完成配置。

編輯使用者搜尋配置

使用此頁面 (如圖 17-4 所示)，可以針對委託管理員在 [管理服務提供者使用者] 頁面上進行的搜尋，配置預設的搜尋設定。這些預設適用於 [管理「服務提供者」使用者] 頁面的所有使用者，但是可在每個階段作業期間置換這些預設。

圖 17-4　　搜尋配置



若要配置預設搜尋設定，以搜尋服務提供者使用者，請執行以下步驟：

1. 按一下功能表列中的 **[服務提供者]**。
2. 按一下 **[編輯使用者配置]**。
3. 爲 **[可傳回的最多結果數目]** 輸入數字 (預設爲 100)。
4. 爲 **[每頁結果數目]** 輸入數字 (預設爲 10)。
5. 使用箭頭鍵選取 **[要顯示的結果屬性]** 旁邊的 **[可用屬性]**。
6. 從清單中選取 **[要搜尋的屬性]**。
7. 從清單中選取 **[搜尋作業]**。
8. 按一下 **[儲存]**。

備註 對搜尋配置所做的變更在您登出並再次登入之後才會生效。

若未配置服務提供者目錄，則無法使用這些配置物件。

作業事件管理

一個作業事件封裝一項佈建作業，例如，建立新使用者或指定新資源。爲確保這些作業事件在資源不可用時也能完成，將其寫入作業事件永久性存放區。

本小節中的以下主題包含用於管理服務提供者作業事件的程序：

- 設定預設作業事件執行選項
- 設定作業事件永久存放區
- 設定進階作業事件處理設定
- 監視作業事件

設定預設作業事件執行選項

這些選項控制執行作業事件的方式，包含同步/非同步處理以及將其保留至「作業事件永久存放區」中的時間。可以在 IDMXUser 檢視中置換它們或透過用於處理作業事件的表單來置換。如需更多資訊，請參閱「Identity Manager Service Provider Deployment」。

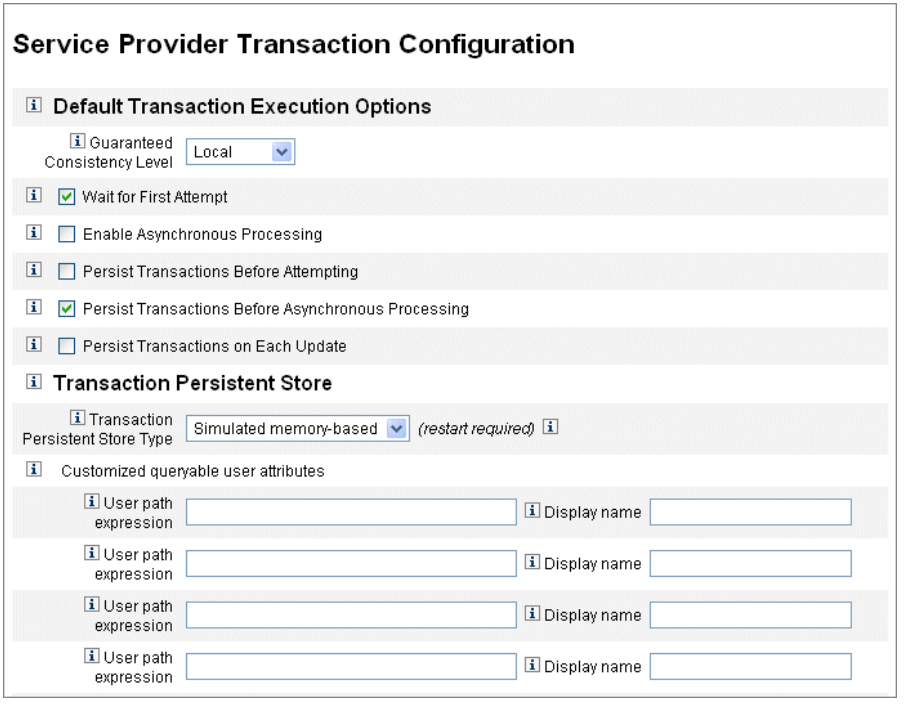
若要配置服務提供者作業事件，請執行以下步驟：

1. 按一下 **[服務提供者] > [編輯作業事件配置]。**

   [服務提供者作業事件配置] 頁面會隨即顯示。

   圖 17-5 顯示了 [預設作業事件執行選項] 區域。

圖 17-5 作業事件配置



2. 從以下選項中選取 **[一致性水準保證]**，以爲使用者更新指定作業事件一致性層級：
   - **無** - 不擔保使用者的資源更新按順序進行
   - **本機** - 擔保由相同伺服器所處理的使用者資源更新按順序進行。
   - **完整** - 擔保使用者的所有資源更新在所有伺服器上都按順序進行。此選項要求在嘗試或非同步處理之前保留所有作業事件。
3. 選取以下您選擇啓用的預設作業事件執行選項：
   - **等待第一次嘗試** - 指定在簽入 IDMXUser 檢視物件時，將控制項傳回給呼叫者的方式。如果啓用此選項，則會封鎖簽入作業，直到佈建作業事件完成一次嘗試。如果停用非同步處理，則傳回控制項時，作業事件會成功或失敗。如果啓用非同步處理，則會繼續在背景中重試作業事件。如果停用該選項，則登入作業會在嘗試佈建作業事件之前將控制項傳回給呼叫者。考慮啓用此選項。
   - **啓用非同步處理** - 此選項可控制在簽入呼叫傳回後，是否繼續處理佈建作業事件。

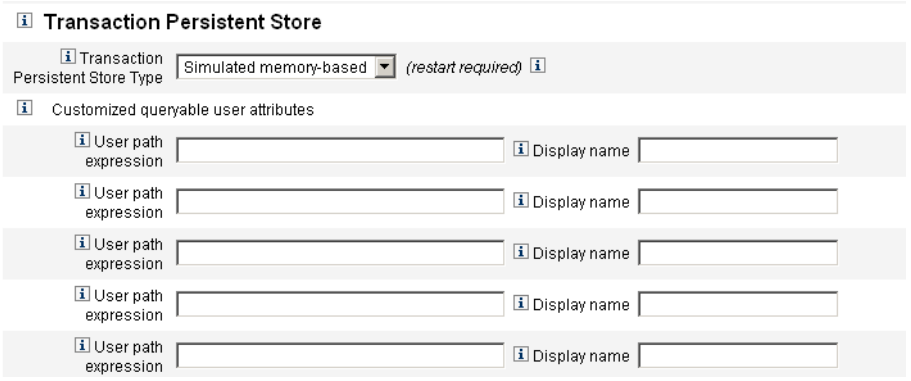
     啓用非同步處理可讓系統重試作業事件。亦可讓「設定進階作業事件處理設定」中所配置的工作者執行緒以非同步方式執行，進而提升流量。如果您選取此選項，則應爲要佈建或透過同步輸入表單更新的資源配置重試間隔和嘗試次數。

     選取 **[啓用非同步處理]** 後，請輸入 **[重試逾時]** 值。這是伺服器重試失敗佈建作業事件的時間長度上限 (以毫秒爲單位)。此設定可補充個別資源 (包括服務提供者使用者 LDAP 目錄) 上的重試設定。例如，如果在達到資源重試限制之前達到此限制，則會中斷作業事件。如果值爲負數，則重試次數僅受個別資源的設定限制。
   - **在嘗試之前保留作業事件** - 如果啓用此選項，則會在嘗試進行佈建作業事件之前，將其寫入作業事件永久存放區。因爲大多數佈建作業事件會在第一次嘗試時即成功，所以啓用此選項可能會帶來不必要的經常性耗用時間。除非已停用 **[等待第一次嘗試]** 選項，否則請考慮停用此選項。如果選取 [完成] 一致性層級，則無法使用此選項。
   - **在非同步處理之前保留作業事件** (預設選項) - 如果啓用此選項，則會在以非同步方式處理佈建作業事件之前，將其寫入作業事件永久存放區。如果啓用 [等待第一次嘗試] 選項，則會在將控制項傳回給呼叫者之前，保留需要重試的作業事件。如果停用 [等待第一次嘗試] 選項，則在嘗試作業事件之前始終會將其保留。建議您啓用此選項。如果選取 [完成] 一致性層級，則無法使用此選項。
   - **每次更新時保留作業事件** - 如果啓用此選項，則會在每次重試嘗試佈建作業事件之後，保留這些作業事件。因爲作業事件永久存放區 (可從 **[搜尋作業事件]** 頁面搜尋) 一律會保持最新狀態，所以這樣可以協助找出問題。

設定作業事件永久存放區

[服務提供者作業事件配置] 頁面上的選項，適用於作業事件永久存放區。可以配置存放區的類型以及要顯示在存放區中的其他可查詢屬性，如下圖所示。

圖 17-6 配置服務提供者作業事件永久存放區



若要設定 [服務提供者作業事件配置] 頁面上的選項，請執行以下步驟：

1. 從清單中選取所需的 **[作業事件永久存放區類型]**。

   如果選取 **[資料庫]** 選項，則在服務提供者主配置頁面上配置的 RDBMS 將用於保留佈建作業事件。這可保證在重新啟動伺服器時，必須重試的作業事件不會遺失。選取此選項需要在服務提供者主配置頁面上配置 RDBMS。如果選取 **[基於虛擬記憶體]** 選項，則需要重試的作業事件僅會儲存在記憶體中，並且在重新啟動伺服器時會遺失。對於生產環境，請啓用 **[資料庫]** 選項。

備註

基於記憶體的作業事件永久存放區不適合在叢集環境中使用。

變更 **[作業事件永久性存放區類型]** 後，您必須重新啟動所有正在執行的 Identity Manager 實例，以使變更生效。

2. 如有需要，請輸入 **[自訂的可查詢使用者屬性]**。

   選取 IDMXUser 物件的其他屬性以顯示在作業事件摘要中。這些屬性可從搜尋作業事件頁面進行查詢，並且顯示在搜尋結果中。其中包含：

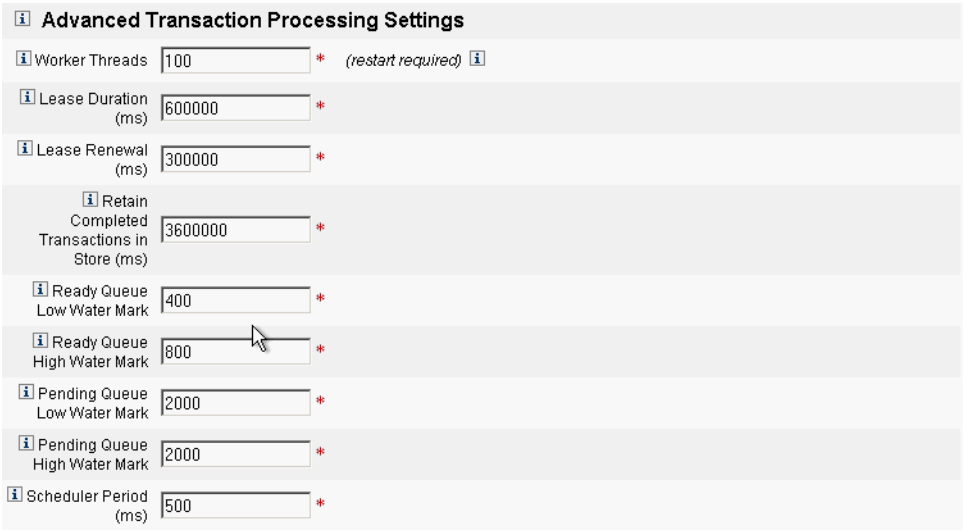
   - **使用者路徑表示式** - 將路徑表示式輸入 IDMXUser 物件中。
   - **顯示名稱** - 選擇與路徑表示式對應的顯示名稱。此顯示名稱會顯示在作業事件搜尋頁面上。

設定進階作業事件處理設定

這些進階選項可控制作業事件管理員的內部工作。請勿變更提供的預設設定，除非效能分析表明它們不是最佳設定。所有項目都是必需的。

圖 17-5 說明了 [編輯作業事件配置] 頁面上的 [進階作業事件處理設定] 區域。

圖 17-7 進階作業事件處理設定



1. 輸入所需的 **[工作者執行緒] 數目 (預設爲 100)。**

   這是用於處理作業事件的執行緒數目。此值可限制同時處理的作業事件數目。這些執行緒在啓動時靜態配置。

備註 變更 **[工作者執行緒]** 設定後，您必須重新啓動所有正在執行的 Identity Manager 實例，以使變更生效。

2. 輸入所需的 **[租用持續時間 (ms)] (預設爲 600000)。**

   其可控制伺服器鎖定其正在重試之作業事件的時間長度。將依需要更新租用。但是，如果伺服器未正常關機，則其他伺服器只有在原始伺服器的租用過期之後才可鎖定該作業事件。值應至少爲一分鐘。將值設定得較小會影響「作業事件永久存放區」的負載。

3. 輸入所需的 **[租用更新 (ms)]** 時間 **(預設爲 300000)**。

   其可控制更新鎖定作業事件租用的時間。當租用還剩餘該毫秒值時會更新。

4. 將所需時間輸入 **[將完成的作業事件保留在存放區中 (ms)] (預設爲 360000)**。

   在從作業事件永久存放區中移除完成的作業事件之前等待的時間長度 (以毫秒爲單位)。除非作業事件配置爲立即保留，否則「作業事件永久存放區」不會包含所有完成的作業事件。

5. 輸入所需的 **[就緒佇列低浮水印] (預設爲 400)**。

   當可以執行之作業事件的作業事件排程程式佇列低於此限制時，將使用可用的可以執行之作業事件重新填充佇列以達到高浮水印。

6. 輸入所需的 **[就緒佇列高浮水印] (預設爲 800)**。

   當可以執行之作業事件的作業事件排程程式佇列低於低浮水印時，將使用可用的可以執行之作業事件重新填充佇列以達到此限制。

7. 輸入所需的 **[擱置佇列低浮水印] (預設爲 2000)**。

   作業事件排程程式的擱置佇列保留擱置重試的失敗作業事件。如果佇列的大小超出高浮水印，則超過低浮水印的所有作業事件都會進入作業事件永久存放區。

8. 輸入所需的 **[擱置佇列高浮水印] (預設爲 2000)**。

   作業事件排程程式的擱置佇列保留擱置重試的失敗作業事件。如果佇列的大小超出高浮水印，則超過低浮水印的所有作業事件都會進入作業事件永久存放區。

9. 輸入所需的 **[排程程式期間 (ms)]** (預設爲 500)。

   這是應執行作業事件排程程式的頻率。當作業事件排程程式執行時，其會將可以執行之作業事件從擱置佇列移至就緒佇列，並執行其他定期任務，例如將作業事件保留在作業事件永久存放區中。

10. 按一下 **[儲存]** 以接受設定。

監視作業事件

將服務提供者作業事件寫入作業事件永久存放區。您可以在作業事件永久存放區中搜尋作業事件，以檢視作業事件狀態。

備註 使用 [編輯作業事件配置] 頁面 (請參閱「作業事件管理」)，管理員可以控制何時保留作業事件。例如，即使在第一次嘗作業事件之前，也可以立即保留它們。

[作業事件搜尋] 頁面可讓您指定搜尋條件，從而可讓您根據與作業事件相關的特定條件 (例如作業事件的使用者、類型、狀態、作業事件 ID、目前狀態以及成功或失敗) 來篩選要檢視的作業事件。其中包含仍在重試的作業事件，以及已完成的作業事件。對於尚未完成的作業事件，則可以將其取消，以防止任何進一步的嘗試。

若要搜尋作業事件，請執行以下步驟：

1. 在管理員介面中，按一下主功能表的 **[伺服器作業]**。
2. 按一下輔助功能表的 **[服務提供者作業事件]**。

   [服務提供者作業事件搜尋] 頁面會隨即開啓，以讓您指定搜尋條件。

備註 搜尋僅傳回符合以下所選的**所有**條件的作業事件。這與 **[帳號] > [尋找使用者]** 頁面相似。

3. 如有需要，選取 **[使用者名稱]**。

   此選項可讓您搜尋僅適用於具有您輸入的 **accountId** 之使用者的作業事件。

備註 如果您已在 [服務提供者作業事件配置] 頁面上配置任何自訂的可查詢使用者屬性，則它們會在此顯示。例如，您可以選擇根據姓氏或全名搜尋 (如果已將其配置爲自訂的可查詢使用者屬性)。

4. 如有需要，選取按 **[類型]** 搜尋。

   此選項可讓您搜尋所選類型的作業事件。

5. 如有需要，選取按 **[狀態]** 搜尋。

   此選項可讓您搜尋處於以下所選狀態的作業事件：

   - 尚未嘗試 **[未嘗試]** 作業事件。
   - 已嘗試一次或多次 **[擱置重試]** 作業事件，出現一個或多個錯誤，且已將其排定重試，重試次數最高爲針對個別資源配置的重試限制。
   - **[成功]** 作業事件已成功完成。
   - **[失敗]** 作業事件已完成，但發生一次或多次故障。

6. 如有需要，選取按 **[嘗試]** 搜尋。

   此選項可讓您根據嘗試作業事件的次數來搜尋作業事件。失敗的作業事件會被重試達到爲個別資源配置的重試限制。

7. 如有需要，選取按 **[已提交]** 搜尋。

   此選項可讓您根據初次提交作業事件的時間 (以小時、分鐘或天爲增量) 來搜尋作業事件。

8. 如有需要，選取按 **[已完成]** 搜尋。

   此選項可讓您依據完成作業事件的時間 (以小時、分鐘或天爲增量) 來搜尋作業事件。

9. 如有需要，選取按 **[取消的狀態]** 搜尋。

   此選項可讓您根據作業事件是否已取消來搜尋作業事件。

10. 如有需要，選取按 **[作業事件 ID]** 搜尋。

    此選項可讓您根據作業事件的唯一 ID 來搜尋作業事件。使用此選項可根據您輸入的 ID 值來尋找作業事件，該 ID 值顯示在所有稽核記錄中。

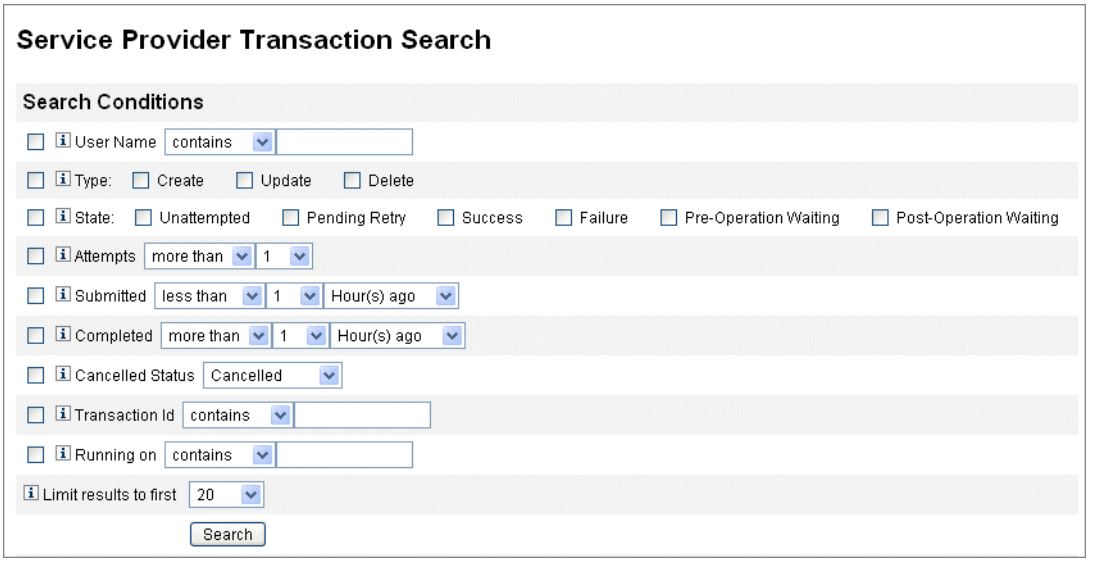
11. 如有需要，選取按 **[執行於]** (伺服器名稱) 搜尋。

    此選項可讓您根據執行作業事件的服務提供者伺服器來搜尋作業事件。除非已在 `Waveset.properties` 檔案中置換伺服器的識別碼，否則伺服器識別碼依其機器名稱而定。

12. 將搜尋結果限制爲從清單中選取的第一個項目數。

    傳回的結果數目不能超過指定的限制。如果有更多的結果可用，不會做任何指示。

圖 17-8 搜尋作業事件



13. 按一下 **[搜尋]**。

    螢幕上將顯示搜尋結果。

14. 如有需要，按一下結果頁面底部的 **[下載所有相符的作業事件]**。這會將結果儲存爲 XML 格式檔案。

備註 您可以取消搜尋結果中傳回的作業事件。在結果表格中選取作業事件，然後按一下 **[已選取 [取消]]**。無法取消已完成或已取消的作業事件。

託管

使用 Identity Manager 管理員角色或透過基於組織的授權模式，可啓用服務提供者使用者的託管。

透過組織授權進行委派

依預設，Identity Manager 透過基於組織的授權模式來提供管理責任委派。在基於組織的授權模式中建立委託管理員時，請記住以下幾點：

- 服務提供者管理員是具有特定權能和所控制的組織之 Identity Manager 使用者。
- 使用者的組織屬性值可以是 Identity Manager 組織的名稱或物件 ID。這取決於 [Identity Manager 主配置] 螢幕中 **[Identity Manager 組織屬性名稱包含 ID]** 欄位的設定。
- 您可以建立 Identity Manager 階層，並以您要委託組織管理的方式將組織置於該階層中。使用組織的特定標識，而不是組織的簡單名稱。
- 服務提供者使用者透過目錄伺服器中的使用者屬性取得其組織。
  - 您必須在目錄伺服器資源的模式對映中設定這些屬性。
  - 透過完全比對管理員之所控制的組織清單，進行屬性的比較。儲存在目錄中的值必須符合組織名稱，而不是整個階層。如果管理員控制 `Top:orgA:sub1`，則 `sub1` 必須是儲存在服務提供者使用者之組織屬性中的值。
  - 如果未設定屬性或屬性未對應至 Identity Manager 組織，則會將服務提供者使用者視爲 Top 組織的成員。這需要服務提供者管理員擁有 `Top` 中的「服務提供者」使用者權能，才能管理這些使用者。
- 屬性設定可確定服務提供者管理員進行搜尋的範圍。
- 若要建立委託管理員帳號，您首先要建立 Identity Manager 管理員，然後增加服務提供者管理員權能。有一些服務提供者作業特有的權能可以指定給使用者 (在 **[編輯使用者]** 頁面的 **[安全性]** 標籤上)。所控制的組織可指定管理員可以修改的服務提供者使用者。適用於服務提供者使用者的所有資源均適用於所有 Identity Manager 管理員。

備註 如需有關 Identity Manager 託管的更多資訊，請參閱第 6 章「管理」中的「託管」。

透過管理員角色指定進行委派

若要授予對服務提供者使用者的細緻權能和控制範圍，請使用服務提供者使用者管理員角色。可以配置管理員角色，以在登入時動態地將其指定給一個或多個 Identity Manager 或服務提供者使用者。

可以定義規則並將其指定給管理員角色，管理員角色可指定授予具有指定管理員角色之使用者的權能 (例如服務提供者建立使用者)。

若要針對服務提供者使用者使用管理員角色委派，則必須在 Identity Manager 系統配置物件中啓用該委派 (第 197 頁)。

若啓用透過管理員角色指定進行委派，則不需要 [服務提供者配置] 中的 [IDM 組織屬性名稱]。

啟用服務提供者管理員角色委派

若要啓用服務提供者管理員角色委派 (服務提供者託管)，請開啓系統配置物件以進行修改 (第 197 頁)，並將下列特性設爲 「`true`」：

`security.authz.external.`*app name*`.`*object type*

其中 *app name* 是 Identity Manager 應用程式 (例如管理員介面)，*object type* 是服務提供者使用者

可以針對 Identity Manager 應用程式 (例如管理員介面或使用者介面) 和物件類型啓用此特性。目前，唯一的受支援物件類型爲服務提供者使用者。預設值爲 `false`。

例如，若要爲 Identity Manager 管理員啓用服務提供者託管，請將 「系統配置」配置物件中的下列屬性設爲 「true」：

```
security.authz.external.Administrator Interface.Service Provider Users
```

若停用指定的 Identity Manager 或服務提供者應用程式的「服務提供者託管」(設爲「false」)，則會使用組織型授權模型。

啓用服務提供者託管時，追蹤的事件會擷取有關執行的授權規則數目和持續時間的資訊。這些統計可在面板上找到。

配置服務提供者使用者管理員角色

若要配置服務提供者的使用者管理員角色，請建立管理員角色，並指定控制範圍、權能以及應該指定該角色的使用者。

備註 在建立服務提供者使用者管理員規則之前，請定義管理員角色的搜尋環境、搜尋篩選、搜尋篩選後、權能和使用者指定規則。您必須指定規則的 `authType`，才能使用這些規則 (即 SPEUsersSearchContextRule、SPEUsersSearchFilterRule、SPEUsersAfterSearchFilterRule、CapabilitiesOnSPEUserRule、UserIsAssignedAdminRoleRule、SPEUserIsAssignedAdminRoleRule)。

Identity Manager 提供了您可以用來爲服務提供者使用者管理員角色建立這些規則的規則範例。您可在 Identity Manager 安裝目錄的 `sample/adminRoleRules.xml` 中找到這些規則。

如需有關爲您的環境建立這些規則的更多資訊，請參閱「Identity Manager Service Provider Deployment」。

若要配置服務提供者的使用者管理員角色，請執行以下步驟：

1. 在管理員介面中，按一下功能表的 **[安全性]**，然後按一下 **[管理員角色]**。

   [管理員角色] 頁面會隨即開啓。

2. 按一下 **[新增...]**。

   [建立管理員角色] 頁面會隨即開啓。

3. 指定管理員角色名稱，並選取 **[「服務提供者」使用者]** 類型。

4. 指定 **[控制範圍]**、**[權能]** 和 **[指定給使用者]** 選項 (如下列各節所述)。

指定控制範圍

服務提供者使用者管理員角色的控制範圍可指定允許指定之 Identity Manager 管理員、Identity Manager 一般使用者或 Identity Manager 服務提供者一般使用者查看的服務提供者使用者。當請求在目錄中列出服務提供者使用者時，會強制指定控制範圍。

對於服務提供者使用者管理員角色的控制範圍，您可以指定以下一個或多個設定：

- **使用者搜尋環境** - 指定要使用規則還是文字字串開始搜尋。

  如果指定 [無]，則預設搜尋環境將是在配置爲服務提供者使用者目錄的 Identity Manager 資源中指定的基底環境。

- **使用者搜尋篩選** - 指定要將規則還是文字字串套用至搜尋篩選。

  所選規則指定或傳回的文字字串應爲表示使用者集的 LDAP 相容搜尋篩選字串，在搜尋環境中，這些使用者將由具有此指定管理員角色的使用者控制。指定的篩選將與使用者指定的搜尋篩選結合，以確保搜尋傳回的使用者不包括未授權具有此指定管理員角色之使用者列出的任何使用者。

- **使用者搜尋篩選後規則** - 選取將在套用使用者搜尋篩選之後套用的規則。

  此規則會在對服務提供者使用者目錄執行初始 LDAP 搜尋之後執行，並會計算結果以決定允許請求使用者存取的辨別名稱 (DN)。

  在以下情況下可使用此類型的規則：當您需要使用非 LDAP 使用者屬性 (例如，群組成員) 確定某使用者是否應在請求使用者的控制範圍內時，或需要使用儲存庫而非服務提供者使用者目錄 (例如 Oracle 資料庫或 RACF) 做出篩選決定時。

指定權能

服務提供者使用者管理員角色的權能可指定，請求使用者對所請求存取之服務提供者使用者具有的權能與權限。當請求在檢視、建立、修改或刪除服務提供者使用者時，會強制指定權能。

在 **[權能]** 標籤上，選取要套用至此管理員角色的 **[權能規則]**。

將管理員角色指定給使用者

透過指定將在登入時進行計算以確定是否爲認證使用者指定管理員角色的規則，可以將服務提供者使用者管理員角色動態地指定給服務提供者使用者。

按一下 **[指定給使用者]** 標籤，然後選取要套用至指定的規則。

備註 必須爲每個登入介面 (例如使用者介面和管理員介面) 啓用將管理員角色動態指定給使用者的功能，方法是將下列系統配置物件 (第 197 頁) 設爲 `true`：

`security.authz.checkDynamicallyAssignedAdminRolesAtLoginTo.logininterface`

所有介面的預設均爲 `false`。

委託服務提供者使用者管理員角色

依預設，服務提供者使用者可以將指定給他們的服務提供者使用者管理員角色指定 (或委託) 給其控制範圍內的其他服務提供者使用者。

事實上，任何具有編輯服務提供者使用者權能的 Identity Manager 使用者均可以將指定給他們的服務提供者使用者管理員角色指定給其控制範圍內的服務提供者使用者。

服務提供者使用者管理員角色也可以包含不論控制範圍爲何均可指定管理員角色的指定者清單。這些直接指定可以確保至少一個已知使用者帳號可指定管理員角色。

管理服務提供者使用者

本小節包含透過 Identity Manager 管理服務提供者使用者的程序和資訊。包含以下主題：

- 使用者組織
- 建立使用者和帳號
- 搜尋服務提供者使用者
- 連結帳號
- 刪除、取消指定或取消連結帳號

使用者組織

透過服務提供者，使用者的屬性值可確定將該使用者指定給的組織。其透過 [服務提供者主配置] (請參閱「初始配置」) 中的 [Identity Manager 組織屬性名稱] 欄位指定。但是，這些組織的名稱必須符合在目錄伺服器中指定的使用者屬性值。

若定義了 **[Identity Manager 組織屬性名稱]**，則 [建立使用者] 和 [編輯使用者] 頁面會顯示可用組織的多重選取清單。依預設，顯示短的組織名稱。您可以修改 [服務提供者使用者表單] 以顯示完整的組織路徑。

您可以挑選哪個屬性將成爲組織名稱屬性。然後便可在服務提供者使用者管理頁面中使用此組織名稱屬性限制可以搜尋和管理該使用者的管理員。

備註 現在有服務提供者和資源帳號的帳號 ID 和密碼策略。

您可以從主 [策略] 表格中取得 **[服務提供者系統帳號策略]**。

建立使用者和帳號

所有服務提供者使用者均必須在服務提供者目錄中具有帳號。如果某使用者在其他資源上具有帳號，則指向這些帳號的連結會儲存在使用者的目錄項目中，因此當檢視該使用者時可使用有關這些帳號的資訊。

備註 提供了用於建立和編輯使用者的服務提供者使用者表單範例。自訂此表單以滿足在您的服務提供者環境中管理使用者的需求。如需更多資訊，請參閱「Identity Manager Workflows, Forms, and Views」。

若要建立服務提供者帳號，請執行以下步驟：

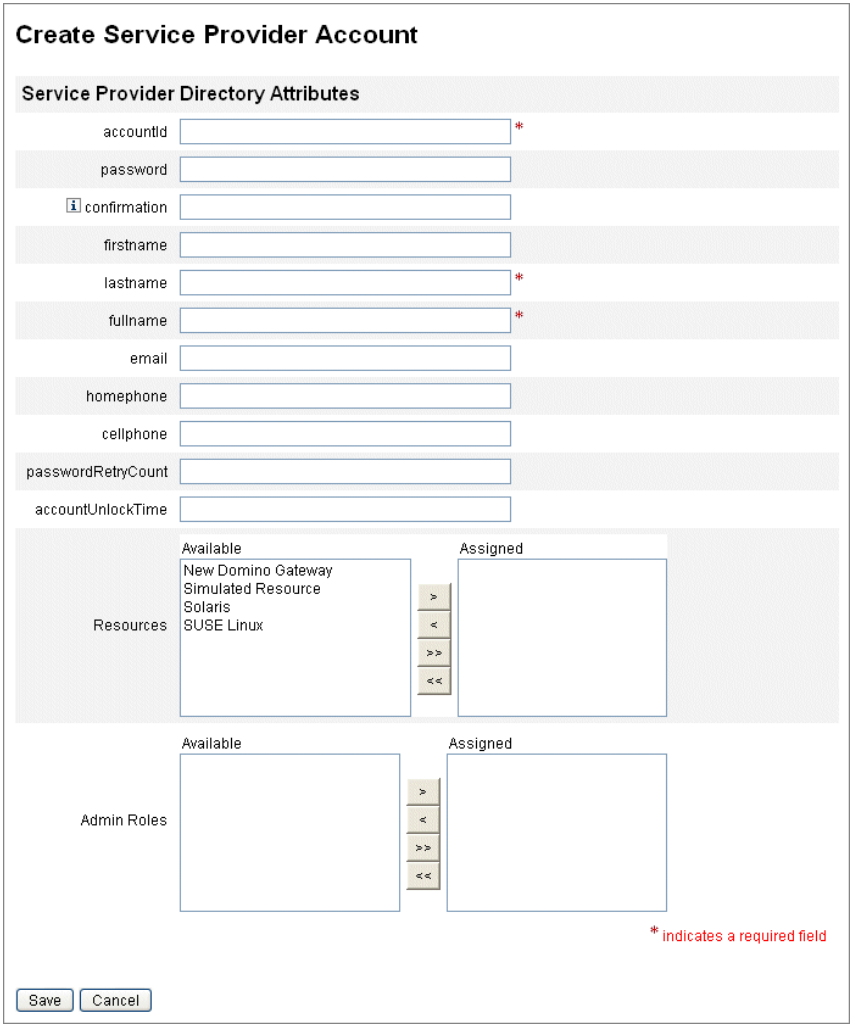
1. 在管理員介面中，按一下功能表列的 **[帳號]**。
2. 按一下 **[管理「服務提供者」使用者]** 標籤。
3. 按一下 **[建立使用者]**。

備註 使用預設服務提供者使用者表單時，實際顯示的欄位取決於在服務提供者目錄資源之 [帳號屬性] 表 (模式對映) 中配置的屬性。而且，當您將資源指定給使用者 (例如委託管理員) 時，可以看到顯示中增加了新的區段，您可以在其中指定這些資源的屬性值。您還可以自訂欄位。

4. 依需要輸入以下值：
   - **accountid** (這是必填欄位)
   - **password**
   - **confirmation** (這是密碼確認)
   - **firstname** (這是必填欄位)
   - **lastname** (這是必填欄位)
   - **fullname**
   - **email**
   - **home phone**
   - **cell phone**
   - **password retry count**
   - **account unlock time**
5. 使用箭頭鍵從 [可用] 清單中指定所需的 [資源]。

6. **[帳號狀態]** 顯示帳號是處於鎖定還是解除鎖定狀態。按一下此選項可鎖定或解除鎖定帳號。

圖 17-9　　建立服務提供者使用者和帳號



備註 此表單可自動根據爲目錄帳號 (在頂部) 定義的屬性寫入資源帳號屬性的值。例如，如果資源定義 `firstName`，則產品會將其與目錄帳號的 `firstName` 值一起寫入。但是在此初始寫入後，對這些屬性所做的修改不會傳遞至資源帳號。請視需要自訂提供的服務提供者使用者表單範例。

7. 按一下 **[儲存]** 以建立使用者帳號。

搜尋服務提供者使用者

服務提供者包含可配置的搜尋權能，可協助管理使用者帳號。搜尋僅會傳回在您的範圍 (如您的組織或其他因子所定義) 內的使用者。

若要執行服務提供者使用者基本搜尋 (從 Identity Manager 介面的 **[帳號]** 區域)，請按一下 **[管理 「服務提供者」使用者]**，然後輸入搜尋值並按一下 **[搜尋]**。

以下主題說明了服務提供者搜尋功能：

- 進階搜尋
- 搜尋結果
- 刪除、取消指定或取消連結帳號
- 設定搜尋選項

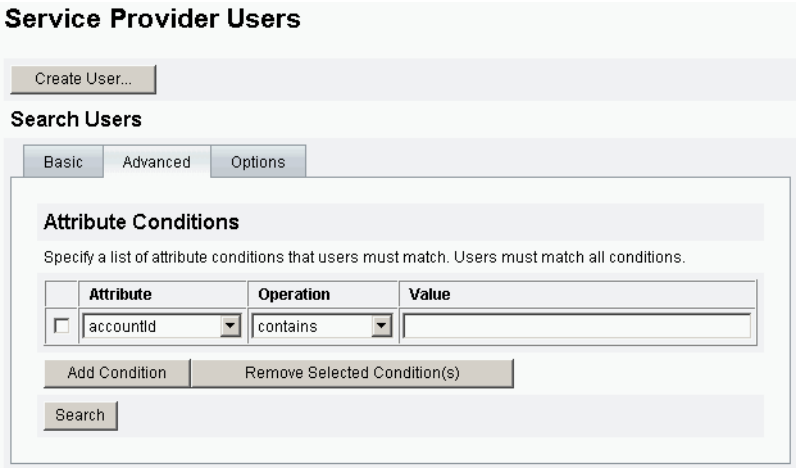
進階搜尋

若要執行服務提供者使用者進階搜尋 (從 [「服務提供者」使用者搜尋] 頁面)，請按一下 **[進階]**，然後完成以下動作：

1. 從清單中選擇所需的 **[屬性]**。
2. 從清單中選擇所需的 **[作業]**。

   您將指定一組條件以便篩選搜尋傳回的使用者，傳回的使用者必須滿足所有指定的條件。
3. 輸入所需的搜尋值，然後按一下 **[搜尋]**。

圖 17-10　搜尋使用者



您可以使用以下選項增加或移除 [屬性條件]：

- 按一下 **[增加條件]** 並指定新屬性。
- 選取項目並按一下 **[移除選取的條件]**。

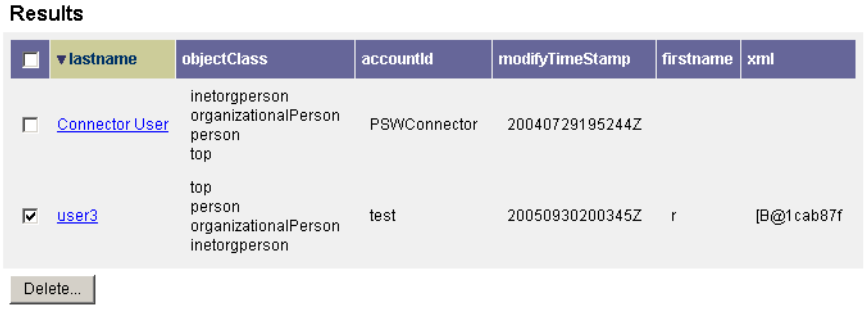
搜尋結果

服務提供者搜尋結果顯示在表格中，如圖 17-11 所示。可透過按一下屬性的欄標頭依任何屬性對結果進行排序。顯示的結果取決於您選取的屬性。

箭頭按鈕可瀏覽至結果的第一頁、上一頁、下一頁和最後一頁。您可以在文字方塊中輸入數字然後按下 Enter 鍵，以跳躍至特定頁面。

若要編輯使用者，請按一下表格中的使用者名稱。

圖 17-11　　搜尋結果範例



在搜尋結果頁面中，您可選取一個或多個使用者並按一下 **[刪除]** 按鈕，以刪除使用者或取消連結資源帳號。此動作可顯示刪除使用者頁面，並顯示其他選項 (請參閱「刪除、取消指定或取消連結帳號」)。

連結帳號

服務提供者可安裝在使用者於多項資源上皆具有帳號的環境中。服務提供者的帳號連結功能可讓您以增量方式，將現有的資源帳號指定給服務提供者使用者。帳號連結程序由服務提供者連結策略所控制，此策略可定義連結相互關聯規則、連結確認規則與連結驗證選項。

若要連結使用者帳號，請執行以下步驟：

1. 在管理員介面中，按一下功能表列的 **[資源]**。
2. 選取所需資源。
3. 從 [資源動作] 功能表中選取 **[編輯服務提供者連結策略]**。
4. 選取連結相互關聯規則。此規則會在資源上搜尋使用者可能擁有的帳號。
5. 選取連結確認規則。此規則可從連結相互關聯規則所選取之潛在帳號的清單中，排除所有資源帳號。

備註 若連結相互關聯規則所選取的帳號不超過一個，則不需要連結確認規則。

---

6. 選取 **[需要進行連結驗證]**，將目標資源帳號連結至服務提供者使用者。

刪除、取消指定或取消連結帳號

若要刪除、取消指定或取消連結使用者帳號，請執行以下步驟：

1. 按一下功能表列中的 **[帳號]**。
2. 按一下 **[管理「服務提供者」使用者]**。
3. 執行基本搜尋或進階搜尋。
4. 選取所需的一個或多個使用者。
5. 按一下 **[刪除]** 按鈕。
6. 如有需要，請選取其中一個全域選項：
   - **Delete All resource accounts**

     備註 刪除資源將刪除該帳號，但是指定資源仍存在。使用者的後續更新會重新建立該帳號。刪除永遠意味著取消連結資源帳號。

   - **Unassign All resource accounts**

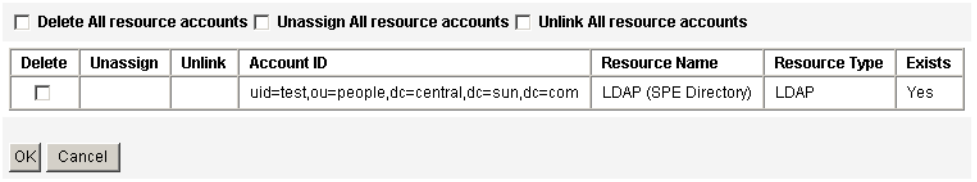
     備註 解除指定資源會移除該指定資源。解除指定意味著取消資源帳號的連結。取消指定資源時，不會刪除資源帳號。

   - **Unlink All resource accounts**

     備註 取消連結將移除使用者和資源帳號之間的連結，但不會刪除帳號。也不會移除指定資源，因此對使用者的後續更新會重新連結帳號或建立一個新的資源帳號。

7. 或者，在 **[刪除]**、**[解除指定]** 或 **[取消連結]** 欄中，爲一個或多個資源帳號選取動作。
8. 選取需要的使用者帳號後，按一下 **[確定]**。

圖 17-12 刪除、取消指定或取消連結帳號



設定搜尋選項

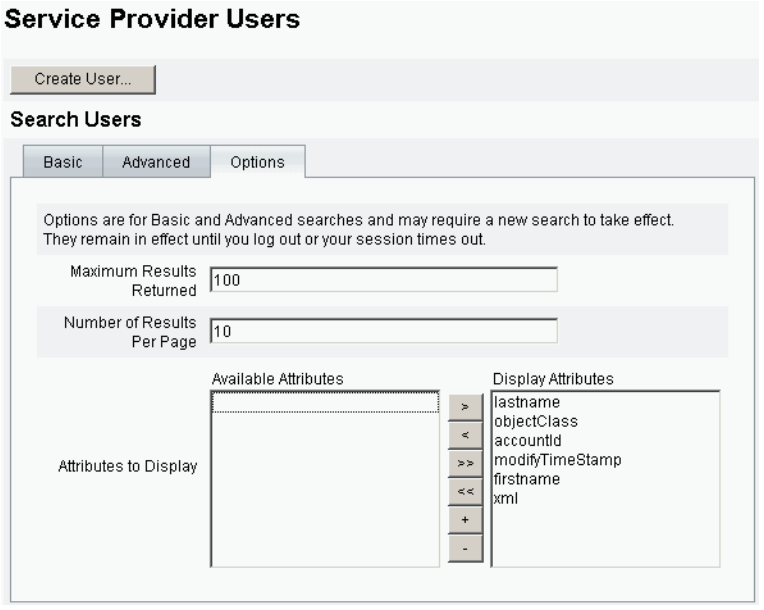
若要設定服務提供者使用者的搜尋選項，請執行以下步驟：

1. 在管理員介面中，按一下功能表列的 **[帳號]**。
2. 按一下 **[服務提供者]**。
3. 按一下 **[選項]**。

備註 這些選項僅對目前的登入階段作業有效。這些選項會影響搜尋結果的顯示方式，影響基本搜尋和進階搜尋結果，並且某些設定僅在進行新的搜尋時才生效。

4. 輸入 **[可傳回的最多結果數目]**。
5. 輸入 **[每頁結果數目]**。
6. 使用箭頭鍵從 **[可用屬性]** 中選擇所需的 **[顯示屬性]**。

圖 17-13 設定服務提供者使用者的搜尋選項



一般使用者介面

隨附的一般使用者頁面範例提供了 xSP 環境中特有的註冊和自助範例。這些範例可延伸且可自訂。您可以變更外觀、修改頁面間的瀏覽規則，或顯示適用於部署的語言環境特定訊息。如需有關自訂一般使用者頁面的進一步資訊，請參閱「Identity Manager Service Provider Deployment」。

除了稽核自助和註冊事件外，還可以使用電子郵件範本傳送給受影響之使用者的通知。還提供了使用帳號 ID 和密碼策略以及登出帳號的範例。應用程式開發者還可以增強 Identity Manager 表單。如果需要，可以延伸或替代作爲 Servlet 篩選器實作的模組認證服務。如此可與存取管理系統 (如 Sun Access Manager) 進行整合。

範例

隨附的一般使用者頁面範例可讓使用者透過一系列容易瀏覽的螢幕註冊並維護基本使用者資訊，以及接收其動作的電子郵件通知。

頁面範例包含以下功能：

- 登入 (和登出)，包括透過詢問問題進行認證
- 註冊
- 變更密碼
- 變更使用者名稱
- 變更詢問問題
- 變更通知地址
- 處理忘記使用者名稱的情況
- 處理忘記密碼的情況
- 電子郵件通知
- 稽核

備註 Identity Manager 使用驗證表進行註冊。僅允許此表中的使用者進行註冊。例如，當使用者 Betty Childs 註冊時，如果在驗證表中找到 Betty Childs 的項目 (包含電子郵件地址 bchilds@example.com)，則接受註冊。

您可以輕鬆地爲您的部署自訂這些頁面。可以自訂以下內容：

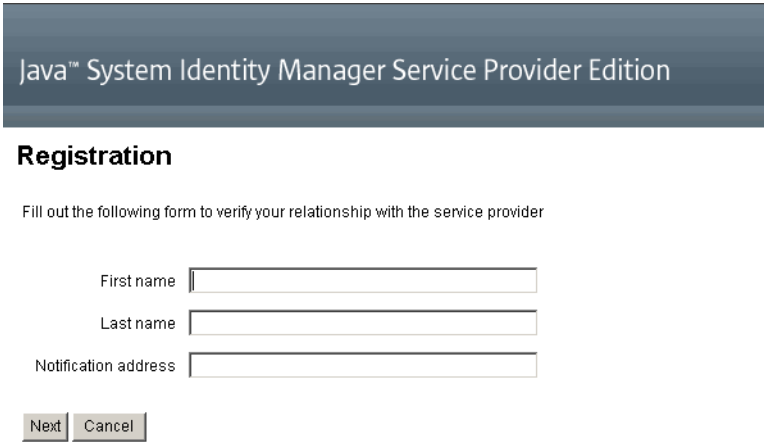
- 商標
- 配置選項 (例如失敗的登入嘗試次數)
- 增加/移除頁面

如需有關自訂頁面的更多資訊，請參閱「Identity Manager Service Provider Deployment」。

註冊

要求新使用者註冊。在註冊期間使用者可以設定其登入、詢問問題以及通知資訊。

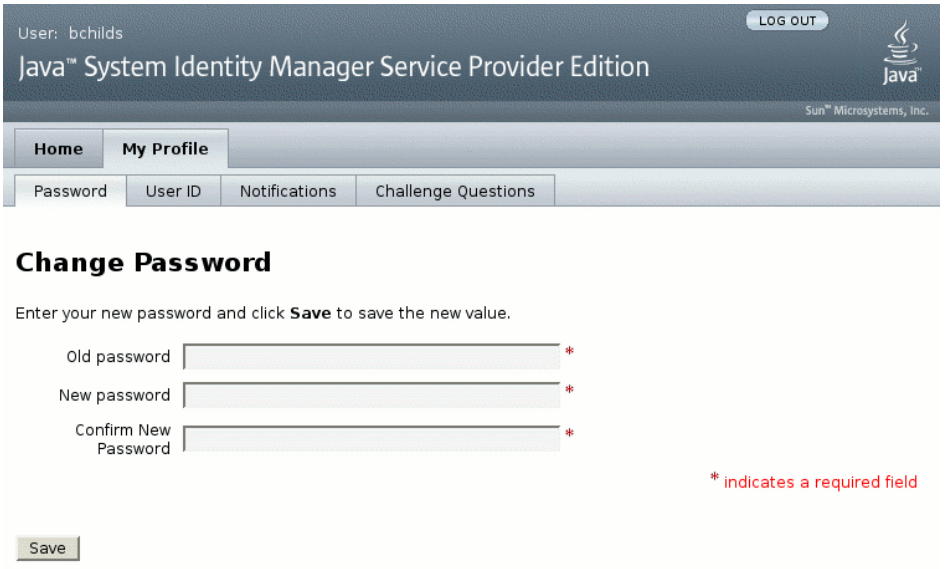
圖 17-14 [註冊] 頁面



[首頁] 螢幕和 [設定檔] 螢幕

圖 17-15 顯示了一般使用者 [首頁] 標籤和 [設定檔] 頁面。使用者可以變更其登入 ID 和密碼、管理通知以及建立詢問問題。

圖 17-15 [我的設定檔] 頁面



同步化

透過同步化策略可以啓用服務提供者使用者的同步化。若要使用 Identity Manager 爲服務提供者使用者同步化資源上屬性的變更，您必須配置服務提供者同步化。以下主題說明了如何在服務提供者實作中啓用同步化：

- 配置同步化
- 監視同步化
- 啓動和停止同步化
- 遷移使用者

備註 從 Identity Manager 之 **[資源]** 區域中的資源清單中配置服務提供者同步化。

配置同步化

若要配置服務提供者同步化，您需要按照第 259 頁的 「配置同步化」中的說明編輯資源的同步化策略。

編輯同步化策略時，必須指定以下選項以啓用服務提供者使用者的同步化程序。

- 選取 **[服務提供者使用者]** 作爲 [目標物件類型]。
- 在 [排程設定] 區段中，選取 **[啓用同步化]**。

按照第 259 頁的 「配置同步化」中的說明，指定適合您環境的其他選項。服務提供者同步化作業的預設同步化間隔爲 1 分鐘。

備註 確認規則和表單必須使用 IDMXUser 檢視，而非 Identity Manager 輸入使用者檢視 (請參閱 「Identity Manager Service Provider Deployment」以取得更多資訊)。

這是必要的，因爲確認規則會存取每個以相互關聯規則識別之使用者的使用者檢視，從而影響同步化效能。

按一下 **[儲存]** 以儲存策略定義。如果在策略中未停用同步化，則會按指定將其排定。如果指定了停用同步化，則會停止同步化服務 (如果目前正執行)。如果啓用，則將在重新啓動 Identity Manager 伺服器後，或在選取 [同步化資源動作] 下的 **[爲服務提供者啓動]** 後啓動同步化。

監視同步化

Identity Manager 提供了以下監視服務提供者同步化的方法。

- 在 [資源] 清單之說明欄位中檢視同步化狀態。
- 使用 JMX 介面監視同步化度量。

啟動和停止同步化

當您爲服務提供者實作配置 Identity Manager 時，預設會啓用服務提供者同步化。

若要停用服務提供者 Active Sync，請執行以下步驟：

1. 在管理員介面中，按一下功能表的 **[資源]**。

   [列出資源] 頁面會隨即開啓。

2. 在 [服務提供者] 區域中，選取資源，然後按一下 **[編輯同步化策略]** 以編輯策略。
3. 清除 **[啓用同步化]** 核取方塊。
4. 按一下 **[儲存]**。

   儲存策略後，同步化將停止。

若要停止同步化而不將其停用，請從 [同步化資源動作] 中選取 **[爲服務提供者停止]**。

備註 如果您使用資源動作停止同步化而不停用同步化，則在啓動任何 Identity Manager 伺服器後會將其再次啓動。

遷移使用者

服務提供者功能包含使用者遷移作業範例以及關聯的程序檔。此作業可將現有的 Identity Manager 使用者遷移至服務提供者使用者目錄。本小節說明了如何使用遷移作業範例。您可以修改此範例以適用於您的狀況。

若要遷移現有 Identity Manager 使用者，請執行以下步驟：

1. 在管理員介面中，按一下功能表的 **[伺服器作業]**。

   [尋找作業] 頁面會隨即開啓。

2. 按一下輔助功能表的 **[執行作業]**。

3. 按一下 **[SPE 遷移]**。

4. 輸入唯一的 **[作業名稱]**。

5. 從清單中選取 **[資源]**。

   此爲 Identity Manager 中表示服務提供者目錄伺服器的資源。不會遷移 Identity Manager 使用者中指向此資源的連結。

6. 輸入 **[身份識別屬性]**。

   此爲包含目錄使用者之唯一短身份識別的 Identity Manager 使用者屬性。

7. 從清單中選取 **[身份識別規則]**。

   這是可以由 Identity Manager 使用者屬性計算目錄使用者名稱的可選規則。身份識別規則可以計算簡單名稱 (通常爲 uid)，該簡單名稱然後會透過資源的身份識別範本得以處理，以形成目錄伺服器的辨別名稱 (DN)。此規則還可傳回不使用 ID 範本的完整指定 DN。

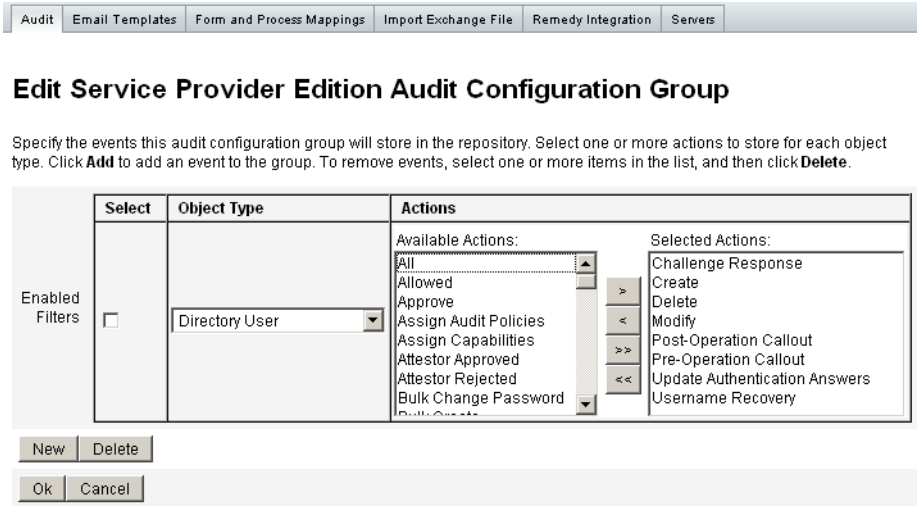
8. 按一下 **[啓動]** 以啓動背景遷移作業。

配置服務提供者稽核事件

在服務提供者實作中，Identity Manager 的稽核記錄系統會對與企業外部網路使用者作業相關的事件進行稽核。Identity Manager 提供 Service Provider Edition 稽核配置群組 (依預設已啓用)，以指定爲服務提供者使用者記錄的稽核事件。請參閱圖 17-16。

如需有關稽核記錄和修改 Service Provider Edition 稽核配置群組中事件的更多資訊，請參閱第 10 章「稽核記錄」。

圖 17-16　[編輯服務提供者稽核配置群組] 頁面



lh 參照

用法

使用下列語法呼叫 Identity Manager 指令行介面，並執行 Identity Manager 指令：

```
lh { $class | $command } [ $arg [$arg... ] ]
```

用法說明

- 若要顯示指令用法說明，請鍵入 `lh` (不使用任何引數)。
- 設定路徑環境變數：
  - 使用 `lh` 指令時，您應該將 `JAVA_HOME` 設定爲包含內有 Java 程式檔的 `bin` 目錄的 JRE 目錄。此位置視具體安裝目錄而有所不同。

    若有 Sun 提供的標準 JRE (不含 JDK)，目錄一般位於 `C:\Program Files\Java\jre1.5.0_14` (或類似位置)。此目錄包含內有 Java 程式檔的 `bin` 目錄。本例將 `JAVA_HOME` 設爲 `C:\Program Files\Java\jre1.5.0_14`。

    完整的 JDK 安裝有多個 Java 程式檔。在此情況下，請將 `JAVA_HOME` 設定爲內嵌的 `jre` 目錄，其中包含正確的 `bin/java.exe` 檔案。若爲一般安裝，請將 `JAVA_HOME` 設爲 `C:\java\jdk1.5.0_14\jre`。

  - 將 `WSHOME` 變數設定爲 Identity Manager 安裝目錄，如下所示：

    `set WSHOME=<`*`path_to_identity_manager_directory`*`>`

    例如，將變數設定爲預設安裝目錄：

    `Š]©w WSHOME=C:\Program Files\tomcat\webapps\idm`

備註 確定 WSHOME 變數的值「不含」下列符號：

- 引號 ( )
- 在路徑結尾處有反斜線 (\)

請勿使用引號，即使應用程式部署目錄的路徑中含有空格也一樣。

在 UNIX 系統上，還必須如下所示匯出路徑變數：

```
export WSHOME

export JAVA_HOME
```

- 若要在 64 位元模式中執行指令，請取消註釋 lh 程序檔中的 `FLAGS="$FLAGS -d64"` 行。
- 在 Windows 上，於指令行鍵入下列內容，即可啓動 Identity Manager 指令行介面：

  ```
  %WSHOME%\bin\lh
  ```

- 在 Unix 上，於指令行鍵入下列內容，即可啓動 Identity Manager 指令行介面：

  ```
  $WSHOME/bin/lh
  ```

class

必須是完全合格的類別名稱，如 `com.waveset.session.WavesetConsole`。

指令

必須爲下列其中一個指令：

- `assessment` - 可用於升級時。支援可報告所有已修改物件及所有已安裝版本 Identity Manager 的子指令。請參閱「Identity Manager Upgrade」一書以取得詳細資訊。
- `config` - 啓動業務程序編輯器。
- `console` - 啓動 Identity Manager 主控台。
- `genReports` - 產生一組隨機資料，用以說明 Identity Manager 報告功能。
- `import` - 匯入 Identity Manager 物件。指定 `-s` 選項表示嚴格模式。啓用嚴格模式時，匯入期間的參照檢查就會更嚴格。
- `js` - 呼叫 JavaScript 程式。
- `javascript` - 與 js 相同。
- `msgtool` - 依據 `WPMessages.properties` 產生自訂訊息目錄。您可運用此目錄自訂文字或語言的變更。
- `script` - 執行 JavaScript 或 BeanShell。
- `setRepo` - 設定 Identity Manager 索引儲存庫。
- `setup` - 啓動 Identity Manager 設定程序，讓您可以設定授權碼、定義 Identity Manager 索引儲存庫，以及匯入配置檔。
- `spml` - 啓動 SPML 瀏覽器。
- `syslog [options]` - 從系統記錄中擷取記錄。請參閱第 595 頁的「syslog 指令」以取得詳細資訊。
- `waveset` - `console` 指令的別名。請參閱上文的 `console`。
- `xmlparse` - 驗證 Identity Manager 物件的 XML。
- `xpress [options]` *Filename* - 計算表示式。有效的選項爲 `-trace` (允許追蹤輸出)。

範例

- `lh com.waveset.session.WavesetConsole`
- `lh console`
- `lh console u $user p` *`PathtoPassword`*`.txt`
- `lh setup -U` *`Administrator`* `-P` *`PathtoPassword`*`.txt`
- `lh setRepo c -A` *`Administrator`* `-C` *`PathtoPassword`*`.txt`
- `lh setRepo t` *`LocalFiles`* `f $WSHOME`

syslog 指令

用法

```
syslog [options]
```

選項

使用下列*選項*可包含或排除資訊：

表 A-1 Syslog 指令選項

選項	描述
-d 數字	顯示前數字天的記錄 (預設值=1)。
-E	僅顯示錯誤嚴重性層級或更高層級的記錄。
-F	僅顯示嚴重嚴重性層級的記錄。
-i *LogID*	僅顯示具有指定 syslog ID 的記錄。 Syslog ID 會出現在某些錯誤訊息中，並會參照特定的系統記錄檔項目。
-W	僅顯示警告嚴重性層級或更高層級的記錄 (預設)。
-X	包括報告的錯誤原因 (如果有)。

稽核記錄資料庫模式

此附錄提供有關受支援資料庫類型之稽核資料模式值，以及稽核記錄資料庫對映的資訊。

Oracle

表 B-1 列出了 Oracle 資料庫類型的資料模式值：

表 B-1 Oracle 資料庫類型的資料模式值 (第 1 頁，共 2 頁)

資料庫欄	值
id	VARCHAR(50) NOT NULL
name	VARCHAR(128) NOT NULL
repomod	TIMESTAMP
resourceName	VARCHAR(128)
accountName	VARCHAR(50)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDateTime	CHAR(21)
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)
message	VARCHAR(255) 或 CLOB (請參閱表格結尾的備註[1])。
acctAttrChanges	VARCHAR(4000) 或 CLOB
acctAttr01label	VARCHAR(50)
acctAttr01value	VARCHAR(128)
acctAttr02label	VARCHAR(50)
acctAttr02value	VARCHAR(128)
acctAttr03label	VARCHAR(50)
acctAttr03value	VARCHAR(128)
acctAttr04label	VARCHAR(50)
acctAttr04value	VARCHAR(128)

表 B-1 Oracle 資料庫類型的資料模式值 (第 2 頁，共 2 頁)

資料庫欄	值
acctAttr05label	VARCHAR(50)
acctAttr05value	VARCHAR(128)
parm01label	VARCHAR(50)
parm01value	VARCHAR(128) 或 CLOB (請參閱表格結尾的備註[1])。
parm02label	VARCHAR(50)
parm02value	VARCHAR(128) 或 CLOB (請參閱表格結尾的備註[1])。
parm03label	VARCHAR(50)
parm03value	VARCHAR(128) 或 CLOB (請參閱表格結尾的備註[1])。
parm04label	VARCHAR(50)
parm04value	VARCHAR(128) 或 CLOB (請參閱表格結尾的備註[1])。
parm05label	VARCHAR(50)
parm05value	VARCHAR(128) 或 CLOB (請參閱表格結尾的備註[1])。
sequence	CHAR(19)
xmlSize	NUMBER(19,0)
xml	BLOB

[1]您可以配置這些欄的欄長度限制。預設資料類型是 VARCHAR，而預設大小限制則備註在括弧中。請參閱第 367 頁的「稽核記錄配置」，以取得有關如何調整大小限制的詳細資訊。

DB2

表 B-2 列出了 DB2 資料庫類型的資料模式值：

表 B-2 DB2 資料庫類型的資料模式值 (第 1 頁，共 2 頁)

資料庫欄	值
id	VARCHAR(50) NOT NULL
name	VARCHAR(128) NOT NULL
repomod	TIMESTAMP
resourceName	VARCHAR(128)
accountName	VARCHAR(50)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDateTime	CHAR(21)
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)
message	VARCHAR(255) 或 CLOB (請參閱表格結尾的備註[1])。
acctAttrChanges	CLOB(16M)
acctAttr01label	VARCHAR(50)
acctAttr01value	VARCHAR(128)
acctAttr02label	VARCHAR(50)
acctAttr02value	VARCHAR(128)
acctAttr03label	VARCHAR(50)
acctAttr03value	VARCHAR(128)
acctAttr04label	VARCHAR(50)
acctAttr04value	VARCHAR(128)

表 B-2 DB2 資料庫類型的資料模式值 (第 2 頁，共 2 頁)

資料庫欄	值
acctAttr05label	VARCHAR(50)
acctAttr05value	VARCHAR(128)
parm01label	VARCHAR(50)
parm01value	VARCHAR(128) 或 CLOB (請參閱表格結尾的備註[1])。
parm02label	VARCHAR(50)
parm02value	VARCHAR(128) 或 CLOB (請參閱表格結尾的備註[1])。
parm03label	VARCHAR(50)
parm03value	VARCHAR(128) 或 CLOB (請參閱表格結尾的備註[1])。
parm04label	VARCHAR(50)
parm04value	VARCHAR(128) 或 CLOB (請參閱表格結尾的備註[1])。
parm05label	VARCHAR(50)
parm05value	VARCHAR(128) 或 CLOB (請參閱表格結尾的備註[1])。
sequence	CHAR(19)
xmlSize	DECIMAL(19,0)
xml	CLOB(16M)

[1] 您可以配置這些欄的欄長度限制。預設資料類型是 VARCHAR，而預設大小限制則備註在括弧中。請參閱第 367 頁的「稽核記錄配置」，以取得有關如何調整大小限制的詳細資訊。

MySQL

表 B-3 列出了 MySQL 資料庫類型的資料模式值：

表 B-3　MySQL 資料庫類型的資料模式值 (第 1 頁，共 2 頁)

資料庫欄	值
id	VARCHAR(50) BINARY NOT NULL
name	VARCHAR(128) BINARY NOT NULL
repomod	TIMESTAMP
resourceName	VARCHAR(128)
accountName	VARCHAR(255)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDateTime	CHAR(21)
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)
message	VARCHAR(255) 或 CLOB (請參閱表格結尾的備註[1])。
acctAttrChanges	TEXT
acctAttr01label	VARCHAR(50)
acctAttr01value	VARCHAR(128)
acctAttr02label	VARCHAR(50)
acctAttr02value	VARCHAR(128)
acctAttr03label	VARCHAR(50)
acctAttr03value	VARCHAR(128)
acctAttr04label	VARCHAR(50)
acctAttr04value	VARCHAR(128)

表 B-3 MySQL 資料庫類型的資料模式值 (第 2 頁，共 2 頁)

資料庫欄	值
acctAttr05label	VARCHAR(50)
acctAttr05value	VARCHAR(128)
parm01label	VARCHAR(50)
parm01value	VARCHAR(128) 或 CLOB (請參閱表格結尾的備註[1])。
parm02label	VARCHAR(50)
parm02value	VARCHAR(128) 或 CLOB (請參閱表格結尾的備註[1])。
parm03label	VARCHAR(50)
parm03value	VARCHAR(128) 或 CLOB (請參閱表格結尾的備註[1])。
parm04label	VARCHAR(50)
parm04value	VARCHAR(128) 或 CLOB (請參閱表格結尾的備註[1])。
parm05label	VARCHAR(50)
parm05value	VARCHAR(128) 或 CLOB (請參閱表格結尾的備註[1])。
sequence	CHAR(19)
xmlSize	BIGINT
xml	MEDIUMTEXT

[1] 您可以配置這些欄的欄長度限制。預設資料類型是 VARCHAR，而預設大小限制則備註在括弧中。請參閱第 367 頁的「稽核記錄配置」，以取得有關如何調整大小限制的詳細資訊。

SQL Server

表 B-4 列出 SQL Server 資料庫類型的資料模式值：

表 B-4 SQL Server 資料庫類型的資料模式值 (第 1 頁，共 2 頁)

資料庫欄	值
id	NVARCHAR(50) NOT NULL
name	NVARCHAR(128) NOT NULL
repomod	DATETIME NOT NULL CURRENT_TIMESTAMP
resourceName	NVARCHAR(128)
accountName	NVARCHAR(255)
objectType	NCHAR(2)
objectName	NVARCHAR(128)
action	NCHAR(2)
actionDateTime	NCHAR(21)
actionStatus	NCHAR(1)
interface	NVARCHAR(50)
server	NVARCHAR(128)
subject	NVARCHAR(128)
reason	NCHAR(2)
message	NVARCHAR(255) 或 CLOB (請參閱表格結尾的備註[1])。
acctAttrChanges	NTEXT
acctAttr01label	NVARCHAR(50)
acctAttr01value	NVARCHAR(128)
acctAttr02label	NVARCHAR(50)
acctAttr02value	NVARCHAR(128)
acctAttr03label	NVARCHAR(50)
acctAttr03value	NVARCHAR(128)
acctAttr04label	NVARCHAR(50)

表 B-4 SQL Server 資料庫類型的資料模式值 (第 2 頁，共 2 頁)

資料庫欄	值
acctAttr04value	NVARCHAR(128)
acctAttr05label	NVARCHAR(50)
acctAttr05value	NVARCHAR(128)
parm01label	NVARCHAR(50)
parm01value	NVARCHAR(128) 或 CLOB (請參閱表格結尾的備註[1])。
parm02label	NVARCHAR(50)
parm02value	NVARCHAR(128) 或 CLOB (請參閱表格結尾的備註[1])。
parm03label	NVARCHAR(50)
parm03value	NVARCHAR(128) 或 CLOB (請參閱表格結尾的備註[1])。
parm04label	NVARCHAR(50)
parm04value	NVARCHAR(128) 或 CLOB (請參閱表格結尾的備註[1])。
parm05label	NVARCHAR(50)
parm05value	NVARCHAR(128) 或 CLOB (請參閱表格結尾的備註[1])。
sequence	NTEXT
xmlSize	NUMERIC(19,0)
xml	NTEXT

[1]您可以配置這些欄的欄長度限制。預設資料類型是 VARCHAR，而預設大小限制則備註在括弧中。請參閱第 367 頁的「稽核記錄配置」，以取得有關如何調整大小限制的詳細資訊。

稽核記錄資料庫對映

表 B-5 說明已儲存稽核記錄資料庫鍵值以及其對映的在稽核報告輸出中的顯示字串。Identity Manager 可將用做常數的項目儲存爲短的資料庫鍵值，以節省儲存庫中的空間。產品介面不會顯示這些對映。僅當檢查稽核報告結果的傾印輸出時，才可看到這些對映。

表 B-6 (第 608 頁) 包含可稽核的動作資料庫鍵值、表 B-7 (第 611 頁) 包含動作狀態鍵值，而表 B-8 (第 611 頁) 包含在資料庫中儲存爲鍵值的原因代碼。

表 B-5 物件鍵值類型資料庫鍵值

類型名稱	英文	資料庫關聯字
AccessReview	AccessReview	AV
AccessReviewWorkflow*	Access Review Workflow	AW
AccessScan	AccessScan	AS
Account	Account	AN
AdminGroup	Capability	AG
Administrator	Administrator	AD
AdminRole	Admin Role	AR
Application	Resource Group	AP
AttributeDefinition	AttributeDefinition	AF
AttrParse	AttrParse	AT
AuditConfig	AuditConfig	AC
AuditPolicy	AuditPolicy	CP
BeanPod	Bean Pod	BP
ComplianceViolation	ComplianceViolation	CV
Configuration	Configuration	CN
DataExporter	Data Exporter	DE
Discovery	Discovery	DS
Email*	Email	EM
EmailTemplate	EmailTemplate	ET
EncryptionKey	EncryptionKey	KY

表 B-5　物件鍵值類型資料庫鍵值

類型名稱	英文	資料庫關聯字
Event	Event	EV
Extract	Extract	ER
ExtractTask	ExtractTask	EX
IDMXUser*	Directory User	UX
LighthouseAccount*	Identity System Account	LA
LoadConfig	LoadConfig	LD
LoadTask	LoadTask	LT
Log	Log	LG
LoginApp	LoginApp	LP
LoginConfig	LoginConfig	LC
LoginModGroup	LoginModGroup	LF
MetaView	Meta View	MV
ObjectGroup	Organization	OG
Policy	Policy	PO
ProvisioningTask	ProvisioningTask	PT
RemediationWorkflow*	Remediation Workflow	RW
RemedyConfig	RemedyConfig	RC
Resource	Resource	RS
ResourceAccount*	Resource Account	RA
ResourceAction	ResourceAction	RN
ResourceForm	ResourceForm	RF
ResourceObject	ResourceObject	RE
RiskReportTask	RiskReportTask	RR
Role	Role	RL
Rule	Rule	RU
SnapShot	SnapShot	SS

表 B-5 物件鍵值類型資料庫鍵值

類型名稱	英文	資料庫關聯字
SysLog	SysLog	SL
System	System	SY
TaskDefinition	TaskDefinition	TD
TaskInstance	TaskInstance	TI
TaskResult	TaskResult	TR
TaskResultPage	ResultPage	TP
TaskSchedule	TaskSchedule	TS
TaskTemplate	TaskTemplate	TT
TestNotification*	Test Notification	TN
User	User	US
UserEntitlement	UserEntitlement	UE
UserForm	UserForm	UF
WorkflowCase*	Workflow Case	WC
WorkItem	WorkItem	WI
XmlData	XmlData	XD

* 延伸類型

表 B-6 動作資料庫鍵值

動作名稱	英文	資料庫關聯字
Allowed*	Allowed	AL
Approve	Approve	AP
Assign Audit Policies	Assign Audit Policies	AA
Assign Capabilities	Assign Capabilities	AC
AttestorApproved*	Attestor Approved	TA
AttestorRejected*	Attestor Rejected	AR
AttestorRemediate*	Remediation Requested	AF

表 B-6　動作資料庫鍵值

動作名稱	英文	資料庫關聯字
AttestorRescan*	Rescan Requested	AN
Bulk Change Password	Bulk Change Password	BW
Bulk Create	Bulk Create	BC
Bulk Delete	Bulk Delete	BD
Bulk Deprovision	Bulk Deprovision	BP
Bulk Disable	Bulk Disable	BF
Bulk Enable	Bulk Enable	BE
Bulk Modify	Bulk Modify	BM
Bulk Reset Password	Bulk Reset Password	BR
Bulk Unassign	Bulk Unassign	BU
Bulk Unlink	Bulk Unlink	BL
Bypass Verify	Bypass Verify	BV
CancelReconcile*	Cancel Reconcile	CR
challengeResponse*	Challenge Response	CD
Change Password	Change Password	CP
Connect	Connect	CN
Control Active Sync	Control Active Sync	CA
Create	Create	CT
CredentialsExpired*	Credentials Expired	CE
Debug	Debug	DB
Delegate	Delegate	DG
Delete	Delete	DL
Deprovision	Deprovision	DP
Disable	Disable	DS
Disconnect	Disconnect	DC
Enable	Enable	EN
End Activity	End Activity	EA

表 B-6 動作資料庫鍵值

動作名稱	英文	資料庫關聯字
End Process	End Process	PE
End Workflow	End Workflow	EW
Execute	Execute	LN
Expired*	Expired	EX
Export	Export	EP
Fixed*	Fixed	FX
Import	Import	IM
List	List	LI
Lock	Lock	LK
Login	Login	LG
Logout*	Logout	LO
Mitigated*	Mitigated	VM
Modify	Modify	MO
Modify Active Sync	Modify Active Sync	MA
NativeChange*	Native Change	NC
Notify*	Notify	NO
PostOperation*	Post-Operation Callout	PT
PreOperation*	Pre-Operation Callout	PP
Prioritize*	Prioritize	PR
Provision	Provision	PV
Recurring*	Recurring	RC
Reject	Reject	RJ
Remediated*	Remediated	VR
Rename	Rename	RE
RequestReconcile*	Request Reconcile	RR
ResetPassword	ResetPassword	RP
Run Debugger	Run Debugger	RD

表 B-6 動作資料庫鍵值

動作名稱	英文	資料庫關聯字
ScanBegin*	Scan Begin	SB
ScanEnd*	Scan End	SE
StartActivity*	Start Activity	SA
StartProcess*	Start Process	SP
StartWorkflow*	Start Workflow	SW
Terminate*	Terminate	TR
Unassign	Unassign	UA
Unlink	Unlink	UN
Unlock	Unlock	UL
updateAuthenticationAnswers*	Update Authentication Answers	AQ
usernameRecovery*	Username Recovery	UR
View	View	VW
View Only	View Only	VO

* 延伸動作

表 B-7 動作狀態資料庫鍵值

結果	資料庫關聯字
Success	S
Failure	F

表 B-8 儲存爲鍵值的原因 (第 1 頁，共 2 頁)

原因名稱	英文	資料庫關聯字
PolicyViolation	Violation of policy {0}: {1}	PV
InvalidCredentials	Invalid Credentials	CR
InsufficientPrivileges	Insufficient Privileges	IP
DatabaseAccessFailed	Database Access Failed	DA

表 B-8 儲存爲鍵值的原因 (第 2 頁，共 2 頁)

原因名稱	英文	資料庫關聯字
AccountDisabled	Account Disabled	DI

使用者介面快速參照

表 C-1 是經常執行之 Identity Manager 作業的快速參照。它會顯示您開始每項作業的主要 Identity Manager 介面位置，以及可以用以執行相同作業的替代位置或方法 (如果適用)。

表 C-1 Identity Manager 介面作業參照 (第 1 頁，共 5 頁)

若要執行此動作：	移至：	或：
管理 Identity Manager 使用者		
建立和編輯使用者	**[帳號]** 標籤，**[列出帳號]** 選項	**[帳號]** 標籤，**[尋找使用者]** 選項 ([使用者帳號搜尋結果] 頁面)
核准使用者帳號建立	**[工作項目]** 標籤，**[核准]** 子標籤	
設定使用者驗證 (策略)	**[安全性]** 標籤，**[策略]** 選項	
變更使用者密碼	**[密碼]** 標籤，**[變更使用者密碼]** 選項	**[帳號]** 標籤，**[列出帳號]** 選項 **[帳號]** 標籤，**[尋找使用者]** 選項 ([使用者帳號搜尋結果] 頁面) Identity Manager 使用者介面
重設使用者密碼	**[密碼]** 標籤，**[重設使用者密碼]** 選項	**[帳號]** 標籤，**[列出帳號]** 選項 **[帳號]** 標籤，**[尋找使用者]** 選項 ([使用者帳號搜尋結果] 頁面)
尋找使用者	**[帳號]** 標籤，**[尋找使用者]** 選項	**[密碼]** 標籤，**[變更使用者密碼]** 選項
啓用或停用使用者	**[帳號]** 標籤，**[列出帳號]** 選項	**[帳號]** 標籤，**[尋找使用者]** 選項 ([使用者帳號搜尋結果] 頁面)

表 C-1 Identity Manager 介面作業參照 (第 2 頁，共 5 頁)

若要執行此動作：	移至：	或：
解除鎖定使用者	**[帳號]** 標籤，**[列出帳號]** 選項	**[帳號]** 標籤，**[尋找使用者]** 選項 ([使用者帳號搜尋結果] 頁面)
管理 Identity Manager 管理員		
設定委託 (透過組織)	**[帳號]** 標籤，**[列出帳號]** 選項，[建立使用者] 頁面	
指定權能	**[帳號]** 標籤，**[列出帳號]** 選項，[建立使用者] 或 [編輯使用者] 頁面 **[安全性]** 子標籤	
指定權能 (透過管理員角色)	**[帳號]** 標籤，**[列出帳號]** 選項，[建立使用者] 或 [編輯使用者] 頁面 **[安全性]** 子標籤	
設定核准人 (以驗證帳號建立)	**[帳號]** 標籤，**[列出帳號]** 選項，[建立組織] 頁面 **[角色]** 標籤，[建立角色] 頁面	
配置 Identity Manager		
建立與管理資源 (資源精靈)	**[資源]** 標籤	
管理資源群組	**[資源]** 標籤，**[列出資源群組]** 選項	
建立與管理角色	**[角色]** 標籤	
尋找角色	**[角色]** 標籤，**[尋找角色]** 選項	
編輯權能	**[安全性]** 標籤，**[權能]** 選項	
建立和編輯管理員角色	**[安全性]** 標籤，**[管理員角色]** 選項，[建立/編輯管理員角色] 頁面	
設定電子郵件範本	**[配置]** 標籤，**[電子郵件範本]** 選項	

表 C-1 Identity Manager 介面作業參照 (第 3 頁，共 5 頁)

若要執行此動作：	移至：	或：
設定密碼、帳號與命名策略；指定策略至組織	**[安全性]** 標籤，**[策略]** 選項	
載入與同步化帳號與資料		
匯入資料檔案 (例如 XML 格式表單)	**[配置]** 標籤，**[匯入交換檔案]** 選項	
載入資源帳號	**[帳號]** 標籤，**[從資源載入]** 選項	
從檔案載入帳號	**[帳號]** 標籤，**[從檔案載入]** 選項	
將 Identity Manager 使用者與資源帳號比較	**[資源]** 標籤，**[調解資源]** 選項	
稽核和管理規範遵循		
停用或啓用稽核	**[配置]** 標籤，**[稽核]** 選項	
設定要擷取的稽核事件	**[配置]** 標籤，**[稽核]** 選項	
定義稽核策略 (建立、編輯、刪除)	**[規範遵循]** 標籤，**[管理策略]** 選項	
指定稽核策略	**[帳號]** 標籤，**[規範遵循]** 選項	
爲稽核策略定義修正者並指定修正工作流程	**[規範遵循]** 標籤，**[管理策略]** 子標籤	
回應策略違規修正請求	**[我的工作項目]** 標籤，**[修正]** 選項	
緩解策略違規	**[工作項目]** 標籤，**[修正]** 子標籤	
檢閱修正的策略違規	**[工作項目]** 標籤，**[修正]** 子標籤	
產生稽核策略報告	**[報告]** 標籤，**[執行報告]** 子標籤	
對一個或多個使用者或組織執行稽核掃描	**[帳號]** 標籤，從 [使用者動作] 或 [組織動作] 清單中選取 **[掃描]**	

表 C-1 Identity Manager 介面作業參照 (第 4 頁，共 5 頁)

若要執行此動作：	移至：	或：
設定定期存取檢閱	**[規範遵循]** 標籤，**[管理存取掃描]** 選項	
監視定期存取檢閱	**[規範遵循]** 標籤，**[存取檢閱]** 選項	
檢視稽核報告	**[報告]** 標籤，**[稽核員報告]** 類型選項	
編輯管理員稽核權能	**[安全性]** 標籤，**[權能]** 子標籤	
設定稽核通知的電子郵件範本	**[配置]** 標籤，**[電子郵件範本]** 子標籤	
匯入資料檔/規則 (例如 XML 格式表單)	**[配置]** 標籤，**[匯入交換檔案]** 子標籤	
定義存取檢閱掃描	**[規範遵循]** 標籤，**[管理掃描]** 子標籤	
執行存取檢閱	**[規範遵循]** 標籤，**[存取檢視]** 子標籤	
終止存取檢閱	**[規範遵循]** 標籤，**[存取檢視]** 子標籤	
排定存取檢閱	**[伺服器作業]** 標籤，**[管理排程]** 子標籤	
設定定期存取檢閱	**[規範遵循]** 標籤，**[管理存取掃描]** 子標籤	
監視存取檢閱狀態	**[規範遵循]** 標籤，**[存取檢視]** 子標籤	
配置驗證者	**[規範遵循]** 標籤，**[管理存取掃描]** 子標籤	
執行驗證者責任 (檢閱與認證使用者軟體權利文件)	**[工作項目]** 標籤，**[我的工作項目]** 標籤，**[驗證]** 子標籤	

表 C-1　Identity Manager 介面作業參照 (第 5 頁，共 5 頁)

若要執行此動作：	移至：	或：
風險分析和報告		
執行與管理報告	**[報告]** 標籤，**[執行報告]** 選項，以建立、執行和下載報告；**[檢視報告]**，以檢視報告結果。	
定義與執行風險分析報告	**[報告]** 標籤，**[風險分析]** 選項	
檢視圖形報告	**[報告]** 標籤，**[檢視面板]** 選項	
檢閱責任分離報告	**[報告]** 標籤，**[執行報告]** 子標籤	
管理 Identity Manager 作業		
執行已定義的作業 (或程序)	**[伺服器作業]** 標籤，**[執行作業]** 選項	
排程作業	**[伺服器作業]** 標籤，**[管理排程]** 選項	
檢視作業結果	**[伺服器作業]** 標籤，**[尋找作業]** 或 **[全部作業]** 選項	
暫停或終止作業	**[伺服器作業]** 標籤，**[全部作業]** 選項	
管理服務提供者使用者		
管理「服務提供者」使用者	**[帳號]** 標籤，**[管理「服務提供者」使用者]** 選項	
管理服務提供者作業事件	**[伺服器作業]** 標籤，**[服務提供者作業事件]** 選項	
配置服務提供者功能	**[服務提供者]** 標籤，**[編輯主配置]** 選項	
配置作業事件預設	**[服務提供者]** 標籤，**[編輯作業事件配置]** 選項	
建立或編輯服務提供者策略	**[安全性]** 標籤，**[策略]** 選項	

附錄 D

權能定義

此附錄分爲以下各節：

- 作業型權能定義
- 功能性權能定義

如需有關權能的一般資訊，請參閱第 215 頁的「瞭解與管理權能」。

備註 所有權能都允許使用者或管理員存取 **[密碼]** > **[變更我的密碼]** 和 **[變更我的答案]** 標籤。

作業型權能定義

本節說明每個可以指定給使用者的作業型權能。也會列出能以每個權能存取的標籤和子標籤。權能會按名稱的字母順序列出。

表 D-1 Identity Manager 作業型權能定義 (第 1 頁，共 13 頁)

權能	允許管理員 / 使用者：	可以存取這些標籤與子標籤：
存取檢閱詳細資訊報告管理員	建立、編輯、刪除和執行存取檢閱詳細資訊報告	**[報告] > [執行報告]** 標籤，**[檢視報告]** 標籤 - 僅 [存取檢視詳細資訊報告] **[報告] > [檢視面板]**
存取檢閱摘要報告管理員	建立、編輯、刪除和執行存取檢閱摘要報告	**[報告]** - 僅 [存取檢視摘要報告] **[報告] > [檢視面板]**
帳號管理員	對使用者執行所有作業，包括指定權能。不包括批次處理作業。	**[帳號]** - **[列出帳號]**、**[尋找使用者]**、**[擷取至檔案]**、**[從檔案載入]**、**[從資源載入]** 標籤 **[密碼]** - 所有子標籤 **[工作項目] - [核准]** 子標籤 **[作業]** - 所有子標籤
管理員報告管理員	建立、編輯、刪除和執行管理員報告。	**[報告]** - **[管理報告]**，**[執行報告]** 子標籤 (僅 [管理員報告])
管理員角色管理員	建立、編輯和刪除管理員角色。	**[安全性] - [管理員角色]** 子標籤
應用程式管理員	建立、編輯和刪除應用程式角色。	**[作業] - [尋找作業]**、**[全部作業]**、**[執行作業]** 子標籤 (同步化角色) **[角色]** - 所有子標籤
核准人管理員	核准或拒絕由其他使用者發起的請求。	**僅 [預設值]**
資產管理員	建立、編輯和刪除資產角色。	**[作業] - [尋找作業]**、**[全部作業]**、**[執行作業]** 子標籤 (同步化角色) **[角色]** - 所有子標籤
指定稽核策略	爲使用者帳號和組織指定稽核策略。	**[帳號]** - [使用者動作] 清單中的 **[編輯使用者稽核策略]**。 **[帳號] - [組織動作] 清單中的 [編輯組織稽核策略]**。
指定組織稽核策略	僅將稽核策略指定給組織。	**[帳號]** - [組織動作] 清單中的 **[編輯組織稽核策略]**；**[列出帳號]** 標籤

表 D-1 Identity Manager 作業型權能定義 (第 2 頁，共 13 頁)

權能	**允許管理員 / 使用者：**	**可以存取這些標籤與子標籤：**
指定使用者稽核策略	僅將稽核策略指定給使用者。	**[帳號]** - [使用者動作] 清單中的 **[編輯使用者稽核策略]**；**[列出帳號]**；**[尋找使用者]** 標籤
指定使用者權能	變更使用者的權能指定 (指定和取消指定)。	**[帳號]** - **[列出帳號]** (僅 [編輯])，**[尋找使用者]** 子標籤。 必須以另一項使用者管理員權能指定 (例如，「建立使用者」或「啓用使用者」)。
稽核策略管理員	建立、修改和刪除稽核策略。	**[規範遵循] - [管理策略]**
稽核策略掃描報告管理員	建立、修改、刪除和執行「稽核策略掃描報告」。	**[報告]** - 僅 [稽核策略掃描報告]
稽核報告管理員	建立、修改、刪除和執行稽核報告。	**[報告]** - 僅 [稽核報告]
已稽核的屬性報告管理員	建立、修改、刪除和執行「已稽核的屬性報告」。	**[報告]** - 僅 [已稽核的屬性報告]
稽核記錄報告管理員	建立、修改、刪除和執行「稽核記錄報告」。	**[報告]** - 僅 [稽核記錄報告]
稽核員存取掃描管理員	建立、編輯和刪除定期存取檢閱掃描	**[規範遵循] - [管理存取掃描]**
Auditor 管理員	設定、管理和監視稽核策略、稽核掃描和使用者規範遵循。	**[規範遵循] -** 所有子標籤 **[報告]** - [執行報告]、[檢視報告] 和 [管理稽核員報告] **[帳號]** - [編輯使用者稽核策略] 和 [編輯組織稽核策略] 動作。
稽核員驗證者	啓用組織安全性後，需要此項權能以驗證其他使用者的驗證作業。	**僅 [預設值]**
稽核員定期存取檢閱管理員	管理定期存取檢閱 (PAR)、管理存取掃描、管理驗證、管理 PAR 報告。	**[規範遵循] - [管理存取掃描]**、**[存取檢視]** 子標籤
Auditor 修正者	修正、緩解和轉寄稽核策略違規。	**[修正]** - 所有子標籤
Auditor 報告管理員	建立、修改、刪除和執行所有 Auditor 報告。	**[報告]** - 對 Auditor 報告的所有動作
Auditor 檢視使用者	檢視與使用者關聯的規範遵循資訊。	**[帳號]** - **[列出帳號]**、**[尋找使用者]** 標籤

表 D-1 Identity Manager 作業型權能定義 (第 3 頁，共 13 頁)

權能	允許管理員 / 使用者：	可以存取這些標籤與子標籤：
稽核策略違規歷程記錄管理員	建立、修改、刪除和執行「稽核策略違規歷程記錄」報告。	**[報告]** - 僅 [稽核策略違規歷程記錄報告]
批次帳號管理員	對使用者執行一般和批次作業，包括指定權能。	**[帳號]** - 所有子標籤 **[密碼]** - 所有子標籤 **[核准]** - 所有子標籤 **[作業]** - 所有子標籤
批次變更帳號管理員	對現有使用者執行一般與批次處理作業，包括指定權能，但刪除作業除外。	**[帳號]** - **[列出帳號]**、**[尋找使用者]**、**[啓動批次處理動作]** 子標籤。無法建立或刪除使用者。 **[密碼]** - 所有子標籤 **[核准]** - 所有子標籤 **[作業]** - 所有子標籤
批次變更資源密碼管理員	變更所指定資源上指定之資源連線帳號的密碼。	**[資源]** - **[啓動批次處理動作]** 子標籤
批次變更使用者帳號管理員	對現有使用者執行一般和批次作業，但刪除作業除外。	**[帳號]** - **[列出帳號]**、**[尋找使用者]**、**[啓動批次處理動作]** 子標籤。無法建立、刪除或指定給使用者的權能。 **[密碼]** - 所有子標籤 **[作業]** - 所有子標籤
批次建立使用者	指定資源和發起使用者建立請求 (對於個別使用者並使用批次作業)。	**[帳號]** - **[列出帳號]** (僅 [建立])、**[尋找使用者]**、**[啓動批次處理動作]** 子標籤 **[作業]** - 所有子標籤
批次刪除使用者	刪除 Identity Manager 使用者帳號；取消佈建、取消指定與取消連結資源帳號 (對於個別使用者並使用批次作業)。	**[帳號]** - **[列出帳號]** (僅 [建立])、**[尋找使用者]**、**[啓動批次處理動作]** 子標籤 **[作業]** - 所有子標籤
批次刪除 IDM 使用者	刪除現有 Identity Manager 使用者帳號 (對於個別使用者並使用批次作業)。	**[帳號]** - **[列出帳號]** (僅 [刪除])、**[尋找使用者]**、**[啓動批次處理動作]** 子標籤 **[作業]** - 所有子標籤

表 D-1 Identity Manager 作業型權能定義 (第 4 頁，共 13 頁)

權能	允許管理員 / 使用者：	可以存取這些標籤與子標籤：
批次取消佈建使用者	刪除現有資源帳號並取消其連結 (對於個別使用者並使用批次作業)。	**[帳號]** - **[列出帳號]** (僅 [取消佈建])、**[尋找使用者]**、**[啓動批次處理動作]** 子標籤
		[作業] - 所有子標籤
批次停用使用者	停用現有使用者和資源帳號 (對於個別使用者並使用批次作業)。	**[帳號]** - **[列出帳號]** (僅 [停用])、**[尋找使用者]**、**[啓動批次處理動作]** 子標籤
		[作業] - 所有子標籤
批次啓用使用者	啓用現有使用者和資源帳號 (對於個別使用者並使用批次作業)。	**[帳號]** - **[列出帳號]** (僅 [啓用])、**[尋找使用者]**、**[啓動批次處理動作]** 子標籤
		[作業] - 所有子標籤
批次重設資源密碼管理員	重設所指定資源上指定之資源連線帳號的密碼。	**[資源]** - **[啓動批次處理動作]** 子標籤
批次取消指定使用者	取消指定現有資源帳號並取消現有資源帳號連結 (對於個別使用者並使用批次作業)。	**[帳號]** - **[列出帳號]** (僅 [取消指定])、**[尋找使用者]**、**[啓動批次處理動作]** 子標籤
		[作業] - 所有子標籤
批次取消連結使用者	取消現有資源帳號連結 (對於個別使用者並使用批次作業)。	**[帳號]** - **[列出帳號]** (僅 [解除連結])、**[尋找使用者]**、**[啓動批次處理動作]** 子標籤
		[作業] - 所有子標籤
批次更新使用者	更新現有使用者和資源帳號 (對於個別使用者並使用批次作業)。	**[帳號]** - **[列出帳號]** (僅 [更新])、**[尋找使用者]**、**[啓動批次處理動作]** 子標籤
		[作業] - 所有子標籤
批次使用者帳號管理員	對使用者執行所有一般和批次作業。	**[帳號]** - 所有子標籤
		[密碼] - 所有子標籤
		[作業] - 所有子標籤
商務角色管理員	建立、編輯和刪除商務角色。	**[作業]** - **[尋找作業]**、**[全部作業]**、**[執行作業]** 子標籤 (同步化角色)
		[角色] - 所有子標籤
權能管理員	建立、修改和刪除權能。	**[配置]** - **[權能]** 子標籤

表 D-1 Identity Manager 作業型權能定義 (第 5 頁，共 13 頁)

權能	允許管理員 / 使用者：	可以存取這些標籤與子標籤：
變更帳號管理員	對現有使用者執行所有作業，包括指定權能，但刪除作業除外。不包括批次作業	**[帳號]** - 所有子標籤。無法刪除使用者。 **[密碼]** - 所有子標籤 **[核准]** - 所有子標籤 **[作業]** - 所有子標籤 **[報告]** - 在範圍內建立管理員和使用者報告、執行和編輯管理員報告，以及執行稽核記錄報告。無法在範圍外的組織上執行管理員與使用者報告。
變更 Active Sync 資源管理員	變更 Active Sync 資源參數。	**[作業] - [尋找作業]**、**[全部作業]**、**[執行作業]** 子標籤 **[資源]** - 對於 Active Sync 資源：[編輯] 動作功能表，[編輯 Active Sync 參數]
變更密碼管理員	變更使用者和資源帳號密碼。	**[帳號] - [列出帳號]**、**[尋找使用者]** 子標籤 (僅限 [變更密碼]) **[密碼]** - 所有子標籤 **[作業]** - 所有子標籤。僅 [匯出密碼掃描] 作業 (從 **[執行作業]** 子標籤)
變更密碼管理員 (需要驗證)	在成功驗證使用者身份認證問題答案後，變更使用者和資源帳號密碼。	**[帳號] - [列出帳號]**、**[尋找使用者]** 子標籤 (僅限 [變更密碼]；必須先驗證才能執行動作) **[密碼]** - 所有子標籤 **[作業]** - 所有子標籤。僅 [匯出密碼掃描] 作業 (從 **[執行作業]** 子標籤)
變更資源密碼管理員	變更資源管理員帳號密碼。	**[作業] -** 所有子標籤 **[資源] - [列出資源]** 子標籤僅變更資源密碼 (從 [動作] 功能表中的 **[管理連線] > [變更密碼]**)

表 D-1 Identity Manager 作業型權能定義 (第 6 頁，共 13 頁)

權能	允許管理員 / 使用者：	可以存取這些標籤與子標籤：
變更使用者帳號管理員	對現有使用者執行所有作業，但刪除作業除外。不包括批次作業	**[帳號] - [列出帳號]**、**[尋找使用者]** 子標籤。無法建立、刪除或指定給使用者的權能。 **[密碼]** - 所有子標籤 **[作業]** - 所有子標籤
配置稽核	配置系統中稽核的事件和配置群組。	**[配置] - [稽核事件]** 子標籤
配置憑證	配置可信任的憑證和 CRL。	**[安全性] - [憑證]** 子標籤
控制 Active Sync 資源管理員	控制 Active Sync 資源狀態 (如開始、停止和重新整理)	**[作業] - [尋找作業]**、**[全部作業]**、**[執行作業]** **[資源]** - 對於 Active Sync 資源：Active Sync 動作功能表 (所有選擇)
建立使用者	指定資源和發起使用者建立請求。不包括批次作業	**[帳號] - [列出帳號]** (僅 [建立])、**[尋找使用者]** 子標籤 **[作業]** - 所有子標籤
資料倉儲管理員	配置「資料匯出程式」，並執行「資料倉儲匯出程式啓動程式」作業。	**[配置] - [倉儲]** 子標籤
資料倉儲查詢	配置並執行鑑識查詢	規範遵循/鑑識查詢
除錯	從 Identity Manager 的除錯頁面存取與執行作業。	您無法從功能表存取 Identity Manager 除錯頁面。若要存取除錯頁面，請在瀏覽器中鍵入下列 URL： `http://<AppServerHost>:<Port>/idm/` 除錯
刪除使用者	刪除 Identity Manager 使用者帳號；取消佈建、取消指定與取消連結資源帳號。不包括批次處理作業。	**[帳號] - [列出帳號]** (僅 [刪除])、**[尋找使用者]** 子標籤 **[作業]** - 所有子標籤
刪除 IDM 使用者	刪除 Identity Manager 使用者帳號。不包括批次處理作業。	**[帳號] - [列出帳號]** (僅 [刪除])、**[尋找使用者]** 子標籤 **[作業]** - 所有子標籤

表 D-1 Identity Manager 作業型權能定義 (第 7 頁，共 13 頁)

權能	允許管理員 / 使用者：	可以存取這些標籤與子標籤：
取消佈建使用者	刪除現有資源帳號並取消其連結。不包括批次處理作業。	**[帳號]** - **[列出帳號]** (僅 [取消佈建])、**[尋找使用者]** 子標籤 **[作業]** - 所有子標籤
停用使用者	停用現有的使用者和資源帳號。不包括批次作業	**[帳號]** - **[列出帳號]** (僅 [停用])、**[尋找使用者]** 子標籤 **[作業]** - 所有子標籤
啓用使用者	啓用現有的使用者和資源帳號。不包括批次作業	**[帳號]** - **[列出帳號]** (僅 [啓用])、**[尋找使用者]** 子標籤 **[作業]** - 所有子標籤
一般使用者管理員	檢視和修改物件類型 (指定於 [一般使用者] 權能和 [一般使用者所控制的組織] 規則) 的權限。	NA
IDM 模式配置	使用 Identity Manager 配置物件 `IDM` 模式配置，檢視和配置有效的使用者或角色模式。	NA
匯入使用者	從定義的資源匯入使用者。	**[帳號]** - **[擷取至檔案]**、**[從檔案載入]**、**[從資源載入]** 子標籤
匯入/匯出管理員	匯入和匯出所有類型的物件。	**[配置]** - **[匯入交換檔案]** 子標籤
IT 角色管理員	建立、編輯和刪除 IT 角色。	**[作業]** - **[尋找作業]**、**[全部作業]**、**[執行作業]** 子標籤 (同步化角色) **[角色]** - 所有子標籤
登入管理員	編輯指定登入介面的一組登入模組。	**[配置]** - **[登入]** 子標籤
組織管理員	建立、編輯和刪除組織。	**[帳號]** - **[列出帳號]** 子標籤 (僅 [編輯組織]、[建立組織]、[編輯目錄結合]、[建立目錄結合] 和 [刪除組織])
組織核准人	核准新組織請求。	**[工作項目]** - **[核准]** 子標籤
組織違規歷程記錄管理員	建立、修改、刪除和執行「組織違規歷程記錄」報告。	**[報告]** - 僅 [組織違規歷程記錄報告]
密碼管理員	變更和重設使用者與資源帳號密碼。	**[帳號]** - **[列出帳號]** (僅限列出、變更及重設密碼)、**[尋找使用者]** 子標籤 **[密碼]** - 所有子標籤 **[作業]** - 所有子標籤

表 D-1 Identity Manager 作業型權能定義 (第 8 頁，共 13 頁)

權能	允許管理員 / 使用者：	可以存取這些標籤與子標籤：
密碼管理員 (需要驗證)	在成功驗證使用者的身份認證問題答案後，變更和重設使用者與資源帳號密碼。	**[帳號]** - **[列出帳號]** (僅限列出、變更及重設密碼；必須先驗證才能進行下一個動作)、**[尋找使用者]** 子標籤 **[密碼]** - 所有子標籤 **[作業]** - 所有子標籤
策略管理員	建立、編輯和刪除策略。	**[配置]** - **[策略]** 子標籤
策略摘要報告管理員	建立、修改、刪除和執行「策略摘要報告」。	**[報告]** - 僅 [策略摘要報告]
產品註冊	向 Sun Microsystems 註冊 Identity Manager 的安裝，或建立本機服務標籤。	**[配置]** - **[產品註冊]** 子標籤
調解管理員	編輯調解策略和控制調解作業。	**[伺服器作業]** - 所有子標籤 (檢視調解作業)。 **[資源]** - **[列出資源]** 子標籤。
調解報告管理員	建立、編輯、刪除和執行調解報告。	**[報告]** - **[執行報告]** (僅 [帳號索引報告])、**[管理報告]** 子標籤
調解請求管理員	管理調解請求。	**[作業]** - 所有子標籤 **[資源]** - **[列出資源]** 子標籤 (僅限列出及調解功能)。
Remedy 整合管理員	修改 Remedy 整合配置。	**[作業]** - 所有子標籤 (檢視作業，執行角色同步化)。 **[配置]** - **[Remedy 整合]** 子標籤
重新命名使用者	重新命名現有的使用者和資源帳號。	**[帳號]** - [列出帳號] 子標籤 (列出範圍中的所有帳號、重新命名使用者)
報告管理員	配置稽核設定和執行所有報告類型。	**[作業]** - 所有子標籤 (檢視作業，執行角色同步化)。 **[報告]** - 所有子標籤
重設密碼管理員	重設使用者和資源帳號密碼。	**[帳號]** - **[列出帳號]**、**[尋找使用者]** 子標籤 (僅限 [重設密碼]) **[密碼]** - 所有子標籤 **[作業]** - 所有子標籤。僅 [匯出密碼掃描] 作業 (從 **[執行作業]** 子標籤)

表 D-1 Identity Manager 作業型權能定義 (第 9 頁，共 13 頁)

權能	允許管理員 / 使用者：	可以存取這些標籤與子標籤：
重設密碼管理員 (需要驗證)	在成功驗證使用者的身份認證問題答案後，重設使用者和資源帳號密碼。	**[帳號] - [列出帳號]**、**[尋找使用者]** 子標籤 (僅限 [重設密碼]；必須先驗證才能執行動作) **[密碼]** - 所有子標籤 **[作業]** - 所有子標籤。僅 [匯出密碼掃描] 作業 (從 **[執行作業]** 子標籤)
重設資源密碼管理員	重設資源管理員帳號密碼。	**[作業] - [尋找作業]**、**[全部作業]**、**[執行作業]** 子標籤 **[資源] - [列出資源]** 子標籤。僅重設資源密碼 (透過 [動作] 功能表的 **[管理連線] -->重設密碼**)
資源管理員	建立、修改和刪除資源。	**[報告]** - 資源使用者報告及資源群組報告會傳回有關範圍之外資源的錯誤。 **[資源] - [列出資源]** 子標籤 (編輯全域策略、編輯參數、資源群組。無法管理連線或資源物件)。
資源核准人	核准資源指定	**[工作項目] - [核准]** 子標籤
資源群組管理員	建立、編輯和刪除資源群組。	**[資源] - [列出資源群組]** 子標籤
資源物件管理員	建立、修改和刪除資源物件。	**[作業] - [尋找作業]**、**[全部作業]**、**[執行作業]** 子標籤 (檢視涉及資源物件的作業)。 **[資源] - [列出資源]** 子標籤 (僅限列出及管理資源物件)。
資源密碼管理員	變更和重設資源代理帳號密碼。	**[作業] - [尋找作業]**、**[全部作業]**、**[執行作業]** 子標籤 **[資源] - [列出資源]** 子標籤。僅變更資源密碼 (從 [動作] 功能表中的 **[管理連線] > [變更密碼]**)
資源報告管理員	建立、編輯、刪除和執行資源報告。	**[報告]** - 所有子標籤 (僅限資源報告)
資源違規歷程記錄管理員	建立、修改、刪除和執行 「資源違規歷程記錄」報告。	**[報告]** - 僅 [資源違規歷程記錄報告]
風險分析管理員	建立、編輯、刪除和執行風險分析。	**[風險分析]** - 所有子標籤

表 D-1 Identity Manager 作業型權能定義 (第 10 頁，共 13 頁)

權能	允許管理員 / 使用者：	可以存取這些標籤與子標籤：
角色管理員	建立、修改和刪除角色。	**[作業]** - **[尋找作業]**、**[全部作業]**、**[執行作業]** 子標籤 (同步化角色) **[角色]** - 所有子標籤
角色核准人	核准角色指定	**[工作項目]** - **[核准]** 子標籤
角色報告管理員	建立、編輯、刪除和執行資源報告。	**[報告]** - 僅 [角色報告]
執行存取檢閱詳細資訊報告	執行存取檢閱詳細資訊報告	**[報告]** - 僅 [存取檢視詳細資訊報告]
執行存取檢閱摘要報告	執行存取檢閱摘要報告	**[報告]** - 僅 [存取檢視摘要報告]
執行管理員報告	執行管理員報告。	**[報告]** - 僅 [管理員報告]。
執行稽核策略掃描管理員	執行和管理稽核策略掃描報告	[報告] - 僅 [稽核策略掃描報告]
執行稽核策略掃描報告	執行稽核策略掃描報告。	**[報告]** - 僅 [稽核策略掃描報告]
執行稽核報告	執行稽核報告。	**[報告]** - 僅 [稽核記錄報告] 及 [使用情況報告]
執行已稽核的屬性報告	執行 「已稽核的屬性報告」。	**[報告]** - 僅 [已稽核的屬性報告] **[報告] > [檢視面板]**
執行 Auditor 報告	執行任何 Auditor 報告。	**[報告]** - 任何 Auditor 報告 **[報告] > [檢視面板]**
執行稽核記錄報告	執行 「稽核記錄報告」。	**[報告]** - 僅 [稽核記錄報告]
執行稽核策略違規歷程記錄	執行 「組織違規歷程記錄」報告。	**[報告]** - 僅 [稽核策略違規歷程記錄報告] **[報告] > [檢視面板]**
執行策略摘要報告	執行 「策略摘要報告」。	**[報告]** - 僅 [策略摘要報告]
執行組織違規歷程記錄	執行 「組織違規歷程記錄」報告。	**[報告]** - 僅 [組織違規歷程記錄報告] **[報告] > [檢視面板]**
執行調解報告	執行調解報告。	**[報告]** - 僅 [稽核記錄報告] 及 [使用情況報告]
執行資源報告	執行資源報告。	**[報告]** - 僅 [稽核記錄報告] 及 [使用情況報告]

表 D-1 Identity Manager 作業型權能定義 (第 11 頁，共 13 頁)

權能	允許管理員 / 使用者：	可以存取這些標籤與子標籤：
執行資源違規歷程記錄	執行「資源違規歷程記錄」報告。	**[報告]** - 僅 [資源違規歷程記錄報告]
執行風險分析	執行風險分析。	**[報告]** - [執行風險分析]、[檢視風險分析] 子標籤
執行角色報告	執行角色報告。	**[報告]** - 僅 [角色報告]
執行責任分離報告	執行責任分離報告	**[報告]** - 僅 [權責區分報告] **[報告] > [檢視面板]**
執行作業報告	執行作業報告。	**[報告]** - 僅 [作業報告]
執行使用者存取報告	執行「詳細使用者報告」。	**[報告]** - 僅 [使用者存取報告] **[報告] > [檢視面板]**
執行使用者報告	執行使用者報告。	**[報告]** - 僅 [使用者報告]
執行違規摘要報告	執行「違規摘要」報告。	**[報告]** - 僅 [違規摘要報告] **[報告] > [檢視面板]**
安全管理員	建立具有權能的管理員、管理加密金鑰、登入配置和策略。	**[帳號]** - **[列出帳號]** (刪除、建立、更新、編輯、變更及編輯密碼)、**[尋找使用者]** 子標籤 (稽核報告) **[密碼]** - 所有子標籤 **[作業]** - **[尋找作業]**、**[全部作業]**、**[執行作業]** 子標籤 **[報告]** - 所有子標籤 **[資源]** - **[列出資源]** (列出及控制資源物件)。 **[安全性]** - **[策略]**、**[登入]** 子標籤
責任分離報告管理員	建立、編輯、執行和刪除責任分離報告。	**[報告]** - 僅限對責任分離報告的所有動作
服務提供者管理員角色	管理服務提供者管理員角色和關聯的規則。	**[安全性]** - **[管理員角色]** 標籤

表 D-1 Identity Manager 作業型權能定義 (第 12 頁，共 13 頁)

權能	允許管理員 / 使用者：	可以存取這些標籤與子標籤：
「服務提供者」的管理員	建立、編輯和管理服務提供者使用者和作業事件；配置作業事件資料庫和追蹤的事件。	**[帳號] - [管理「服務提供者」使用者]** 子標籤 **[伺服器作業] > [服務提供者作業事件]** 標籤 **[報告] > [檢視面板]** 標籤 **[報告] > [面板配置]** 標籤 **[服務提供者]** - 所有子標籤
「服務提供者」的建立使用者	爲服務提供者 (企業外部網路) 使用者建立使用者帳號。	**[帳號] - [管理「服務提供者」使用者]** 子標籤
「服務提供者」的刪除使用者	刪除服務提供者使用者帳號。	**[帳號] - [管理「服務提供者」使用者]** 子標籤
「服務提供者」的更新使用者	更新服務提供者使用者帳號。	**[帳號] - [管理「服務提供者」使用者]** 子標籤
服務提供者使用者管理員	管理服務提供者 (企業外部網路) 使用者。	**[帳號] > [管理「服務提供者」使用者]** - 所有子標籤
服務提供者檢視使用者	檢視服務提供者 (企業外部網路) 使用者帳號資訊。	**[帳號] - [管理「服務提供者」使用者]** 子標籤
SPML 存取	允許存取 Identity Manager 中的服務佈建標記語言 (SPML) 功能。	**[安全性] - [權能]** 子標籤
作業報告管理員	建立、編輯、刪除和執行作業報告。	**[報告]** - 僅 [作業報告]。
取消指定使用者	取消指定現有資源帳號並取消其連結。不包括批次處理作業。	**[帳號] - [列出帳號]** (僅 [取消指定])、**[尋找使用者]** 子標籤 **[作業]** - 所有子標籤
取消連結使用者	取消現有資源帳號連結。不包括批次處理作業。	**[帳號] - [列出帳號]** (僅 [解除連結])、**[尋找使用者]** 子標籤 **[作業]** - 所有子標籤
解除鎖定使用者	解除鎖定支援此項作業之現有使用者的資源帳號。不包括批次處理作業。	**[帳號] - [列出帳號]** (僅 [解除鎖定])，**[尋找使用者]** 子標籤 **[作業] - [尋找作業]**、**[全部作業]**、**[執行作業]** 子標籤

表 D-1 Identity Manager 作業型權能定義 (第 13 頁，共 13 頁)

權能	允許管理員 / 使用者：	可以存取這些標籤與子標籤：
更新使用者	編輯現有使用者和發起使用者更新請求。	**[帳號]** - 編輯和更新使用者 **[作業]** - 管理現有作業 (從 **[全部作業]** 子標籤)
使用者存取報告管理員	建立、執行、編輯和刪除使用者存取報告	**[報告]** - 僅 [使用者存取報告] **[報告] > [檢視面板]**
使用者帳號管理員	對使用者執行所有作業。	**[帳號]** - **[列出帳號]**、**[尋找使用者]**、**[擷取至檔案]**、**[從檔案載入]**、**[從資源載入]** 子標籤。無法指定使用者權能 (**[列出帳號]** 子標籤上的 **[安全性]** 表單標籤)。 **[作業]** - **[尋找作業]**、**[全部作業]**、**[執行作業]** 子標籤
使用者報告管理員	建立、編輯、刪除和執行使用者報告。	**[報告]** - [執行使用者報告]。
檢視使用者	檢視個別使用者詳細資訊。	**[帳號]** - 從清單選取使用者以檢視個別使用者帳號資訊。不允許執行變更動作。
違規摘要報告管理員	建立、修改、刪除和執行 「違規摘要」報告。	**[報告]** - 僅 [違規摘要報告] **[報告] > [檢視面板]**
Waveset 管理員	執行系統範圍的作業，如修改系統配置物件。	**[伺服器作業]** - 所有子標籤。同步化角色、編輯來源介面範本，並排程報告。 **[報告]** - 所有子標籤 **[資源]** - [列出資源] (僅列出，不允許變更動作) **[配置]** - **[稽核]**、**[電子郵件範本]**、**[表單與程序對映]** 和 **[伺服器]** 子標籤

功能性權能定義

功能性權能包含作業型權能，以及其他功能性權能。

帳號管理員

- 核准人管理員
  - 組織核准人
  - 資源核准人
  - 角色核准人
- 指定使用者權能
- SPML 存取
- 使用者帳號管理員
  - 建立使用者
  - 刪除使用者
    - 刪除 IDM 使用者
    - 取消佈建使用者
    - 取消指定使用者
    - 取消使用者連結
  - 停用使用者
  - 啓用使用者
  - 密碼管理員
    - 變更密碼管理員
    - 重設密碼管理員
  - 重新命名使用者
  - 解除鎖定使用者
  - 更新使用者
  - 檢視使用者
  - 匯入使用者

管理員角色管理員

Auditor 管理員

- 指定稽核策略
  - 指定組織稽核策略
  - 指定使用者稽核策略
- 稽核策略管理員
  - Auditor 檢視使用者
- 稽核員定期存取檢閱管理員
  - 稽核員存取掃描管理員
- Auditor 報告管理員
- 密碼管理員
- 使用者帳號管理員
- 指定使用者權能

Auditor 報告管理員

- 存取檢閱詳細資訊報告管理員
  - 執行存取檢閱詳細資訊報告
- 存取檢閱摘要報告管理員
  - 執行存取檢閱摘要報告
- 稽核策略掃描報告管理員
  - 執行稽核策略掃描報告
- 已稽核的屬性報告管理員
  - 執行已稽核的屬性報告
- 稽核策略違規歷程記錄管理員
  - 執行稽核策略違規歷程記錄報告
- 組織違規歷程記錄管理員
  - 執行組織違規歷程記錄報告
- 策略摘要報告管理員

- 資源違規歷程記錄管理員
  - 執行資源違規歷程記錄報告
- 執行 Auditor 報告
- 責任分離報告管理員
  - 執行責任分離報告
- 使用者存取報告管理員
  - 執行使用者存取報告
- 違規摘要報告管理員

Auditor 檢視使用者

- 檢視使用者

批次帳號管理員

- 核准人管理員
- 指定使用者權能
- 批次使用者帳號管理員
  - 批次建立使用者
  - 批次刪除使用者
    - 批次刪除 IDM 使用者
    - 批次取消佈建使用者
    - 批次取消指定使用者
    - 批次取消連結使用者
  - 批次停用使用者
  - 批次啓用使用者
  - 密碼管理員
  - 重新命名使用者
  - 解除鎖定使用者
  - 檢視使用者
  - 匯入使用者

批次變更帳號管理員

- 核准人管理員
- 指定使用者權能
- 批次變更使用者帳號管理員
  - 批次停用使用者
  - 批次啓用使用者
  - 批次更新使用者
  - 密碼管理員
  - 重新命名使用者
  - 解除鎖定使用者
  - 檢視使用者

批次資源管理員

- 變更 Active Sync 資源管理員
- 控制 Active Sync 資源管理員
- 資源群組管理員

批次資源密碼管理員

- 批次變更資源密碼管理員
- 批次重設資源密碼管理員

權能管理員

變更帳號管理員

- 核准人管理員
- 指定使用者權能
- 變更使用者帳號管理員
  - 密碼管理員
    - 變更密碼管理員
    - 重設密碼管理員
  - 停用使用者

- 啓用使用者
- 重新命名使用者
- 解除鎖定使用者
- 更新使用者
- 檢視使用者

配置憑證

資料倉儲管理員

資料倉儲查詢

除錯

一般使用者管理員

IDM 模式配置

匯入/匯出管理員

授權管理員

登入管理員

中介檢視管理員

組織管理員

密碼管理員 (需要驗證)

- 變更密碼管理員 (需要驗證)
- 重設密碼管理員 (需要驗證)

策略管理員

產品註冊

調解管理員

- 調解請求管理員

Remedy 整合管理員

報告管理員

- 管理員報告管理員
  - 執行管理員報告
- 稽核報告管理員
  - 執行稽核報告
- Auditor 報告管理員
  - 存取檢閱詳細資訊報告管理員
    - 執行存取檢閱詳細資訊報告
  - 存取檢閱摘要報告管理員
    - 執行存取檢閱摘要報告
  - 稽核策略掃描報告管理員
    - 執行稽核策略掃描報告
  - 已稽核的屬性報告管理員
    - 執行已稽核的屬性報告
  - 稽核記錄報告管理員
    - 執行稽核記錄報告
  - 稽核策略違規歷程記錄管理員
    - 執行稽核策略違規歷程記錄
  - 組織違規歷程記錄管理員
    - 執行組織違規歷程記錄
  - 策略摘要報告管理員
    - 執行策略摘要報告
  - 調解報告管理員
    - 執行調解報告
  - 資源違規歷程記錄管理員
    - 執行資源違規歷程記錄

- 執行 Auditor 報告
  - 執行存取檢閱詳細資訊報告
  - 執行存取檢閱摘要報告
  - 執行稽核策略掃描報告
  - 執行已稽核的屬性報告
  - 執行稽核記錄報告
  - 執行稽核策略違規歷程記錄
  - 執行組織違規歷程記錄
  - 執行策略摘要報告
  - 執行資源違規歷程記錄
  - 執行責任分離報告
  - 執行使用者存取報告
  - 執行違規摘要報告
- 責任分離報告管理員
  - 執行責任分離報告
- 使用者存取報告管理員
  - 執行使用者存取報告
- 違規摘要報告管理員
  - 執行違規摘要報告

- 調解報告管理員
  - 執行調解報告
- 資源報告管理員
  - 執行資源報告
- 風險分析管理員
  - 執行風險分析
- 角色報告管理員
  - 執行角色報告

- 作業報告管理員
  - 執行作業報告
- 使用者報告管理員
  - 執行使用者報告
- 配置稽核

資源管理員

- 變更 Active Sync 資源管理員
- 控制 Active Sync 資源管理員
- 資源群組管理員

資源物件管理員

資源密碼管理員

- 變更資源密碼管理員
- 重設資源密碼管理員

角色管理員

- 應用程式管理員
- 資產管理員
- 商務角色管理員
- IT 角色管理員

安全管理員

「服務提供者」的管理員

- 「服務提供者」的使用者管理員
  - 「服務提供者」的建立使用者
  - 「服務提供者」的刪除使用者
  - 「服務提供者」的更新使用者
  - 服務提供者檢視使用者

服務提供者管理員角色管理員

Waveset 管理員

字彙表

存取檢閱　可讓管理員或其他負責人檢閱及驗證使用者存取權限的受稽核程序。此程序可自動核准或拒絕使用者軟體權利文件記錄，亦可手動驗證。另請參閱「驗證作業」。

帳號屬性　帳號屬性提供 Identity Manager 管理員建立標準名稱集的方法，這些名稱將對映到受管資源上的屬性。例如，名爲 **fullname** 的 Identity Manager 屬性可能對映至 Active Directory 資源上的 **displayName** 屬性，以及 LDAP 資源上的 **cn** 屬性。使用者 Identity Manager 內 **fullname** 屬性的任何變更，都會傳遞到使用者遠端資源帳號上的使用者 **displayName** 與 **cn** 屬性。

管理員角色　指定給管理使用者的每組組織的獨特權能群組。

管理員　配置 Identity Manager 或負責操作作業的人員，如建立使用者和管理資源的存取權。

管理員介面　管理員用以配置及管理 Identity Manager 的使用者介面。

應用程式 (角色)　Identity Manager 的四種角色類型之一，應用程式角色類型是使用者執行工作時，所需的一組資源、資源群組及 (或) 資源上特定應用程式之集合。應用程式角色無法直接指定給使用者，但可指定給 IT 角色與業務角色。

核准　授予或拒絕使用者對角色、資源或組織的存取請求之程序。具有檢視及回應核准工作項目權限的 Identity Manager 管理員，稱爲**核准人**。

核准人　具有管理權能的使用者，負責核准或拒絕存取請求。

資產 (角色)　Identity Manager 的四種角色類型之一，資產角色類型 (一般) 會保留給需要手動佈建的非連線及 (或) 非數位資源，例如行動電話和可攜式電腦。資產角色無法直接指定給使用者，但可指定給 IT 角色與業務角色。

驗證　驗證者在進行存取檢閱過程中執行的動作，以確認使用者軟體權利文件是適當的。

驗證　驗證特定使用者是否在特定時間點，對適當資源具有適當權限的程序。有權檢視及回應驗證工作項目的 Identity Manager 使用者稱之爲**驗證者**。Identity Manager 規則會決定使用者軟體權利文件記錄是否需要手動驗證，或者是否可自動核准或拒絕。

驗證作業　需驗證的使用者軟體權利文件檢閱程序之邏輯集合。如果使用者軟體權利文件指定給相同的驗證者，且由相同的存取檢閱實例所產生，則會將其分組爲單一驗證作業。

驗證者　負責檢驗 (**驗證**) 使用者軟體權利文件是否適用的使用者。驗證者在 Identity Manager 中具有延伸權限，這些權限是管理需要驗證的使用者軟體權利文件所必需。

商務角色　商務角色是 Identity Manager 的四種角色類型之一，將組織中執行類似作業之人員的存取權限分組。商務角色的角色類型由一個或多個資產角色、應用程式角色及 (或) IT 角色所組成。商務角色可直接指定給使用者。

業務程序編輯器 (BPE)　Identity Manager 7.0 之前版本所提供的圖形化檢視，用於檢視 Identity Manager 表單、規則和工作流程。在目前版本的 Identity Manager 中，BPE 已由 Identity Manager IDE 所取代。請參閱「**Identity Manager IDE**」。

權能　使用者帳號的存取權限群組，可管理 Identity Manager 所執行的動作；Identity Manager 內的低階存取控制。

委派　在特定期間，暫時將未來工作項目指定給一個或多個其他使用者的程序。

目錄結合　是一組階層式的相關組織，對目錄資源中的一組實際階層式容器進行鏡像。目錄結合中的每個組織皆是**虛擬組織**。

軟體權利文件　請參閱「使用者軟體權利文件」。

上報逾時時間　爲工作項目請求指定的時間範圍；在此時間範圍內，指定的工作項目所有者必須在 Identity Manager 程序會將其傳送至下一個指定的回應者之前做出回應。

表單　網頁所關聯的物件，包含瀏覽器如何在該網頁上顯示使用者檢視屬性的規則。表單可包含業務邏輯，且通常可用以操作檢視資料，再將該資料呈現給使用者。

IDE　**請參閱**「Identity Manager IDE」。

Identity Manager IDE　Identity Manager 整合開發環境 (IDE) 是一個應用程式，可讓您針對自己部署中的 Identity Manager 物件進行檢視、自訂和除錯。IDE 係以 NetBeans 外掛程式方式提供。

身份識別範本　定義使用者的資源帳號名稱。

IT 角色　Identity Manager 的四種角色類型之一，IT 角色的角色類型是一組角色 (資產、應用程式及 (或) 其他巢式 IT 角色)，以及資源 及 (或) 資源群組的集合。在某些配置中，IT 角色可直接指定給使用者，但通常 IT 角色會指定給商務角色，再指定給使用者。

組織　用於啓用管理委派的 Identity Manager 容器。

組織可定義管理員控制或管理的實體範圍 (如使用者帳號、資源和管理員帳號)。組織提供了「位置」環境，主要用於 Identity Manager 的管理作業。

定期存取檢閱　在定期間隔執行的存取檢閱，例如每個日曆季。

策略　建立 Identity Manager 帳號的限制。

Identity Manager 策略可建立使用者、密碼和認證選項，並繫結到組織或使用者。資源密碼和帳號 ID 策略可設定規則、允許的文字和屬性值，並繫結到個別資源。

調解　將位於資源本身之帳號定期與 Identity Manager 中資源帳號相比對的 Identity Manager 功能。調解會使帳號資料產生相互的關聯，並凸顯其差異。

修正　更正由 Identity Manager 稽核功能所發現之規範遵循違規的程序。Identity Manager 會稽核企業內的資料，以確保會遵循內部與外部策略與規定。有權檢視及回應策略違規的管理員稱之爲**修正者**。

修正者　指定爲稽核策略之指定修正者的 Identity Manager 使用者。

當 Identity Manager 偵測到需要修正的規範遵循違規時，就會建立一個修正工作項目，並將此工作項目傳送至修正者的工作項目清單。

資源　在 Identity Manager 中，資源會儲存有關如何連線至帳號建立所在之遠端資源或系統的資訊。Identity Manager 提供的遠端存取資源包括主機安全性管理員、資料庫、目錄服務、應用程式、作業系統、ERP 系統、訊息傳送平台等。

資源介面　提供 Identity Manager 引擎與資源之間之連結的 Identity Manager 元件。

此元件可讓 Identity Manager 管理指定資源的使用者帳號 (包括建立、更新、刪除、認證及掃描功能)，以及利用該資源來通過認證。

資源介面帳號　Identity Manager 資源介面用以存取受管資源的憑證。

資源群組　爲資源集合，可發出建立、刪除及更新使用者資源帳號的命令。

資源精靈　可用來指示資源建立和修改程序步驟的 Identity Manager 工具，包括安裝及配置資源參數、帳號屬性、身份識別範本和 Identity Manager 參數。

角色　角色是 Identity Manager 物件，可將資源存取權限分組，並以效率極高的方式指定給使用者。角色分爲四種角色類型：商務角色、IT 角色、應用程式角色及資產。IT 角色、應用程式和資產可將資源軟體權利文件劃分爲不同群組。這三個群組接著會指定給商務角色，如此一來，使用者即可存取執行工作所需的資源。

規則　Identity Manager 儲存庫中的物件，包含以 XPRESS、XML 物件或 JavaScript 語言所撰寫的函數。規則提供了一個機制，可用來儲存常用的邏輯或靜態變數，以便在表單、工作流程和角色中重複使用。

模式　資源的使用者帳號屬性之清單。

模式對映　資源帳號屬性與資源的 Identity Manager 帳號屬性間的對映。

Identity Manager 帳號屬性可爲多個資源建立一個共用連結，並由表單參照。

服務提供者使用者　企業外部網路使用者，或單獨從服務提供者公司的人員或企業內部網路使用者中區別出來的服務提供者用戶。

user　擁有 Identity Manager 系統帳號的人員。使用者可在 Identity Manager 中擁有某些權能；具有許多權能者爲 Identity Manager **管理員**。

使用者帳號　使用 Identity Manager 建立的帳號。

可指 Identity Manager 帳號，或指位於 Identity Manager 所管理之遠端資源上的帳號。使用者帳號設定程序是動態的。需要完成哪些資訊或欄位，取決於是透過指定角色將資源直接還是間接提供給使用者而定。

使用者軟體權利文件　在 Identity Manager 中，係指對於執行存取限制的資源或系統，授予其使用者可稽核的存取權限。

使用者介面　在 Identity Manager 中，使用者介面可讓不具有管理權能的使用者執行特定範圍的自助作業，例如變更密碼及設定認證問題的解答，以及管理已委託的任務。又稱爲**一般使用者介面**。

虛擬組織　在目錄結合內定義的組織。請參閱「目錄結合」。

工作流程　一個邏輯且可重複的程序，可讓文件、資訊或作業在參與者之間傳送。Identity Manager 工作流程包含多個程序，可控制使用者帳號的建立、更新、啓用、停用和刪除。

工作項目　Identity Manager 工作流程、表單或程序所產生的動作請求。核准、變更核准、驗證與修正是四大工作項目。

索引

I

J

L

M

O

P

六畫

七畫

八畫

九畫

十畫

十一畫

十二畫

十三畫

十四畫

十五畫

十七畫

十八畫

十九畫

二十一畫

二十二畫

二十三畫