Sun Java™ System

Identity Manager 7.0
管理指南

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

文件號碼：820-0141

目錄

圖清單

表格清單

前言

本指南說明如何使用 Sun Java™ System 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 管理指南」適用於使用 Sun Java System 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。

瞭解以下技術將有助於您應用本書中說明的資訊：

- 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 Java System 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 和 http://docs.sun.com/app/docs/coll/DirectoryServer_04q2_zh_TW)。

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。	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)	您鍵入的內容，與螢幕畫面輸出相對。	`% su` `Password:`
AaBbCc123 (斜體)	指令或路徑名稱中要由真實名稱或值替代的預留位置。	該檔案位於 *install-dir*`/bin` 目錄中。
術語強調變數	新的字彙或術語、要強調的詞。	這些稱爲**類別**選項。 請**勿**儲存此檔案。
「AaBbCc123」	用於書名及章節名稱。	請閱讀 「使用者指南」中的第 6 章。

* 瀏覽器中的設定可能會與這些設定不同。

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。	Control-A	按下 Control 鍵的同時按下 A 鍵。
+	連續按下多個按鍵。	Ctrl+A+N	按下 Control 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考資訊。
- 「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考資訊。
- 「Identity Manager Administration」— 說明如何使用 Identity Manager 來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、表單和檢視的參考資訊和程序資訊 (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 部署工具的參考資訊和程序資訊，包括規則和規則程式庫、一般作業和程序、字典支援以及由 Identity Manager 伺服器提供的基於 SOAP 的 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 並使其同步化的參考資訊和程序資訊。
- 「Identity Manager Tuning, Troubleshooting, and Error Messages」— 說明 Identity Manager 錯誤訊息和異常，並爲追蹤和疑難排解工作中可能遇到的問題提供指示的參考資訊和程序資訊。
- 「Identity Manager Service Provider Edition Deployment」— 說明如何計劃與實作 Sun Java™ System Identity Manager Service Provider Edition 的參考資訊和程序資訊。
- 「Identity Manager Help」— 提供有關 Identity Manager 的完整程序、參考和術語資訊的線上指導與資訊。按一下 Identity Manager 功能表列中的 [Help] 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 [Send Comments (傳送您的意見)]。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。

例如，本書的標題爲 Sun Java System Identity Manager 7.0 管理指南，文件號碼爲 820-0141。

在您提出意見時，可能需要在表單中輸入英文版書名和文件號碼，本書的英文版文件號碼和書名爲：819-6123 和「Sun Java System Identity Manager 7.0 Administration」。

Identity Manager 簡介

Sun Java™ System Identity Manager 系統可讓您安全有效地管理和稽核對帳號和資源的存取。Identity Manager 爲您提供快速處理定期工作與每日工作的權能與工具，可讓您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 服務爲其提供持續增加的靈活性以及各項權能。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。而後越來越多的情況顯示，管理存取不僅意味著處理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，您必須讓人們 (不論是企業內部或外部) 有效與安全地執行他們的工作。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。在受到與遵循性相關的法律規定的環境下，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 (GLB)」，爲了監控和報告活動所產生的管理費用益發龐大及高昂。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。藉由將 Identity Manager 物件對映至您管理的實體 (使用者與資源)，您將可以大幅提昇作業效率。

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。
- 爲每位使用者的系列帳號安全地管理動態帳號資訊。
- 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。

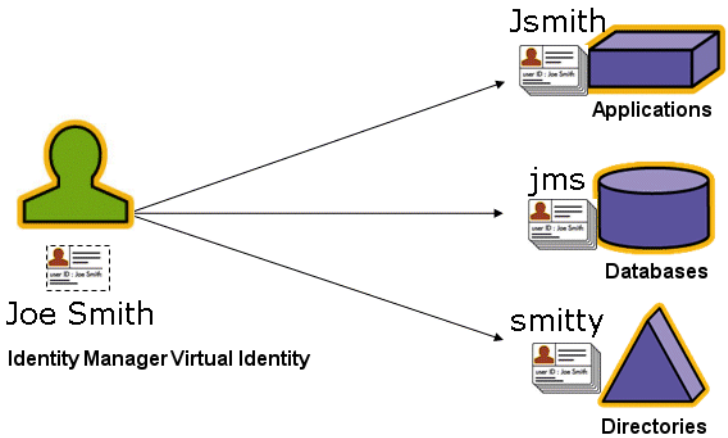
定義使用者存取

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 使用者帳號與資源的關係



若要有效地管理大量使用者，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。

委託管理

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。這些情況說明如下：

- 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

使用者帳號

Identity Manager 使用者帳號：

- 提供使用者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。
- 指定角色，角色設定使用者能否存取各種資源。
- 爲組織的一部份，可決定管理使用者帳號的方式與人員。

使用者帳號設定程序爲動態的。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。

您可以授予使用者管理使用者帳號、資源與其他 Identity Manager 系統物件和工作的管理權限。Identity Manager 管理員負責管理組織，並被指定了適用於每個受管理組織中之物件的一系列權能。

角色

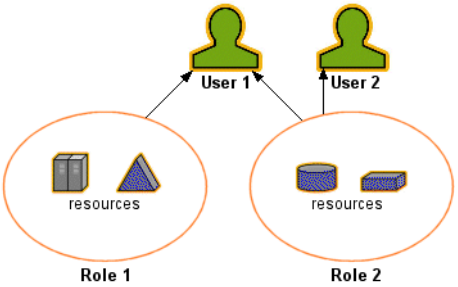
所謂角色是指代表 Identity Manager 使用者類型的 Identity Manager 物件，它允許將資源分組並指定給使用者。一般而言，角色代表使用者職務類別。例如在金融機構中，角色可能相當於銀行行員、貸款員、分支經理、記帳員、會計人員或行政主任等職務類別。

角色定義使用者的基本資源組以及資源屬性。也可以定義與其他角色之間的關係；例如包含或排除其他角色的角色。

擁有相同角色的使用者會存取共同的基礎資源群組。您可以爲每個使用者指定一個或多個角色，也可以不指定任何角色。

如圖 1-2 所示，使用者 1 和使用者 2 藉由被指定爲角色 2 而共同存取相同資源。而使用者 1 還可藉由被指定爲角色 1 而存取其他資源。

圖 1-2 使用者帳號，角色，資源關係



資源與資源群組

Identity Manager 資源會儲存有關如何與建立帳號的資源或系統建立連線的資訊。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™)

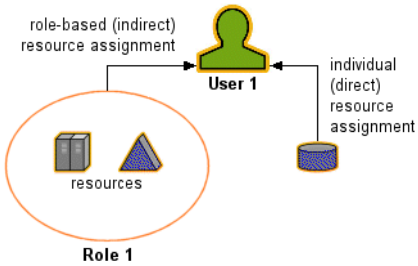
每個 Identity Manager 資源所儲存的資訊會分類成數個主要群組：

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

Identity Manager 使用者帳號透過以下指定存取資源，如圖 1-3 所示：

- 以角色爲基礎指定 — 藉由將角色指定給使用者，您可以間接地將使用者指定給與該角色連接的一個或多個資源。
- 個別指定 — 您可以直接將個別資源指定給使用者帳號。

圖 1-3 指定資源



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資訊，請參閱第 106 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。

組織也可表示與目錄式資源的直接連結；它們稱爲**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。

目錄結合

目錄結合是一組階層式的相關組織，它鏡射一組目錄資源的實際階層式容器。**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射。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，而且還鏡射一個爲已定義資源的基底環境容器之子系的目錄資源容器。

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。

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。

管理員角色

透過管理員角色，您可以爲由管理使用者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受控組織，隨後可將該管理員角色指定給管理使用者。

權能與受控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。

策略

藉由爲帳號 ID、登入與密碼特性建立限制，**策略**可爲 Identity Manager 使用者設定限制。*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。

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。稽核策略建立一或多個規則，並根據這些規則來評估使用者的遵循性違規。這些規則需視資源所定義之一或多個屬性而定。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。

Object Relationships

下表爲 Identity Manager 物件及其相互關係的簡要介紹。

表 1-1 Identity Manager Object Relationships

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，會為每個使用者帳號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，做為組織的一部份。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	描述某類別使用者的概況並定義用以管理帳號的資源集合與資源屬性。	**資源與資源群組** 資源與資源群組會指定給角色。 **使用者帳號** 將具有類似特性的使用者帳號分組的角色。 **角色** 定義與其他角色之間的關係 (包括或排除)。
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** 資源會指定給角色；使用者帳號會透過其角色指定來「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 Object Relationships (繼續)

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** 資源群組會指定給角色；使用者帳號會透過其指定角色「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		
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	設定用來評估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。

Identity Manager 專有名詞

Identity Manager 介面與指南定義這些專有名詞如下：

存取檢閱
驗證一組員工在特定日期是否具有適當的使用者軟體權利文件的管理和稽核程序。

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
設定 Identity Manager 或負責營運作業的人員，如建立使用者和管理資源的存取。

管理員介面
Identity Manager 的主要管理檢視。

核准人
具有管理權能的使用者，負責核准或拒絕存取請求。

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。

驗證作業
需要驗證之使用者軟體權利文件檢閱的邏輯集合。如果將使用者軟體權利文件指定給同一驗證者，並且它們產生於同一存取檢閱實例，則它們將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當的使用者。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。

業務程序編輯器 *(BPE)*
Identity Manager 表單、規則和工作流程的圖形檢視。BPE 雖然仍受支援，但在目前版本的 Identity Manager 中已由 Identity Manager IDE 取代。

權能
使用者帳號的存取權群組，可監控 Identity Manager 所執行的動作；Identity Manager 內部的低層級存取控制。

目錄結合
組織的階層式相關集合，可鏡射目錄資源的階層容器實際集合。目錄結合中的每個組織皆是**虛擬組織**。

提昇逾時
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，且通常可用來操作檢視資料，再將該資料呈現給使用者。

身份識別範本
定義使用者的資源帳號名稱。

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。

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，會建立一個修正工作項目並將該工作項目傳送至修正者的工作項目清單。

資源
在 Identity Manager 中，儲存如何與建立帳號的資源或系統連線的相關資訊。Identity Manager 提供的存取資源包括主機安全管理程式、資料庫、目錄服務、應用程式、作業系統、ERP 系統和訊息平台。

資源配接器
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。

資源配接器帳號
Identity Manager 資源適配器用來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
Identity Manager 中的使用者類別之範本或設定檔。每個使用者可指定給一或多個角色，這些角色定義帳號資源存取權和預設的資源屬性。

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。模式對映做爲資源精靈的一部分顯示。

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。

使用者
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；擁有延伸權能的使用者即爲 Identity Manager 管理員。

使用者帳號
使用 Identity Manager 建立的帳號。指 Identity Manager 帳號或位於 Identity Manager 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，則取決於系統透過指定角色，將資源提供給使用者的方式 (直接或間接)。

使用者軟體權利文件
針對特定日期的單一使用者，顯示指定資源及其重要屬性的使用者檢視。

使用者介面
Identity Manager 系統的有限檢視。針對不含管理權能的使用者所特別設計的介面，可讓該使用者執行某個範圍的自助工作，如變更密碼及設定身份驗證問題的答案。

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 中的工作流程、表單或程序所產生的動作請求，已將其指定給指定爲核准人、驗證者或修正者的使用者。

章節 2

Identity Manager 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 介面

Identity Manager 系統包括三個主要圖形化介面，使用者可透過這些介面來執行作業：

- 管理員介面
- 使用者介面
- Identity Manager IDE

Identity Manager 管理員介面

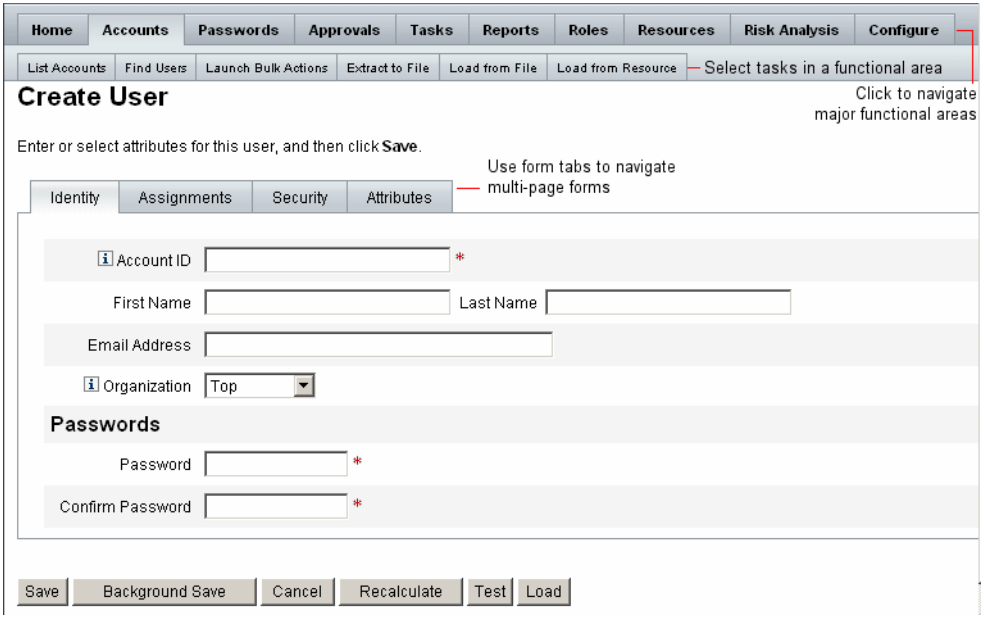
Identity Manager 管理介面可以做爲本產品的主要管理檢視。透過此介面，Identity Manager 管理員可以管理使用者、設定與指定資源、定義權限與存取等級，以及稽核 Identity Manager 系統中的規範遵循。

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，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 [Accounts]) 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。

圖 2-1 Identity Manager 管理員介面

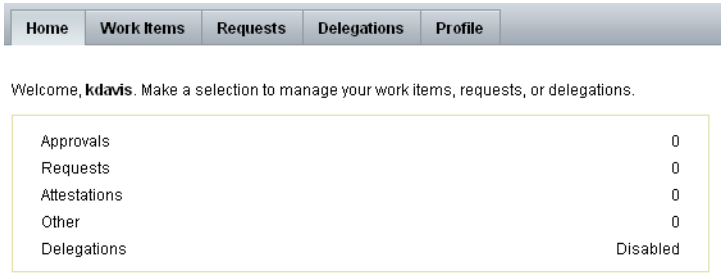


Identity Manager 使用者介面

Identity Manager 使用者介面只顯示 Identity Manager 系統的一部分視圖。此視圖專爲不具備管理權能的使用者而設計。

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

圖 2-2 使用者介面 ([Home] 標籤)



[Home] 標籤提供對任何擱置項目的快速存取。按一下清單中的項目可以回應工作項目請求或執行其他可用動作。動作完成以後，按一下 **[Return to Main Menu]** 可以返回到 [Home] 頁面。

使用者可以從使用者介面執行各種動作，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。

使用者介面爲使用者提供以下選項：

- **[Work Items]** — 核准或拒絕所有您擁有或對其具有執行動作權限的擱置工作項目。

  工作項目可以包括核准、驗證或由 Identity Manager 產生的其他請求動作項目。

- **[Requests]** — 將更新請求提交給使用者帳號資源指定、角色指定以及資源群組成員。

  這些請求可以對使用者或其員工執行。

  使用 [Requests] 標籤上的 **[View]** 子標籤可檢視請求的處理狀態詳細資訊。

- **[Delegations]** — 檢視目前的委託或指定委託。

- **[Profile]** — 使用以下子標籤變更您的使用者密碼或帳號屬性或者執行其他自我佈建作業：
  - **[Change Password]** — 選取此選項可在所選資源或所有資源上變更您的密碼。
  - **[Account Attributes]** — 選取此選項可變更使用者可編輯的屬性，例如您的帳號電子郵件地址。(此電子郵件地址爲 Identity Manager 用於傳送有關您帳號之通知的地址。)
  - **[Authentication Questions]** — 選取此選項可變更您的使用者帳號認證問題答案。
  - **[Access Privileges]** — 選取此選項可檢視此帳號的資源指定 (直接或間接)。

自訂使用者介面

通常將使用者介面自訂爲顯示唯一的公司特定檢視並提供自訂選項。

如果願意，可以將使用者介面中的瀏覽從水平標籤檢視 (預設) 變更爲垂直樹狀結構檢視。若要配置垂直瀏覽檢視，請設定以下配置物件：

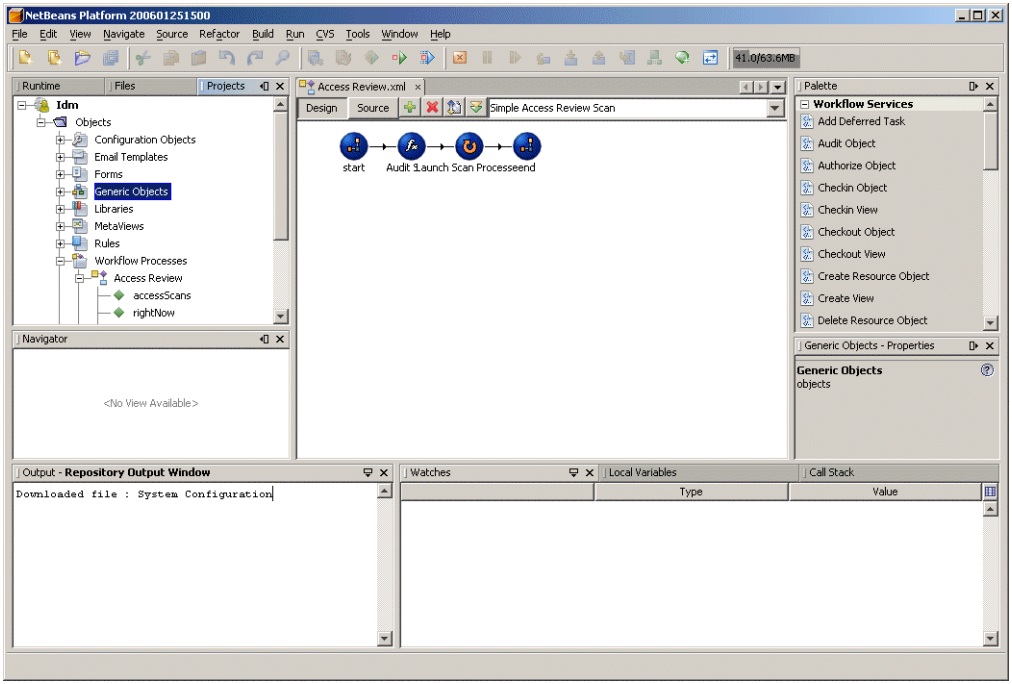
```
ui.web.user.menuLayout = 'vertical'
```

如需有關自訂使用者介面的詳細資訊，請閱讀「Identity Manager Technical Deployment Overview」。

Identity Manager IDE

Sun 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視圖。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 Identity Manager 中定義的用於確定工作流程運作方式的規則。下圖顯示了 IDE 介面。

圖 2-3 Sun Identity Manager IDE 介面



如需有關 IDE 以及使用其處理 Identity Manager 表單和工作流程的更多資訊，請參閱 「Identity Manager Workflows, Forms, and Views」。

如果您已與舊版 Identity Manager 一並安裝了業務程序編輯器 (BPE)，則也可以使用業務程序編輯器來進行自訂。

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 [Help] 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 **[Help]** 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 2-4 所示。

圖 2-4 [Help] 按鈕（位於 Identity Manager interface）

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

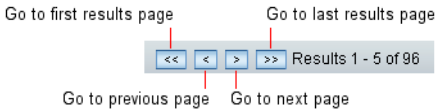
尋找資訊

使用 [Help] 視窗的搜尋功能可以找到包含在 Identity Manager 說明和文件中的主題和資訊。若要搜尋線上文件，請執行以下程序：

1. 在搜尋區域中輸入一個或多個字詞。
2. 選取搜尋兩個文件類型中的一個。依預設，該功能搜尋線上說明。
   - **[Online Help]** — 通常，線上資訊提供一些步驟，可協助您執行作業或完成表單。
   - **[Documentation]**（指南）— Identity Manager 指南主要提供有助於您理解概念和系統物件的資訊以及完整的參考資訊。
3. 按一下 **[Search]**。

搜尋將傳回連結的搜尋結果。使用 **[Previous]/[Next]** 或 **[First]/[Last]** 按鈕可以遍覽列出的結果，如 圖 2-5 所示。

圖 2-5 搜尋結果瀏覽



按一下 **[Reset]** 可以清除 [Help] 視窗中的內容。

搜尋運作方式

如果搜尋多個詞，則搜尋功能將傳回包含某一詞、所有詞和變體的結果。

例如，如果輸入以下搜尋條件：

```
resource adapter
```

則傳回的結果將包含以下詞的相符項：

- `resource` (和變體)
- `adapter` (和變體)
- `resource` 和 `adapter` (順序不限)，中間有 0 至 *n* 個詞

但是，如果將搜尋字詞包含在引號中 (例如「resource adapter」則搜尋功能將僅傳回該片語的精確相符項。

或者，您可以使用進階查詢語法明確地包括、排除或排序查詢元素。

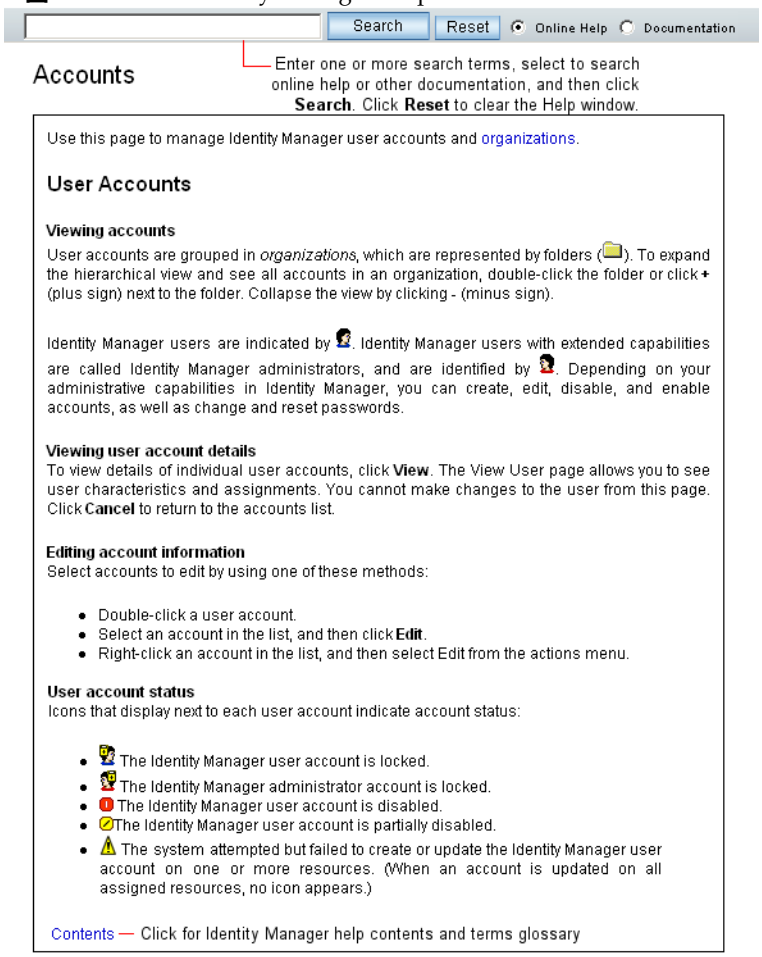
進階查詢語法

搜尋功能支援的進階查詢語法包括：

- **萬用字元符號** (? 和 *)，可讓您指定拼字式樣，而非完整的詞或片語
- **查詢運算子** (AND 或 OR)，可讓您確定如何組合查詢元素

請參閱本指南中的附錄 *B*「線上文件進階搜尋」，以取得有關 Identity Manager 進階文件搜尋功能的更多資訊。

圖 2-6 Identity Manager Help

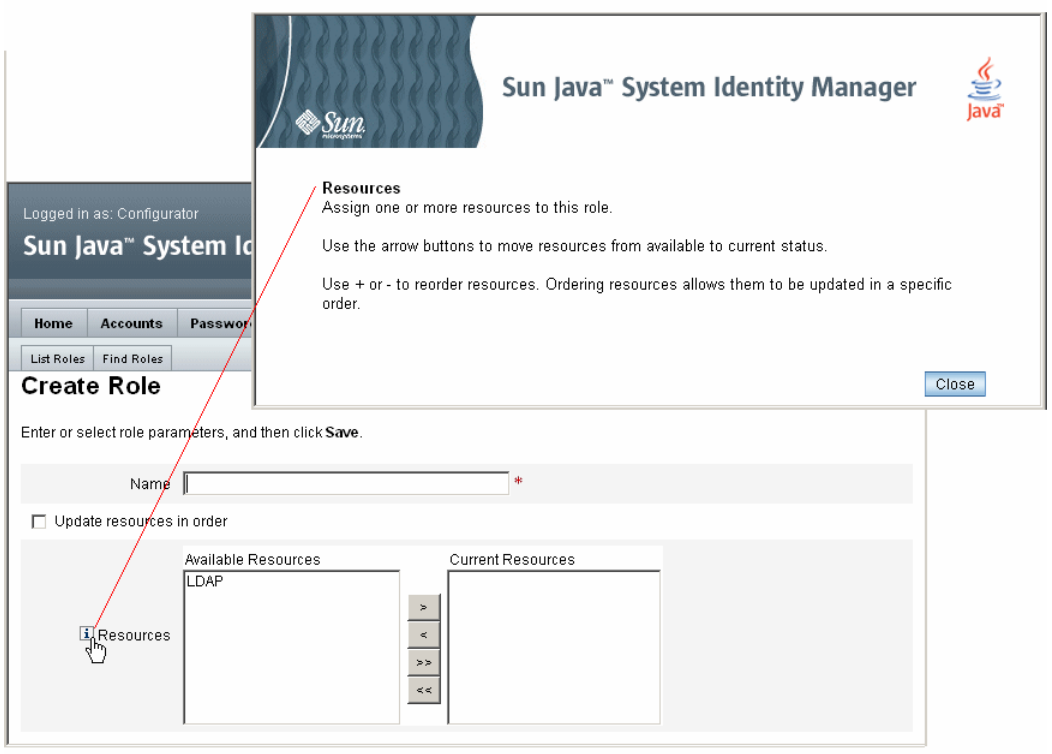


Identity Manager 指導

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。

以下符號會顯示在有指導之欄位的旁邊：。按一下此圖示可開啓一個視窗並顯示與其關聯的資訊。

圖 2-7 Identity Manager 指導



Identity Manager 作業

以下工作表提供了最常執行的 Identity Manager 工作的快速參考。它顯示您開始每項工作的主要 Identity Manager 介面位置，以及可用於執行相同工作的替代位置或方法 (如果適用)。

表 2-1 Identity Manager 介面作業參照

管理 Identity Manager 使用者		
若要執行以下動作：	**移至：**	**或：**
建立與編輯使用者	**[Accounts]** 標籤，**[List Accounts]** 選項	**[Accounts]** 標籤，**[Find Users]** 選項 ([User Account Search Results] 頁面)
核准使用者帳號建立	**[Work Items]** 標籤，**[Approvals]** 子標籤	
設定使用者驗證 (策略)	**[Security]** 標籤，**[Policies]** 選項	
變更使用者密碼	**[Passwords]** 標籤，**[Change User Password]** 選項	**[Accounts]** 標籤，**[List Accounts]** 選項 **[Accounts]** 標籤，**[Find Users]** 選項 ([User Account Search Results] 頁面) Identity Manager 使用者介面
重設使用者密碼	**[Passwords]** 標籤，**[Reset User Password]** 選項	**[Accounts]** 標籤，**[List Accounts]** 選項 **[Accounts]** 標籤，**[Find Users]** 選項 ([User Account Search Results] 頁面)
尋找使用者	**[Accounts]** 標籤，**[Find Users]** 選項	**[Passwords]** 標籤，**[Change User Password]** 選項
啟用或停用使用者	**[Accounts]** 標籤，**[List Accounts]** 選項	**[Accounts]** 標籤，**[Find Users]** 選項 ([User Account Search Results] 頁面)
解除鎖定使用者	**[Accounts]** 標籤，**[List Accounts]** 選項	**[Accounts]** 標籤，**[Find Users]** 選項 ([User Account Search Results] 頁面)
管理 Identity Manager 管理員		
若要執行這個動作：	**移至：**	
設定委託管理 (透過組織)	**[Accounts]** 標籤，**[List Accounts]** 選項，[Create User] 頁面	
指定權能	**[Accounts]** 標籤，**[List Accounts]** 選項，[Create User] 或 [Edit User] 頁面 **[Security]** 子標籤	

表 2-1 Identity Manager 介面作業參照 (繼續)

指定權能 (透過管理員角色)	**[Accounts]** 標籤，**[List Accounts]** 選項，[Create User] 或 [Edit User] 頁面 **[Security]** 子標籤
設定核准人 (以驗證帳號建立)	**[Accounts]** 標籤，**[List Accounts]** 選項，[Create Organization] 頁面 **[Roles]** 標籤，[Create Roles] 頁面
配置 Identity Manager	
若要執行這個動作：	**移至：**
建立與管理資源 (資源精靈)	**[Resources]** 標籤
管理資源群組	**[Resource]** 標籤，**[List Resource Groups]** 選項
建立與管理角色	**[Roles]** 標籤
尋找角色	**[Roles]** 標籤，**[Find Roles]** 選項
編輯權能	**[Security]** 標籤，**[Capabilities]** 選項
建立與編輯管理員角色	**[Security]** 標籤，**[Admin Roles]** 選項，[Create/Edit Admin Role] 頁面
設定電子郵件範本	**[Configure]** 標籤，**[Email Templates]** 選項
設定密碼、帳號與命名策略；指定策略至組織	**[Security]** 標籤，**[Policies]** 選項
配置身份屬性	**[Meta View]** 標籤，**[Identity Attributes]** 選項
配置身份識別事件	**[Meta View]** 標籤，**[Identity Events]** 選項
配置變更記錄檔	**[Meta View]** 標籤，**[ChangeLogs]** 選項
載入與同步化帳號與資料	
若要執行這個動作：	**移至：**
匯入資料檔案 (例如 XML 格式表單)	**[Configure]** 標籤，**[Import Exchange File]** 選項
載入資源帳號	**[Account]** 標籤，**[Load from Resource]** 選項
從檔案載入帳號	**[Account]** 標籤，**[Load from File]** 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、風險分析與報告	
若要執行這個動作：	**移至：**
設定要擷取的稽核事件並啟用稽核	**[Configure]** 標籤，**[Audit]** 選項
執行與管理報告	**[Reports]** 標籤，**[Run Reports]** 選項，以建立、執行和下載報告；**[View Reports]**，以檢視報告結果。
定義與執行風險分析報告	**[Reports]** 標籤，**[Risk Analysis]** 選項
檢視圖形報告	**[Reports]** 標籤，**[View Dashboards]** 選項

表 2-1 Identity Manager 介面作業參照 (繼續)

管理規範遵循	
若要執行這個動作：	**移至：**
定義稽核策略	**[Compliance]** 標籤，**[Manage Policies]** 選項
指定稽核策略	**[Accounts]** 標籤，**[Compliance]** 選項
管理規範遵循違規	**[My Work Items]** 標籤，**[Remediation]** 選項
設定定期存取檢閱	**[Compliance]** 標籤，**[Manage Access Scans]** 選項
監視定期存取檢閱	**[Compliance]** 標籤，**[Access Review]** 選項
檢視稽核報告	**[Reports]** 標籤，**[Auditor Report]** 類型選項
管理 Identity Manager 作業	
若要執行這個動作：	**移至：**
執行已定義的作業 (或程序)	**[Server Tasks]** 標籤，**[Run Tasks]** 選項
排程作業	**[Server Tasks]** 標籤，**[Manage Schedule]** 選項
檢視作業結果	**[Server Tasks]** 標籤，**[Find Tasks]** 或 **[All Tasks]** 選項
暫停或終止作業	**[Server Tasks]** 標籤，**[All Tasks]** 選項
管理服務提供者使用者	
若要執行這個動作：	**移至：**
管理「服務提供者」使用者	**[Accounts]** 標籤，**[Manage Service Provider Users]** 選項
管理服務提供者作業事件	**[Server Tasks]** 標籤，**[Service Provider Transactions]** 選項
配置服務提供者功能	**[Service Provider]** 標籤，**[Edit Main Configuration]** 選項
配置作業事件預設	**[Service Provider]** 標籤，**[Edit Transaction Configuration]** 選項
建立或編輯服務提供者策略	**[Security]** 標籤，**[Policies]** 選項

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，使用以下參考可引導您至想要重點瞭解的主題：

章節主題	說明
第 3 章「使用者和帳號管理」	說明介面的 [Accounts] 區域，並提供管理使用者帳號的程序。
第 4 章「配置」	說明配置作業以及如何設定 Identity Manager 物件。
第 5 章「管理」	說明如何建立與管理 Identity Manager 管理員和組織。
第 6 章「資料同步化與載入」	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 7 章「報告」	說明報告以及如何產生報告。
第 8 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 9 章「PasswordSync」	說明如何設定 PasswordSync 公用程式，以使 Windows Active Directory 和 Windows NT 網域中的密碼變更與 Identity Manager 中的變更同步。
第 10 章「安全性」	說明安全性功能以及如何使用這些功能。
第 11 章「身份識別稽核」	說明如何定義稽核策略和管理規範遵循。
第 12 章「稽核記錄」	說明稽核記錄以及稽核系統如何工作。
第 13 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「線上文件進階搜尋」	在線上說明中使用進階查詢來搜尋 Identity Manager 文件的說明。
附錄 C「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
附錄 D「Active Sync 精靈」	用於配置 7.0 之前版本的 Identity Manager 的使用中同步化。

使用者和帳號管理

本章提供透過 Identity Manager 管理員介面管理使用者的資訊與程序。您將瞭解到 Identity Manager 使用者和帳號管理工作，包括：

關於使用者帳號資料

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。總體而言，此類資訊會構成每個使用者的 Identity Manager 身份。

從管理員介面的 [Create User] 頁面 (**[Accounts]** 標籤) 來看，Identity Manager 將使用者資料歸類在四個區域中：

- 身份
- 指定

- 安全性
- 屬性

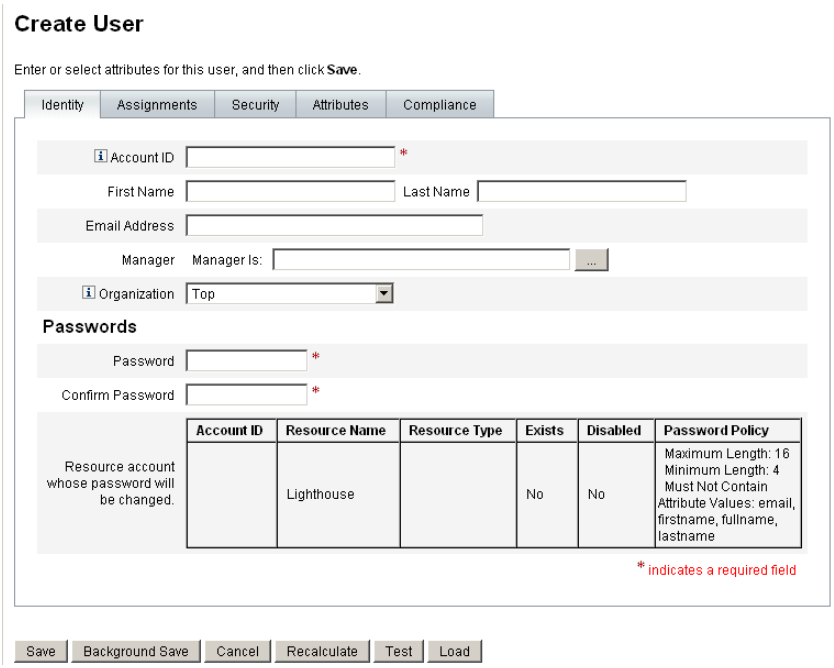
身份

[Identity] 區域定義使用者的帳號 ID、名稱、連絡人資訊、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 81 頁的「運用使用者帳號密碼」的小節。

下圖說明 [Create User] 頁面的 [Identity] 區域。

圖 3-1 建立使用者 - 身份



指定

[Assignments] 區域設定存取 Identity Manager 物件 (如資源) 的限制。

按一下 **[Assignments]** 表單標籤以設定以下指定：

- **[Identity Manager account policy** assignment] — 建立密碼和認證限制。
- **[Roles** assignment] — 概括一類使用者。角色通過間接指定來定義使用者對資源的存取。
- **[Resources and resource groups** access] — 顯示可以直接指定給使用者的可用資源和資源群組，以及不允許使用者存取的資源。這些資源補充透過角色指定間接指定給使用者的資源。

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**。您可透過以下指定，使用 [Security] 標籤爲使用者建立這些擴充的管理權能：

- **[Admin roles]** — 組合特定且唯一的權能與受控制組織集合，以對管理使用者進行協調指定。
- **[Capabilities]** — 在 Identity Manager 系統中啓用權限。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。
- **[Controlled organizations]** — 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，以及一個或多個受控制的組織。如需有關 Identity Manager 管理員的更多資訊，請參閱第 140 頁的「瞭解 Identity Manager 管理」。

- **[User Form]** — 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 **[None]**，則管理員將繼承指定給其組織的使用者表單。
- **[View User Form]** — 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 **[None]**，則管理員將繼承指定給其組織的檢視使用者表單。
- **[Delegate work items to]** — 將使用者帳號的工作項目委託給使用者的管理員、一個或多個其他使用者，或按照委託核准人規則的指定進行委託。若要停用工作項目委託，請將值設定爲 [None]。

屬性

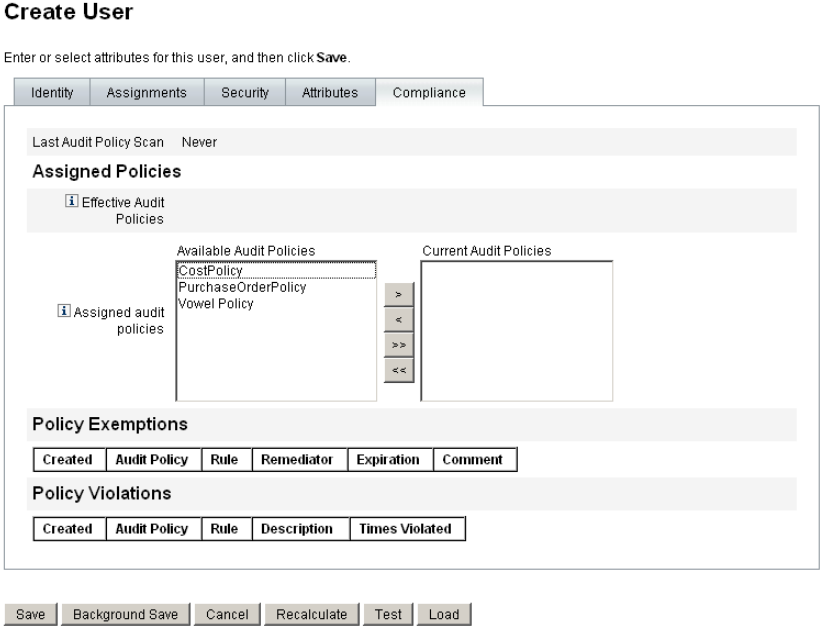
[Create User] 頁面上的 [Attributes] 標籤定義與指定資源關聯的帳號屬性。列出的屬性按指定的資源分類，具體情況根據已指定資源的不同而異。

規範遵循

[Compliance] 標籤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生效的稽核策略。您僅可以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。

此頁面還指示策略掃描、違規和豁免的目前狀態，如下圖所示 (如果適用於使用者帳號)。

圖 3-2 [Create User] 頁面 - [Compliance] 標籤



若要指定稽核策略，請從 [Available Audit Policies] 清單中將選取的策略移至 [Current Audit Policies] 清單中。

介面的 [帳號] 區域

Identity Manager 帳號區域可讓您管理 Identity Manager 使用者。若要存取此區域，請從管理員介面功能表列中選取 **[Accounts]**。

帳號清單會顯示所有的 Identity Manager 使用者帳號。帳號會被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 ([Name])、使用者姓氏 ([Last Name]) 或使用者名字 ([First Name]) 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 ([Name] 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。

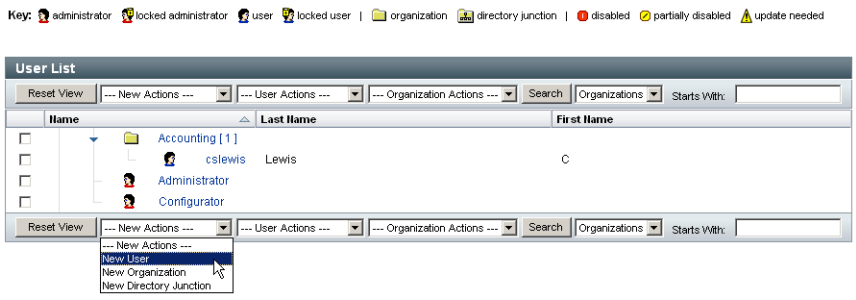
若要展開階層式視圖並察看組織中的帳號，請按一下資料夾旁邊的三角形指示器。再次按一下該指示器可以摺疊此視圖。

帳號區域中的動作清單

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

- **[New Actions]** — 建立使用者、組織和目錄結合。
- **[User Actions]** — 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。
- **[Organization Actions]** — 執行一系列組織和使用者動作。

圖 3-3 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 [Organizations] 或 [Users]，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 **[Search]**。如需有關在 [Accounts] 區域搜尋的更多資訊，請參閱第 75 頁的「尋找帳號」。

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
	Identity Manager 使用者帳號已鎖定。這意味著使用者因不成功的登入嘗試超過為資源建立的限制而鎖定在資源帳號之外。
	Identity Manager 管理員帳號已鎖定。
	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。)
	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。)

運用使用者帳號

在管理員介面的 [Accounts] 區域，您可以對以下系統物件執行一系列動作：

- **[Users]** — 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
- **[Passwords]** — 變更和重設
- **[Organizations]** — 針對組織成員建立、編輯、重新整理和執行使用者動作。
- **[Directory Junctions]** — 建立

使用者

本小節中主題的重點在於管理使用者帳號。如需有關 Identity Manager 組織和建立目錄結合的更深入說明，請參閱第 5 章「管理」

檢視

若要檢視使用者帳號詳細資訊，請在清單中選取使用者，然後從 [User Actions] 清單中選取 **[View]**。

[View User] 頁面顯示編輯或建立使用者時所選身份、指定、安全性和屬性資訊的子集。無法編輯 [View User] 頁面上的資訊。按一下 **[Cancel]** 以返回至 [Accounts] 清單。

建立 ([New Actions] 清單、[New User] 選項)

若要建立使用者帳號，請從 [New Actions] 清單中選取 **[New User]**。如果您要在組織中 (而非頂層) 建立使用者，請選取組織資料夾，然後從 [New Actions] 清單中選取 **[New User]**。

在一個區域可選擇之選項可能取決於您在另一個區域中所做的選擇。

[Create User] 頁面 (由**使用者表單定義**) 可讓您爲使用者帳號設定以下項目：

- **[Identity]** — 名稱、電子郵件、組織和密碼詳細資訊
- **[Assignments]** — 帳號策略、角色和資源
- **[Security]** — 組織與權能
- **[Attributes]** — 已指定資源的特定屬性

若要更好地反映您的業務程序或特定管理員權能，您可以針對您的環境專門配置使用者表單。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」。

按一下 [Create User] 頁面上的標籤可以在建立使用者設定中瀏覽。您可以依任何順序在標籤中移動。完成選取後，您可以使用兩個選項來儲存使用者帳號：

- **[Save]** — 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。
- **[Background Save]** — 此程序以背景工作的方式儲存使用者帳號，這讓您可以繼續使用 Identity Manager。對於每個執行中的儲存工作，[Accounts] 頁面、[Find User Results] 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。

建立多個使用者帳號（身份）

您可以在單一資源上建立一個或多個使用者帳號。建立 (或編輯) 使用者並爲使用者指定一個或多個資源時，您也可在該資源上請求和定義附加帳號。

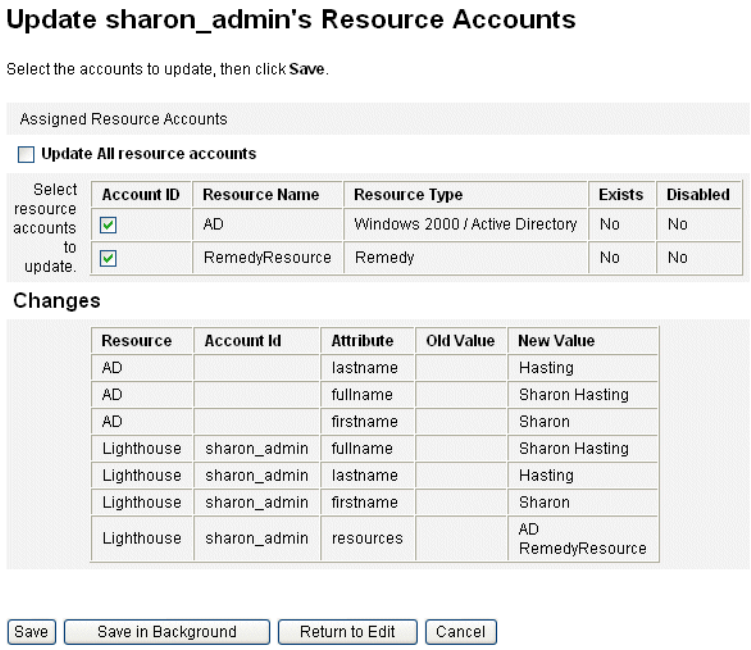
編輯

若要編輯帳號資訊，請選擇以下任一動作：

- 按一下帳號清單中的使用者帳號。
- 在清單中選取使用者帳號，然後從 [User Actions] 清單中選取 **[Edit]**。

建立與儲存變更後，Identity Manager 會顯示 [Update Resource Accounts] 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。選取 **[Update All resource accounts]** 以將變更套用至所有已指定的資源；或分別選取無、一個或多個與要更新之使用者關聯的資源帳號。

圖 3-4 編輯使用者 (更新資源帳號)



再按一下 **[Save]** 以完成編輯作業，或按一下 **[Return to Edit]** 以建立更進一步的變更。

移動使用者 ([User Actions])

[Change Organization of User] 工作可讓您從目前指定的組織中移除使用者，然後將使用者重新指定給或移動至新組織。

若要將使用者移至其他組織，請在清單中選取一個或多個使用者帳號，然後從 [User Actions] 清單中選取 **[Move]**。

重新命名 ([User Actions])

一般而言，重新命名資源上的帳號是一個複雜的動作。因爲這個原因，Identity Manager 提供一個單獨功能，可重新命名使用者的 Identity Manager 帳號，或一個或多個與該使用者關聯的資源帳號。

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 [User Actions] 清單中選取 **[Rename]** 選項。

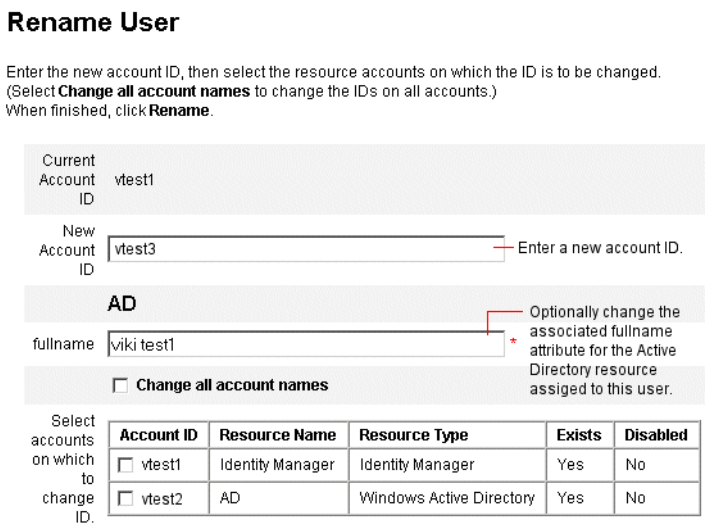
[Rename User] 頁面可讓您變更使用者帳號名稱、關聯的資源帳號名稱以及與使用者的 Identity Manager 帳號關聯的資源帳號屬性。

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 3-5 重新命名使用者



停用使用者（使用者動作、組織動作）

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

備註 對於不支援帳號停用的指定資源，將藉由指定隨機產生的密碼來停用使用者帳號。

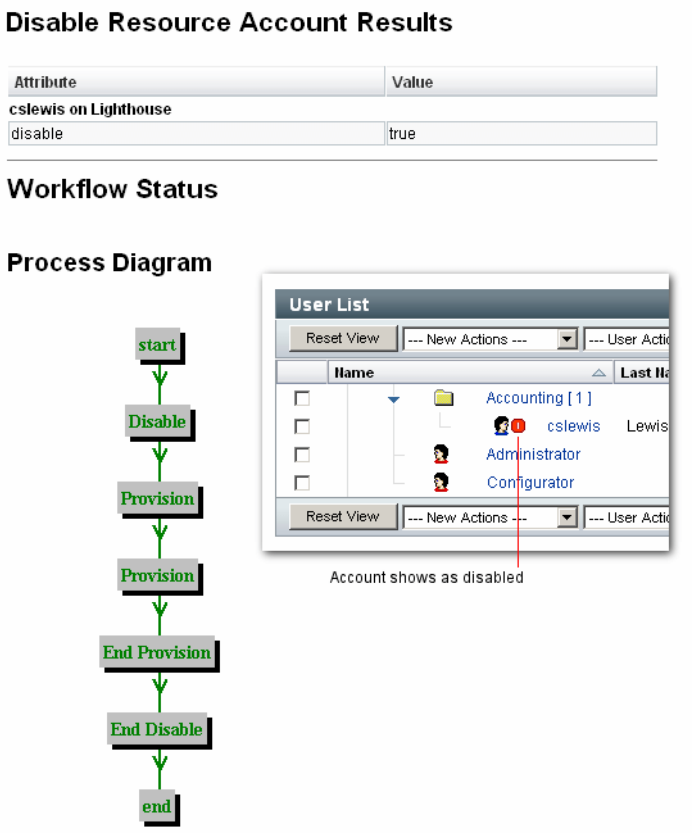
停用單一使用者帳號

若要停用使用者帳號，請在清單中選取此帳號，然後從 [User Actions] 清單中選取 **[Disable]**。

在顯示的 [Disable] 頁面上，選取要停用的資源帳號，然後按一下 **[OK]**。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。

圖 3-6 說明了 [Disable] 頁面上已停用的帳號。

圖 3-6 已停用的帳號



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 [User Actions] 清單中選取 **[Disable]**。

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 ([User Actions]、[Organization Actions])

使用者帳號啓用與停用程序相反。對於不支援帳號啓用的資源，Identity Manager 會產生新的隨機密碼。根據選取的通知選項，也會在管理員的結果頁面上顯示該密碼。

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。

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 [User Actions] 清單中選取 **[Enable]**。

在顯示的 [Enable] 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 [User Actions] 清單中選取 [Enable]。

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。

更新使用者 ([User Actions]、[Organization Actions])

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 [Find User] 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

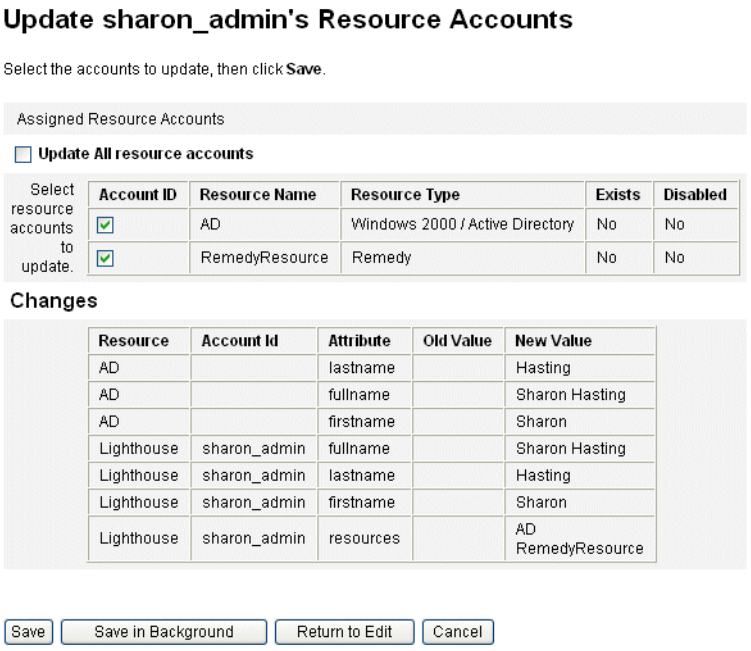
若要更新使用者帳號，請在清單中選取此帳號，然後從 [User Actions] 清單中選取 **[Update]**。

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 **[Update All resource accounts]** 以更新所有已指定的資源帳號。完成後，按一下 **[OK]** 以開始更新程序。或者，按一下 **[Save in Background]** 以作爲後台程序執行該動作。

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。在圖中，Lighthouse 參照 Identity Manager。

圖 3-7 更新資源帳號



更新多個帳號

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 [User Actions] 清單中選取 **[Update]**。

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。

解除鎖定使用者 ([User Actions]、[Organization Actions])

因爲使用者登入重試次數已超過爲該資源建立的登入限制，所以可能將該使用者鎖定在一個或多個資源帳號之外。使用者的有效 Lighthouse 帳號策略建立密碼或問題登入嘗試可以失敗的最大次數。

當使用者因超過密碼登入嘗試失敗的最大次數而鎖定時，將不允許其進行任何 Identity Manager 應用程式介面 (包括使用者介面、管理員介面、[Forgot My Password]、Identity Manager IDE、SOAP 和主控台) 認證。如果使用者因超過問題登入嘗試失敗的最大次數而鎖定，則他可以對除 [Forgot My Password] 以外的任何 Identity Manager 應用程式介面進行認證。

密碼登入嘗試失敗

如果因密碼登入嘗試失敗而鎖定，使用者帳號將保持鎖定狀態，直到：

- 管理使用者爲其解除鎖定。若要成功解除鎖定帳戶，必須爲管理員指定解除鎖定使用者功能，並且管理員必須具有使用者成員組織的管理控制。
- 目前日期與時間晚於使用者的鎖定過期日期與時間 (若鎖定過期日期與時間已設定)。([Lihthouse Account Policy] 中的 [Lock Timeout] 值可以設定鎖定過期時間。)

問題登入嘗試失敗

如果因超過問題登入嘗試失敗的最大次數而鎖定，則使用者帳號將保持鎖定狀態，直到發生以下任一動作：

- 管理使用者爲其解除鎖定。若要成功解除鎖定帳戶，必須爲管理員指定解除鎖定使用者功能，並且管理員必須具有使用者成員組織的管理控制。
- 已鎖定的使用者或具有相應權能的使用者可以變更或重設使用者的密碼。

具有相應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

處於鎖定狀態的使用者無法登入任何 Identity Manager 應用程式，包括管理員介面、使用者介面和 Identity Manager IDE。使用者無論透過提供使用者 ID 和認證問題的答案，還是透過一個或多個資源通路來嘗試使用其 Identity Manager 使用者 ID 和密碼登入，此限制都適用。

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 [User Actions] 或 [Organization Actions] 清單中選取 [Unlock Users]。

刪除 (使用者動作、組織動作)

刪除動作包括從資源移除 Identity Manager 使用者帳號存取的多個選項：

- **[Delete]** — 對於選取的每個資源，Identity Manager 會刪除關聯的資源帳號。也會解除 Identity Manager 使用者與選取資源的連結。
- **[Unassign]** — 對於選取的每個資源，Identity Manager 會從使用者的已指定資源清單中移除關聯的資源。也會解除使用者與選取資源的連結。相關的資源帳號不會被刪除。
- **[Unlink]** — 對於選取的每個資源，Identity Manager 會從 Identity Manager 使用者中移除關聯的資源帳號資訊。

備註 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。

若要開始刪除動作，請選取使用者帳號，然後在 [User Actions] 或 [Organization Actions] 清單中選取相應的刪除動作。

Identity Manager 顯示 [Delete Resource Accounts] 頁面。

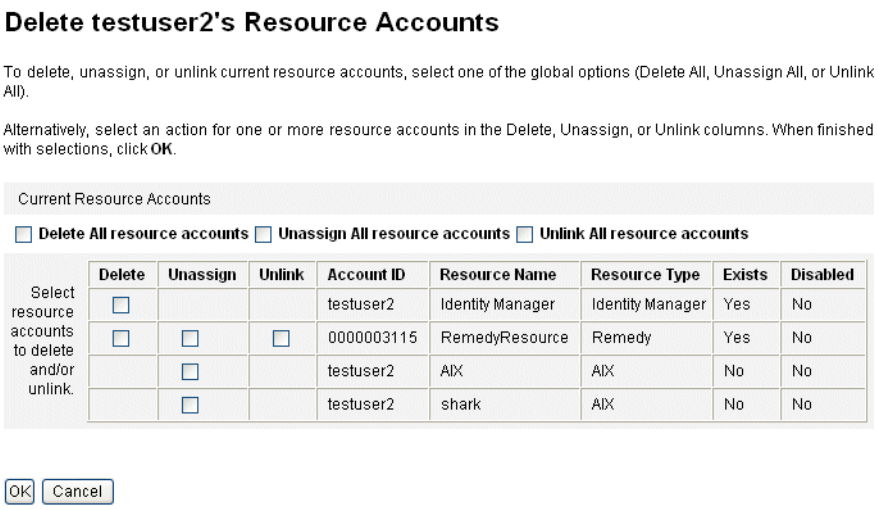
刪除 「使用者帳號」與 「資源帳號」

若要刪除 Identity Manager 使用者帳號或資源帳號，請在 [Delete] 欄位中進行選取，然後按一下 **[OK]**。若要刪除全部資源帳號，請選取 [Delete All resource accounts] 選項，然後按一下 **[OK]**。

取消指定或取消連結資源帳號

若要從 Identity Manager 使用者帳號取消指定或解除連結資源帳號，請在 [Unassign] 或 [Unlink] 欄位中進行個別選擇，然後按一下 **[OK]**。若要取消指定全部資源帳號，請選取 [Unassign All resource accounts] 或 [Unlink All resource accounts] 選項，然後按一下 **[OK]**。

圖 3-8 刪除「使用者帳號」與「資源帳號」



密碼

您可以使用 [User Actions] 中的 **[Change Password]** 和 **[Reset Password]** 來呼叫 [Edit User] 頁面及變更或重設所選使用者的使用者密碼。另請參閱第 81 頁的「運用使用者帳號密碼」。

尋找帳號

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 **[Accounts]**，然後選取 **[Find Users]**。您可按下列一個或多個搜尋類型來搜尋帳號：

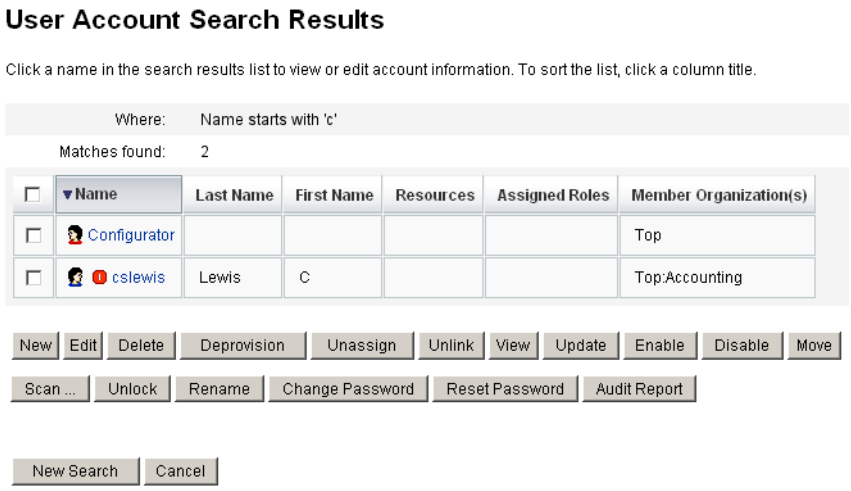
- 帳號詳細資訊，例如使用者名稱、電子郵件帳號，或姓氏、名字。這些選項取決於您組織所特有的 Identity Manager 實作。
- 使用者的管理員。

- 資源帳號狀態，包括：
  - **[Disabled]** — 使用者不能存取任何 Identity Manager 或指定的資源帳號。
  - **[Partially Disabled]** — 使用者不能存取一個或多個指定的資源帳號。
  - **[Enabled]** — 使用者擁有對所有已指定資源帳號的存取權。
- 使用者帳號狀態，包括：
  - **[Locked]** — 因密碼或問題登入嘗試失敗的最大次數超過允許的最大次數，使用者帳號鎖定。
  - **[Not Locked]** — 未限制使用者帳號存取
- 更新狀態，包括：
  - **[no]** — 尚未對任何資源進行更新的使用者帳號。
  - **[some]** — 已對至少一個 (但非所有) 指定的資源進行更新的使用者帳號。
  - **[all]** — 已對所有指定的資源進行更新的使用者帳號。
- 指定的資源
- 角色
- 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 **[Edit]**。
- 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 3-9 使用者帳號搜尋結果



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：

- **[Delete]** — 刪除、取消指定和解除連結所有選取的資源帳號。選取 [Target the Identity Manager Account] 選項可刪除每一位使用者的 Identity Manager 帳號。
- **[Delete and Unlink]** — 刪除所有選取的資源帳號，並取消帳號與使用者的連結。
- **[Disable]** — 停用所有選取的資源帳號。選取 [Target the Identity Manager Account] 選項可停用每個使用者的 Identity Manager 帳號。
- **[Enable]** — 啓用所有選取的資源帳號。選取 [Target the Identity Manager Account] 選項可啓用每個使用者的 Identity Manager 帳號。
- **[Unassign, Unlink]** — 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。
- **[Unlink]** — 移除資源帳號與 Identity Manager 使用者帳號的關聯 (連結)。解除連結不會從資源中移除該帳號。如果您解除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。在**帳號**標籤的 [Find Users] 頁面上搜尋使用者。

作業完成後顯示作業結果時，按一下 **[Download 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

若要啓動批次處理動作，請選取或輸入值，然後按一下**啟動**。Identity Manager 會啓動後台工作以執行批次處理動作。

若要監視批次處理動作的作業狀態，請前往 **[Tasks]** 標籤，再按一下作業連結。

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與更新動作。

CSV 格式包含兩個或多個輸入行。每行包含一份以逗點分隔的值清單。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：

- **[user]** — 包含 Identity Manager 使用者的名稱。
- **[command]** — 包含對 Identity Manager 使用者採取的動作。有效的指令有：
  - **[Delete]** — 刪除、取消指定與取消連結資源帳號、Identity Manager 帳號或二者。
  - **[DeleteAndUnlink]** — 刪除與取消連結資源帳號。
  - **[Disable]** — 停用資源帳號、Identity Manager 帳號或二者。
  - **[Enable]** — 啓用資源帳號、Identity Manager 帳號或二者。
  - **[Unassign]** — 取消指定與解除連結資源帳號。
  - **[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 [resources]。使用資源欄位可指定哪些資源上的哪些帳號將受影響。它可有下列值：

- **[all]** — 處理所有資源帳號 (包括 Identity Manager 帳號)。
- **[resonly]** — 處理 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 [user] 與 [command] 欄位外，還可以指定 [User View] 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]** — 要指定給 Identity Manager 帳號的一個或多個角色名稱清單。
- **[waveset.resources]** — 要指定給 Identity Manager 帳號的一個或多個資源名稱清單。
- **[waveset.applications]** — 要指定給 Identity Manager 帳號的一個或多個角色名稱清單。
- **[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,
accounts[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) 來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]** — 將目前值換成指定的值。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]** — 將指定值增加到目前值。系統將篩選出重複值。
- **[Remove]** — 從目前值移除指定值。
- **[List]** — 以處理多值的方式強制處理欄位的值，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

如果您的欄位值中有逗號 (,) 或雙引號 (") 字元，或想要保留前導或結尾的空格，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 [User Form] 中參考這些屬性，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***]** — 僅會針對爲其指定了指令的那些欄位定義這些屬性此值爲指示字串。
- **[waveset.bulk.abort]** — 將這個布林屬性設爲 true，以中斷目前動作。
- **[waveset.bulk.abortMessage]** — 將此屬性設爲訊息字串，以便在 waveset.bulk.abort 設爲 true 時顯示。若未設定此屬性，則會顯示一般中斷訊息。

運用使用者帳號密碼

所有 Identity Manager 使用者皆有指定的密碼。Identity Manager 使用者密碼設定後，用於同步化該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)，則可分別設定它們。

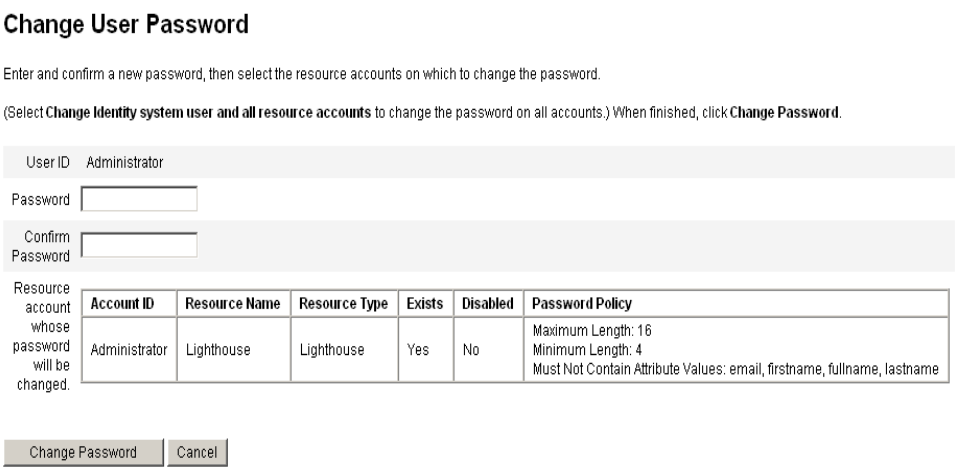
變更使用者帳號密碼

若要變更使用者帳號密碼：

1. 在功能表列中，選取 **[Passwords]**。

   依預設，會顯示 [Change User Password] 頁面，如下圖所示。

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 **[Find]**，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 [Change User Password] 頁。
4. 輸入並確認新密碼資訊，然後按一下 **[Change Password]** 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。

重設使用者帳號密碼

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 [Reset Notification Option]，Identity Manager 會使用電子郵件傳送新密碼給使用者，或 (在 [Results] 頁面) 將其顯示給要求重設的 Identity Manager 管理員。

重設時密碼過期

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，從而根據與使用者相關的 [Lighthouse Account Policy] 中設定的過期密碼策略而確定讓使用者密碼是否過期。

例如，在 [Reset User Password] 中，您會將 `resourceAccounts.currentResourceAccounts[Lighthouse].expirePassword` 設爲 `false` 值。

在 [Lighthouse Account Policy] 的 [Reset Option] 欄位中，有兩種密碼過期方法：

- **[permanent]** — 當重設密碼時，會使用在 passwordExpiry 策略屬性中指定的時期計算出相對於目前日期的密碼過期日期，然後爲使用者設定此日期。如果沒有指定值，則變更或重設的密碼將永不過期。
- **[temporary]** — 當重設密碼時，會使用在 tempPasswordExpiry 策略屬性中指定的時期計算出相對於目前日期的密碼過期日期，然後爲使用者設定此日期。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。

  只在重設密碼時 (隨機變更)，才會套用 `tempPasswordExpiry` 屬性；此屬性不會套用至密碼變更。

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，請從功能表列中選取 **[Security]**，然後選取 **[Policies]**。

若要編輯密碼策略，請在 [Policies] 清單中選取密碼策略。若要建立密碼策略，請從 [New] 選項清單中選取 **[String Quality Policy]**。

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，您需要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：

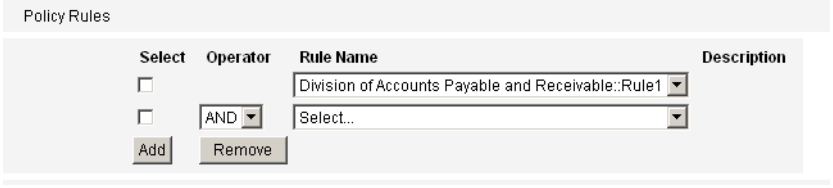
- 字母、數字、大寫、小寫與特殊字元的最小與最大數目
- 內嵌數字字元的最小與最大數目
- 重複與循序字元的最多數目
- 開始字母與數字字元的最少數目

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。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 [Policies] 頁面配置字典。如需有關如何設定字典的詳細資訊，請閱讀 Identity Manager 部署工具中標題爲「Configuring Dictionary Support」的一章。

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 [Number of Previous Passwords that Cannot be Reused] 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 [Maximum Number of Similar Characters from Previous Passwords that Cannot be Reused] 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。

如果輸入值爲 0，則不論順序如何，所有字元都必須不同。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。

此規則可套用至一或多個舊密碼上。所檢查的舊密碼數就是 [Number of Previous Passwords that Cannot be Reused] 欄位中所指定的數字。

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 128 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：

- 帳號 ID
- email
- firstname
- fullname

- lastname

您可以在 UserUIConfig 配置物件中變更密碼允許的「不得包含」屬性集。UserUIConfig 中的密碼屬性列示在 <PolicyPasswordAttributeNames> 中。

執行密碼策略

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 [Password Policy] 選項清單中將其選取，該清單位於「建立或編輯資源精靈」的 [Policy Configuration] 區域：[Identity Manager Parameters] 頁面。

使用者認證

若使用者忘記其密碼或其密碼被重設，則可以回答一個或多個帳號認證問題以存取 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 [Create and Edit User] 頁面)。

在帳號策略中設定認證：

1. 從功能表列中選取 **[Security]**，然後選取 **[Policies]**。
2. 從策略清單中選取 [Default Lighthouse Account Policy]。

   在頁面的 [Secondary Authentication Policy Options] 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 Identity Manager 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。

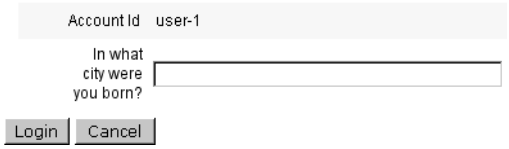
根據認證規則設定，您可以要求使用者回答：

- 全部認證問題
- 任何一個認證問題
- 隨機從問題集選取的問題；問題數目由您指定的值決定
- 從問題集中依序選取的一個或多個問題

您可以驗證您的認證選擇，方法爲登入 Identity Manager 使用者介面，按一下 [Forgot Your Password?]，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

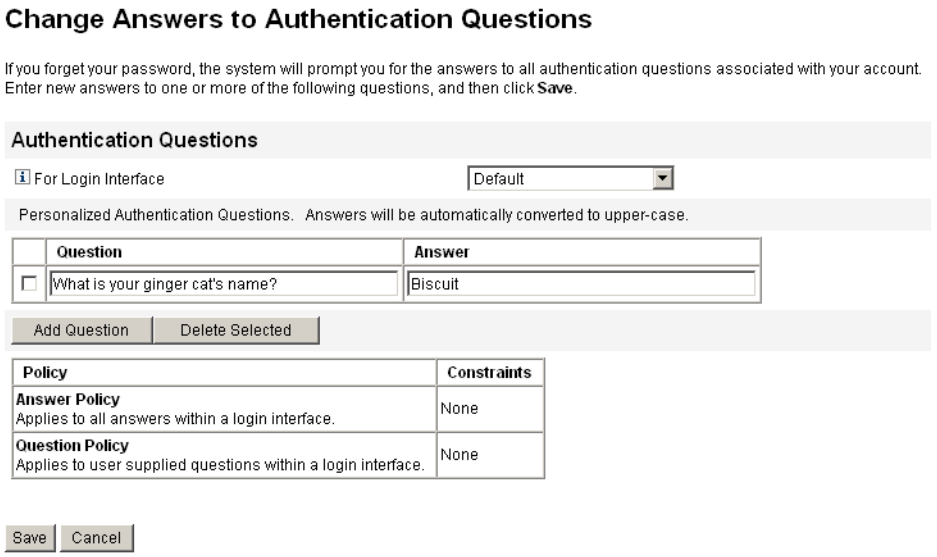


個性化的認證問題

在 Lighthouse 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大數目。

然後，使用者可在 [Change Answers to Authentication Questions] 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 變更回答 — 個性化的認證問題



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。

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：

代碼範例 3-1 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：

代碼範例 3-2 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：

- [Admin Roles] — 具有指定的管理員角色的使用者會繼承該角色定義的權能和受控制組織。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「配置 Identity Manager 資源」。
- [Capabilities] — 權能由規則定義。Identity Manager 提供了幾組分組爲功能權能的權能，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 5 章中的「瞭解與管理權能」。
- [Controlled organizations] — 受控制的組織可爲指定組織授予管理控制權限。如需更多資訊，請參閱第 5 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 5 章 「管理」。

使用者自我探索

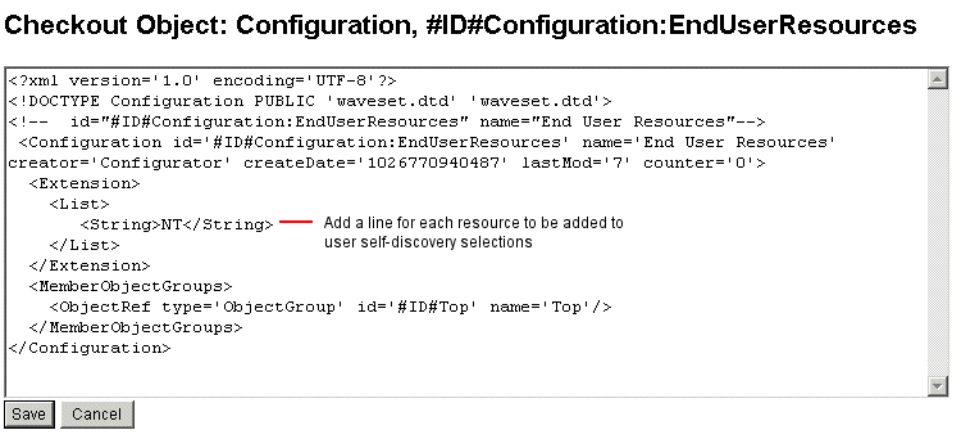
Identity Manager 使用者介面可讓使用者**探索**資源帳號。這表示具有 Identity Manager 身份的使用者可與現有的但無關聯的資源帳號相關聯。

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。若要執行此作業，請執行以下步驟：

1. 開啓 Identity Manager [System Settings] 頁 (`idm/debug`)。
2. 從 [Configuration] 類型清單中選取 **[Configuration]**，然後按一下 **[List Objects]**。
3. 按一下 [End User Resources] 旁的 **[Edit]** 來顯示配置物件。
4. 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



5. 按一下 **[Save]**。

啓用自我探索後，會透過 Identity Manager 使用者介面上的新功能表項目 ([Inform Identity Manager of Other Accounts]) 表示使用者。此區域允取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。

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評估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)
- 字串元素清單 (各個使用者名稱或 ID)
- WSAttribute 元素清單
- AttributeCondition 元素清單

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。在 Identity Manager `UserUIConfig` 物件中會將它們配置爲 `QueryableAttrNames`。

在延伸屬性上進行相互關聯需要特殊配置：

- 必須在 `UserUIConfig` 中將延伸屬性指定爲可查詢 (增加至 `QueryableAttrNames` 清單)。
- Identity Manager 應用程式 (或應用程式伺服器) 可能需要重新啓動，才能使 `UserUIConfig` 變更生效。

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布林值 true；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可選擇第二階段，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評估的檢查)。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。

章節 4

配置

本章提供有關使用管理員介面設定 Identity Manager 物件和伺服器程序的資訊和程序。如需有關 Identity Manager 物件的更多資訊，請參閱簡介一章中的第 34 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 13 章 「服務提供者管理」

本章包含以下主題：

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。

角色是甚麼？

Identity Manager 角色可定義管理帳號之資源的集合。角色可讓您設定使用者的類別，將具有類似特性的 Identity Manager 使用者進行分組。

您可以指定每個使用者到一個或多個角色，或者不指定爲任何角色。指定到一個角色的所有使用者會分享相同資源基礎群組的存取權。

與角色相關的所有資源均被**間接**指定給使用者。間接指定不同於**直接**指定，在直接指定中，資源是爲使用者特別選取的。

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。

您可透過 [Administrator Interface] 的 [Create and Edit User] 頁面將角色指定給使用者。

建立角色

您可以使用以下任一方法建立角色：

1. 從 Identity Manager 功能表列中，選取 **[Roles]**。
2. 在 [Roles] 頁面中，按一下 **[New]**。

   [Create Role] 頁面可讓您：

   - 將資源和資源群組指定給角色。
   - 選取角色核准人並進行通知選擇。

提示 若要瞭解有關核准程序的更多資訊，請參閱第 180 頁的「帳號核准」。

   - 排除角色。這表示如果將此角色指定給一個使用者，則排除的角色可能也不會被指定。

- 選取可將此角色指定到的組織。
- 編輯指定給角色之資源的屬性值。

編輯指定的資源屬性值

在 [Create Role] 頁面上的 [Assigned Resources] 區域按一下 **[Set Attribute Values]** 可顯示指定給角色的每一資源的屬性清單。在此 [Edit] 屬性頁面中，您可以指定每個屬性的新值並決定如何設定屬性值。Identity Manager 可讓您直接設定值或使用規則設定值，也提供置換或合併現有值的一組選項。

選取用於建立各資源帳號屬性值的選項：

- **[Value override]** — 選取以下某個選項：
  - **[None]** — 預設的選項。未建立任何值。
  - **[Rule]** — 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。
  - **[Text]** — 使用指定文字來設定值。如果您選取此選項，則必須輸入文字。
- **[How to set]** — 選取以下任一選項：
  - **[Default value]** — 將規則或文字設定爲預設屬性值。使用者可以變更或置換該值。
  - **[Set to value]** — 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。
  - **[Merge with value]** — 將目前的屬性值與規則或文字所指定的值合併。
  - **[Merge with value, clear existing]** — 移除目前的屬性值，並將值設定爲此角色和其他指定角色所指定值的合併值。
  - **[Remove from value]** — 移除屬性值中由規則或文字所指定的值。
  - **[Authoritative set to value]** — 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。
  - **[Authoritative merge with value]** — 將目前的屬性值與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，指示其包含逗號分隔值 (CSV) 字串；例如：

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

- **[Authoritative merge with value, clear existing]** — 移除目前的屬性值，並將值設定爲此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，即使該屬性先前具有相應值。

- **[Rule Name]** — 如果您在 [Value override] 區域中選取 [Rule]，請從清單中選取規則。
- **[Text]** — 如果您在 [Value override] 區域中選取 [Text]，請輸入要增加至屬性值、自屬性值中刪除或做爲屬性值的文字。

按一下 **[OK]** 儲存變更，並返回 [Create Role] 或 [Edit Role] 頁面。

管理角色

您可以對 [Roles] 頁面上角色清單中的角色執行一系列動作。

- [Edit roles] — 在角色清單中選取角色，並在開啓的頁面中修改角色的屬性。
- [Find roles] — 在 [Roles] 區域選取 **[Find roles]**。您可以按以下的一或多個搜尋類型來搜尋角色：
  - 名稱
  - 可用性
  - 核准人
  - 資源
  - 資源群組

如果您選取多個搜尋類型，則搜尋必須符合所有指定條件才能順利傳回結果。搜尋並不區分大小寫。

- [Clone or rename a role] — 選取要編輯的角色，在 [Name] 欄位中輸入新的名稱，然後按一下 **[Save]**。在顯示的頁面中，按一下 **[Create]** 以建立新角色。

重新命名角色

若要重新命名角色，請執行以下步驟：

1. 選取要編輯的角色。
2. 在 [Name] 欄位中輸入新的名稱，然後按一下 **[Save]**。

   Identity Manager 顯示 [Create or Rename] 頁面。
3. 按一下 **[Renam]** 變更角色名稱。

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。依照預設，在進行同步時，資源將被指定給角色。角色可以是作業所建立的角色，也可以是符合其中一個資源角色名稱的現有 Identity Manager 角色。

在功能表列中，選取 **[Tasks]**，然後選取 **[Run Tasks]** 標籤，以存取 [Synchronize Identity System Roles with Resource Roles] 作業頁面。若要啓動作業，請指定同步化作業的名稱、資源、要使用的資源角色屬性以及將套用角色的組織，然後按一下 [Launch]。

配置 Identity Manager 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戶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 [Resources] 頁中現有資源的資訊。

若要存取資源，請選取功能表列上的 **[Resources]**。

資源依照類型分組，在清單中以命名的資料夾表示。若要展開階層式視圖並查看目前定義的資源，請按一下資料夾旁邊的指示器。再次按一下該指示器可以摺疊此視圖。

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啓動管理作業：

- **[Resource Actions]** — 在資源上執行一系列動作，包括編輯、啓動同步化、重新命名與刪除；還包括處理資源物件和管理資源連線。
- **[Resource Object Actions]** — 編輯、建立、刪除、重新命名、另存新檔與尋找資源物件。
- **[Resource Type Actions]** — 編輯資源策略、處理帳號索引和配置受管理的資源。

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

您可以從清單中選取要建立的資源，該清單透過管理員介面的 [Resources] 標籤進行管理。從 [Resource Type Actions] 選項清單中選取 [Configure Managed Resources]，來選擇要寫入資源清單的資源。

在 [Managed Resources] 頁面中，Identity Manager 將資源劃分爲兩類：

- **[Identity Manager Resources]** — 此表格中包括的資源是最常由 Identity Manager 管理的資源。此表格顯示資源類型及版本。藉由在 [Managed?] 欄中選取選項來選擇一個或多個資源，然後按一下 **[Save]** 將其增加到 [Resources] 清單。
- **[Custom resources]** — 使用此頁面區域可將自訂資源增加到 [Resources] 清單中。

若要增加自訂資源，請：

1. 按一下 **[Add Custom Resource]**，在表格中新增一列。
2. 輸入資源的資源類別路徑，或輸入您自訂開發的資源。
3. 按一下 **[Save]** 將資源新增到 [Resources] 清單。

表 4-1 列出了自訂資源類別。

表 4-1 自訂資源類別

自訂資源	資源類別
Access Manager	com.waveset.adapter.AccessManagerResourceAdapter
ACF2	com.waveset.adapter.ACF2ResourceAdapter
ActivCard	com.waveset.adapter.ActivCardResourceAdapter
Active Directory	com.waveset.adapter.ADSIResourceAdapter
Active Directory Active Sync	com.waveset.adapter.ActiveDirectoryActiveSyncAdapter
ClearTrust	com.waveset.adapter.ClearTrustResourceAdapter
DB2	com.waveset.adapter.DB2ResourceAdapter
INISafe Nexess	com.waveset.adapter.INISafeNexessResourceAdapter
Microsoft SQL Server	com.waveset.adapter.MSSQLServerResourceAdapter
MySQL	com.waveset.adapter.MySQLResourceAdapter
Natural	com.waveset.adapter.NaturalResourceAdapter
NDS SecretStore	com.waveset.adapter.NDSSecretStoreResourceAdapter
Oracle	com.waveset.adapter.OracleResourceAdapter
Oracle Financials	com.waveset.adapter.OracleERPResourceAdapter
OS400	com.waveset.adapter.OS400ResourceAdapter
PeopleSoft	com.waveset.adapter.PeopleSoftCompIntfcAdapter com.waveset.adapter.PeopleSoftComponentActiveSyncAdapter
RACF	com.waveset.adapter.RACFResourceAdapter
SAP	com.waveset.adapter.SAPResourceAdapter
SAP HR	com.waveset.adapter.SAPHRResourceAdapter
SAP Portal	com.waveset.adapter.SAPPortalResourceAdapter
Scripted Host	com.waveset.adapter.ScriptedHostResourceAdapter
SecurID	com.waveset.adapter.SecurIdResourceAdapter com.waveset.adapter.SecurIdUnixResourceAdapter
Siebel	com.waveset.adapter.SiebelResourceAdapter
SiteMinder	com.waveset.adapter.SiteminderAdminResourceAdapter com.waveset.adapter.SiteminderLDAPResourceAdapter com.waveset.adapter.SiteminderExampleTableResourceAdapter
Sun ONE Identity Server	com.waveset.adapter.SunISResourceAdapter
Sybase	com.waveset.adapter.SybaseResourceAdapter
Top Secret	com.waveset.adapter.TopSecretResourceAdapter

建立資源

您可使用**資源精靈**建立資源。資源精靈會指導您完成建立 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中的物件。

使用此「資源精靈」可設定下列項目：

- **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** — 在資源的模式對映中定義。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** — 設定策略、建立資源核准人、設定組織對資源的存取權。

若要建立資源，請：

1. 從 [Resource Type Actions] 選項清單中選取 **[New Resource]**。

   Identity Manager 顯示 [New Resource] 頁面。

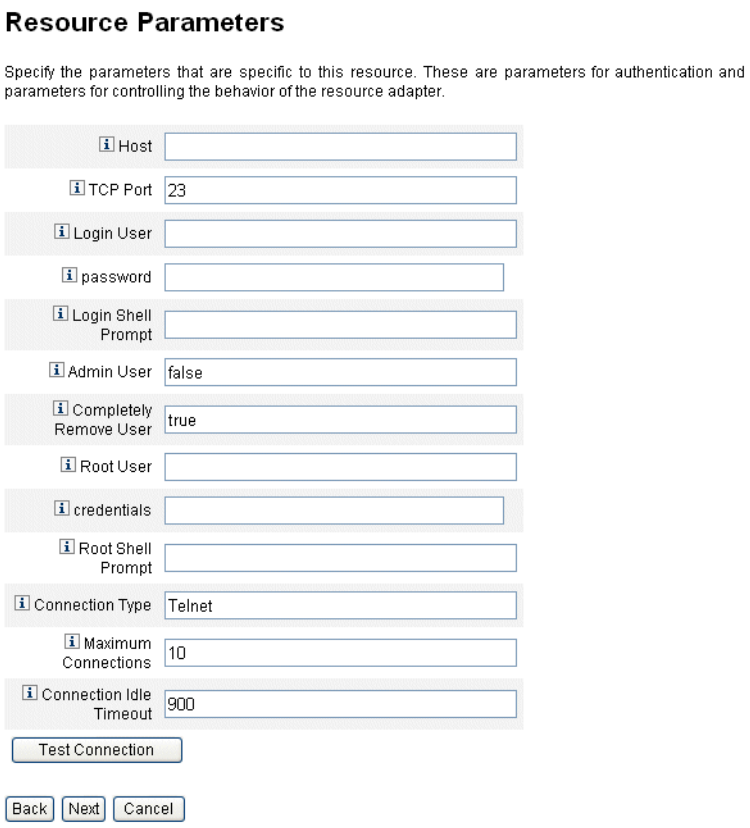
2. 選取資源類型，然後按一下 **[New]** 以顯示 [Resource Wizard Welcome] 頁面。

備註 或者，也可以從資源清單中選取資源類型，然後再從 [Resource Type Actions] 清單中選取 [New Resource]。在此情況下，Identity Manager 不會顯示 [New Resource] 頁面，而是立即啓動資源精靈。

---

3. 按 **[Next]** 開始定義資源。資源精靈的步驟和頁面以如下順序顯示：
   - **[Resource Parameters]** — 設定用於控制認證和資源配接卡運作方式的資源特定參數。輸入參數，然後按一下 **[Test Connection]** 來確保連線有效。確認後，按 **[Next]** 以設定帳號屬性。圖 4-1 顯示了 [Resource Parameters] 頁面。

圖 4-1 資源精靈：資源參數

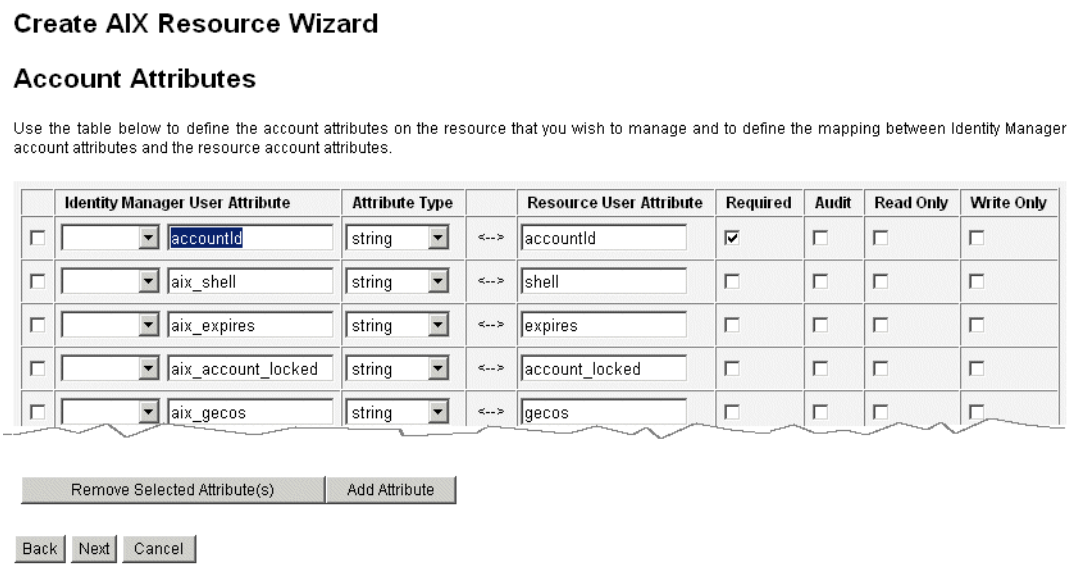


- **[Account Attributes (Schema Map)]** — 將 Identity Manager 帳號屬性對映到資源帳號屬性。

  若要新增屬性，按一下 **[Add Attribute]**。選取一個或多個屬性，然後按一下 **[Delete Selected Attributes]** 從模式對映中刪除屬性。完成後，按 **[Next]** 設定身份識別範本。

  圖 4-2 顯示了資源精靈中的 [Account Attributes] 頁面。

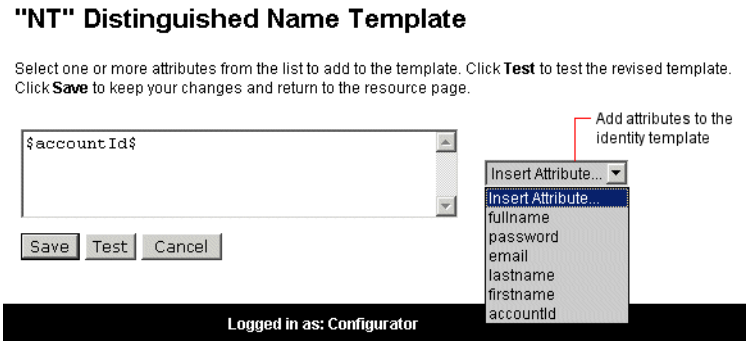
圖 4-2 資源精靈：帳號屬性 (模式對映)



- **[Identity Template]** — 定義使用者的帳號名稱語法。此功能對階層式名稱空間特別重要。

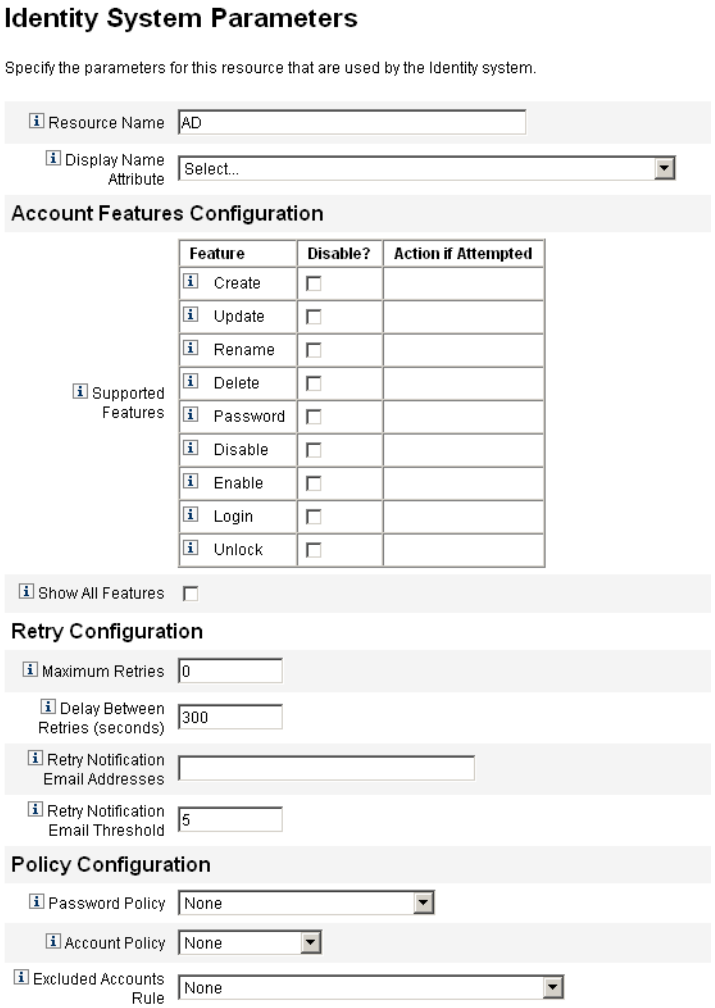
  從 [Insert Attributes] 清單中選取屬性。從範本刪除屬性，在清單中按一下並從字串中刪除一個或多個項目。刪除屬性名稱以及前置與後置的 $ (美元符號) 字元。

圖 4-3 資源精靈：身份識別範本



- **[Identity System Parameters]** — 設定資源的 Identity Manager 參數，包括重試和策略配置，如圖 4-4 所示。

圖 4-4 資源精靈：Identity 系統參數



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

管理資源

您可以對資源清單中的資源執行一系列編輯動作。除了在每一 [Resource Wizard] 頁上的編輯權限外，您還可以：

- **刪除資源** — 選取一個或多個資源，然後從 [Resource Actions] 清單中選取 [Delete]。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 [Resource Object Actions] 清單中選取 [Find Resource Object]，以按照物件特性尋找資源物件 (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，您可以建立新的物件。選取資源，然後從 [Resource Object Actions] 清單中選取 [Create Resource Object]。
- **重新命名資源** — 選取資源，然後從 [Resource Actions] 清單中選取 [Rename]。在出現的輸入方塊中輸入新名稱，然後按一下 **[Rename]**。
- **複製資源** — 選取資源，然後從 [Resource Actions] 清單中選取 [Save As]。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** — 指定資源和動作清單，以套用 (從 CSV 格式的輸入) 至清單中的所有資源。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

Identity Manager 資源使用模式對映定義來自外部資源 (**資源帳號屬性**) 的屬性名稱和類型；然後它們會將這些屬性對映到標準的 Identity Manager 帳號屬性。透過設定模式對映 (在 [Resource Wizard] 的 [Account Attributes] 頁中)，您可以：

- 將資源屬性限制爲只有您公司所必需的那些屬性。
- 建立用於多個資源的共用 Identity Manager 屬性名稱。
- 識別必要的使用者屬性和屬性類型。

若要存取這些值，請從資源清單中選取資源，然後從 [Resource Actions] 清單中選取 **[Edit Resource Schema]**。

模式對映的左欄 (標題爲 [Identity system User Attribute]) 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 (標題爲「資源使用者屬性」) 的右欄包含來自外部來源的屬性名稱。

透過定義 Identity 系統屬性名稱，可以使用共用名稱定義來自不同資源的屬性。例如，在 Active Directory 資源上，Identity Manager 中的 `lastname` 屬性對映至 Active Directory 資源屬性 `sn`；在 GroupWise 上，`fullname` 屬性可以對映至 GroupWise 屬性 `Surname`。因此，要求管理員只用一次完成 `lastname` 的值；當儲存使用者以後，會以不同的名稱將其傳送到資源。

資源群組

同樣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。在群組中加入及排序資源並將該群組指定給某個使用者，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動作。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，一個 Exchange 5.5 資源依賴現有的 Windows NT 或 Windows Active Directory 帳號：在成功建立 Exchange 帳號前，必須存在這些項目其中之一。在以 (依序) Windows NT 資源和 Exchange 5.5 資源建立資源群組後，您需要在建立使用者時確保正確的序列。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 **[Resources]**，然後選取 **[List Resource Groups]** 以顯示目前定義的資源群組之清單。在該頁中，按一下 **[New]** 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 [Global Resource Policy] 中編輯資源的特性。在 [Edit Global Resource Policy Attributes] 頁面中，您可以編輯以下策略屬性：

- **[Default Capture Timeout]** — 輸入一個值 (以毫秒爲單位)，以指定在指令行提示之後配接卡逾時之前，配接卡應等待的最長時間。此值僅適用於 GenericScriptResourceAdapter 或 ShellScriptSourceBase 配接卡。當指令或程序檔的結果很重要且將由配接卡剖析時，請使用此設定。

  此設定的預設值爲 30000 (30 秒)。

- **[Default Wait for Timeout]** — 輸入一個值 (以毫秒爲單位)，以指定在輪詢之間檢查指令是否具有就緒字元 (或結果) 之前，程序檔配接卡應等待的最長時間。此值僅適用於 GenericScriptResourceAdapter 或 ShellScriptSourceBase 配接卡。當配接卡不檢查指令或程序檔結果時，請使用此設定。

- **[Wait for Ignore Case]** — 輸入一個值 (以毫秒爲單位)，以指定在逾時之前配接卡應等待指令行提示的最長時間。此值僅適用於 GenericScriptResourceAdapter 或 ShellScriptSourceBase 配接卡。當不區分大小寫 (大寫或小寫) 時，請使用此設定。
- **[Resource Account Password Policy]** — 請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 **[None]**。
- **[Excluded Resource Accounts Rule]** — 請選取管理已排除資源帳號的規則 (如果適用)。預設選項爲 **[None]**。

您必須按一下 **[Save]** 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：

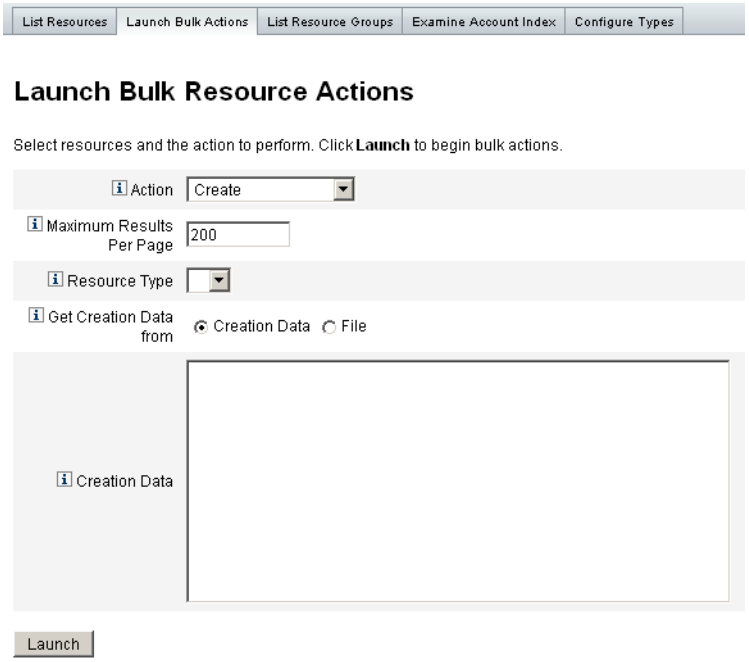
```
com.waveset.adapter.ScriptedConnection.ScriptedConnection.maxwaitMilliseconds.
```

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 4-5 顯示了使用建立動作的批次處理作業的啓動頁面。

圖 4-5 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 **[From Action List]** 以指定多個動作。

- **[Actions]** — 若要指定單一動作，請選取以下某個選項：[Create]、[Clone]、[Update]、[Delete]、[Change Password]、[Reset Password]。

  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 [Create] 動作，您將指定資源類型。

  如果您指定 [From Action List]，請使用 **[Get action list from]** 區域指定要使用的含動作檔案或您在 [Input] 區域中指定的動作。

備註 您在 [Input] 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。

- **[Maximum Results Per Page]** — 使用此選項可以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 **[Launch]** 可以啓動作業，其將做爲背景作業執行。

Identity Manager 變更記錄檔

請閱讀本節，以取得有關 Identity Manager 變更記錄檔功能的資訊，和有助於配置並使用變更記錄檔的程序。

什麼是變更記錄檔？

可以在**變更記錄檔**中檢視 Identity Manager 資源包含的身份識別屬性資訊。將每個變更記錄檔定義爲擷取身份識別屬性某個子集的變更。

資源上的屬性資料變更後，Active Sync 配接卡會擷取該資訊，然後將變更寫入變更記錄檔。自訂程序檔是專門開發用來與企業中的資源互動，然後讀取變更記錄檔並更新資源。

變更記錄檔功能與 Identity Manager 之標準資源使用中的同步化和調解功能不同，因爲它與佈建系統資源間接通訊 (透過自訂程序檔)。

變更記錄檔與安全性

Identity Manager 的變更記錄檔功能需要具有寫入本機檔案系統中指定目錄的權限。依預設，某些 Web 容器不允許本機檔案系統存取託管的 Web 模組 (如 Identity Manager)。

透過編輯 Java 策略檔案，您可以取得存取授權。若將 `/tmp/changelogs` 做爲目錄，則策略檔案應包含：

```
grant {
    permission java.io.FilePermission "/tmp/changelogs/*",
"read,write,delete";
};
```

您必須爲每個指定的變更記錄檔目錄定義一個檔案權限。

Java 的預設安全策略檔案位於：

```
$JAVA_HOME/jre/lib/security/java.policy
```

編輯此檔案即可；但如果您使用自己的檔案 (非預設檔案)，則伺服器將執行以下選項：

```
-Djava.security.manager -Djava.security.policy=/path/to/your/java.policy
```

在此情況下，請編輯由 `java.security.policy` 系統特性識別的檔案。

備註 編輯安全策略檔案之後，您可能需要重新啓動 Web 容器。

變更記錄檔功能的需求

變更記錄檔功能需要您配置身份識別屬性，然後才能配置變更記錄檔。

備註 請完成第 120 頁的 「配置身份識別屬性和事件」小節中說明的程序，以滿足這些需求。

配置變更記錄檔

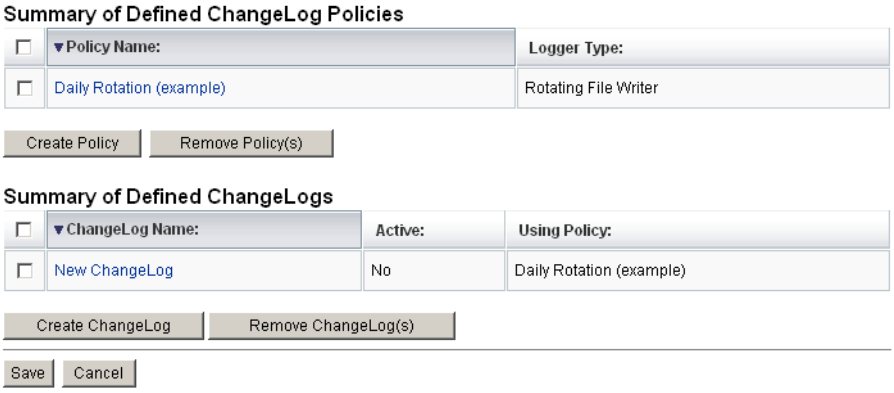
透過建立變更記錄檔策略與變更記錄檔，配置變更記錄檔。每個變更記錄檔必須具有一個關聯的變更記錄檔策略。變更記錄檔定義應將哪些變更子集 (由 Active Sync 偵測並透過身份識別屬性推入) 寫入記錄中。其關聯的變更記錄檔策略定義寫入變更記錄檔的方式。變更記錄檔將被自訂程序檔消耗。

若要配置變更記錄檔和變更記錄檔策略，請選取 **[Meta View]**，然後選取 **[ChangeLogs]**。

Identity Manager 會顯示 [ChangeLog Configuration] 頁面，其中顯示兩個摘要區域。

備註 如果尚未配置任何身份識別屬性，則 [ChangeLogs] 標籤不可見。

圖 4-6 變更記錄檔配置



變更記錄檔策略摘要

變更記錄檔策略摘要區域顯示目前定義的變更記錄檔策略。若要編輯現有的變更記錄檔策略，請按一下清單中該策略的名稱。若要建立變更記錄檔策略，請按一下 **[Create Policy]**。

若要移除一個或多個變更記錄檔策略，請從清單中選取它們，然後按一下 **[Remove Policy]**。(不需要確認此動作。)

變更記錄檔摘要

變更記錄檔摘要區域顯示目前定義的變更記錄檔。若要編輯現有的變更記錄檔，請按一下清單中該變更記錄檔的名稱。若要建立變更記錄檔，請按一下 **[Create ChangeLog]**。

若要移除一個或多個變更記錄檔，請從清單中選取它們，然後按一下 **[Remove ChangeLog]**。(不需要確認此動作。)

儲存變更記錄檔配置變更

您對變更記錄檔配置 (無論是變更記錄檔策略還是定義的變更記錄檔) 做出任何變更之後，必須從 [ChangeLog Configuration] 頁面儲存這些變更。按一下 **[Save]** 以儲存變更並返回至 [Meta View]。

建立和編輯變更記錄檔策略

在 [Edit ChangeLog Policy] 頁面上提供輸入並進行選取，以建立或編輯變更記錄檔策略：

- **[Policy Name]** — 爲策略輸入唯一的名稱。
- **[Daily Start Time]** — 建立每天用來評估自動重建開始或變更的時間。使用此策略的變更記錄檔將在該時間啓動新的週轉，並以從該時間評估的增量啓動新的週轉。例如，如果啓動時間設定爲午夜 (00:00) 且 [Rotations Per Day] 設定爲 3，則記錄檔的前綴將在 00:00、08:00 與 16:00 變更。

  檔案名稱遵循 `cl_User_yyyyMMddHHmmss.n.suffix` 式樣，其中 *HHmmss* 是最近啓動自動重建的時間。(*n* 是序列號，*suffix* 是在變更記錄檔定義中提供的後綴。)

  在使用「00:00」做爲啓動時間，3 做爲週轉數的情況下，如果您在某天上午 9:24 啓動變更記錄檔，則產生的週轉名稱將包含最近啓動週轉的時間 (例如，08:00)。在此情況下，檔案名稱將以 `cl_User_yyyyMMdd080000` 開頭。在 16:00 時，新的週轉 (檔案名稱上的新前綴) 將啓動。
- **[Rotations Per Day]** — 指定每天您要週轉記錄的次數。例如，如果您要每 4 小時週轉一次，則輸入值 6。

  此值僅限於非負整數。值 0 表示忽略此欄位。如果此欄位爲非零值，則將忽略 [`Maximum Age of a Rotation`] 設定。

  如果以秒爲單位指定自動重建的時間長度，且 [`Rotations Per Day`] 欄位爲 0，則此值將用於確定自動重建的週期。

  此值僅限於非負整數值。如果您將 [`Rotations Per Day`] 指定爲非零數值，則將使用該指定的值 (不使用此值)。如果這兩個欄位的值均爲 0，則僅套用序列資訊。(在此情況下，甚至不使用 [`Daily Start Time`]。)
- **[Number of Rotations to Keep]** — 指定允許累計的週轉次數，超過此次數 Identity Manager 將刪除週轉。例如，如果您現在每天執行 3 次週轉，並要在記錄中保留 2 天的變更，則指定值 6。
- **[Maximum File Size in Bytes]** — 如果向目前的檔案寫入變更後將超過此限制，則將啓動新記錄檔 (具有相同的自動重建前綴，但具有新的序列號)。值 0 表示不使用此限制。會使用所有值爲非零的限制欄位 (大小、行數、時間)；但是，會在檢查其他限制之前檢查該限制。
- **[Maximum File Size in Lines]** — 如果寫入變更將導致目前檔案的行數超出此限制，則會建立新的序列檔案，且將行寫入新檔案。值 0 表示**無限制**。會在檢查大小限制之後、檢查時間限制之前檢查此限制。

- **[Maximum File Age in Seconds]** — 如果收到變更，且現有的序列檔案的存在時間已經超過此處指定的秒數，則會在寫入變更之前建立新的序列檔案。值 0 表示不使用此限制。其他限制如果爲非零，會在該值之前套用。

按一下 **[OK]** 返回至 [ChangeLog Configuration] 頁面。您必須從配置頁面按一下 [OK]，才能將新的變更記錄檔策略或變更儲存至現有的策略。

建立和編輯變更記錄檔

在 [Edit ChangeLogs] 頁面上提供輸入並進行選取，以建立或編輯變更記錄檔：

- **[ChangeLog Name]** — 爲變更記錄檔輸入唯一的名稱。
- **[Active]** — 如果您選取此選項，則變更記錄檔將在變更經過 Active Sync 資源並進入身份識別屬性時監視並寫入變更 (Active Sync 必須爲身份識別屬性應用程式，才能實現此作業)。
- **[Filter]** — 輸入要使用的變更記錄檔篩選器的名稱。`Noop` 表示使用預設篩選器，此篩選器可接受所有變更。對於大多數情況，選取該篩選器即可。若不使用預設篩選器，則必須命名一個實作 `com.sun.idm.changelog.ChangeLogFilter` 的 Java 類別。此類別必須在伺服器的類別路徑中，且必須具有公用預設建構子。
- **[Log these Operations]** — 記錄所選類型的事件，包括 [Create]、[Update] 與 [Delete]。忽略未選取的事件。
- **[ChangeLog View]** — 使用此表格可定義變更記錄檔的內容 (欄)。每個表格列指定變更記錄檔中的一欄。按一下 **[Add Column]** 可增加變更記錄檔欄。每個欄都有名稱、類型與身份識別屬性名稱。列的順序表示欄的順序。定義欄之後，使用 **[Up]** 與 **[Down]** 按鈕對欄進行排序。

備註 在每個變更記錄檔中，表格中均有一個名爲 `changeType` 的隱含第一欄。此隱含第一欄指出變更的類型。此欄的類型爲 [Text]。記錄中的資料將是下列值之一：`ADD`、`MOD` 或 `DEL`。

- **[Use the Policy Named]** — 從清單中選取已定義的變更記錄檔策略以用於記錄。
- **[Output Path]** — 輸入檔案系統上將包含該記錄檔的目錄名稱。此路徑可以是網路掛載的位置；但最好使用伺服器本機上的目錄。同樣也建議每個變更記錄檔使用唯一的位置。
- **[Suffix]** — 爲變更記錄檔輸入後綴 (例如，`.csv`)。選取的後綴可以用來區別這些檔案與其他的變更記錄檔。

按一下 **[OK]** 返回至 [ChangeLog Configuration] 頁面。您必須從配置頁面按一下 [OK]，才能將新的變更記錄檔或變更儲存至現有的變更記錄檔。

範例

以下範例詳細說明了如何設定身份識別屬性與變更記錄檔，以擷取特定屬性資料集。

範例：定義身份識別屬性

在此範例中，兩個 Identity Manager 資源 (資源 1 與資源 2) 向第三個資源 (資源 3) 提供來源資料。資源 3 不直接連接至 Identity Manager 系統。需要變更記錄檔來從資源 1 和資源 2 提取資料子集並保留到資源 3 中。

```
資源 1：EmployeeInfo
employeeNumber*
givenname
mi
surname
phone

資源 2：OrgInfo
employeeNum*
managerEmpNum
departmentNumber

資源 3：PhoneList
empId*
fullname
phone
department
```

備註 * 表示用來關聯記錄的鍵。

下表中定義了身份識別屬性。

表 4-2 使用變更記錄檔之範例的身份識別屬性

屬性	<==	來自 Resource.Attribute
employee	<==	EmployeeInfo.employeeNumber
dept	<==	OrgInfo.departmentNumber
reportsTo	<==	OrgInfo.managerEmpNum

表 4-2 使用變更記錄檔之範例的身份識別屬性 (繼續)

屬性	<==	來自 Resource.Attribute
firstname	<==	EmployeeInfo.givename
lastname	<==	EmployeeInfo.givename
middleInitial	<==	EmployeeInfo.mi
fullname	<==	firstName + ""+ middleInitial + ""+ lastName
phoneNumber	<==	EmployeeInfo.phone

範例：配置變更記錄檔

定義身份識別屬性後，定義稱爲 PhoneList ChangeLog 的變更記錄檔。目的是將身份識別屬性的子集寫入變更記錄檔。

PhoneList ChangeLog 中的變更記錄檔視圖

欄名稱	類型	身份識別屬性
empId	文字	employee
fullname	文字	fullname
phone	文字	phoneNumber

當資源 1 或資源 2 中的記錄發生變更之後，變更記錄檔記錄 (來自身份識別屬性的所有資料) 的資料全集 (不僅是變更) 將寫入變更記錄檔。自訂程序檔會讀取該資訊並將其寫入資源 3。

變更記錄檔中的 CSV 檔案格式

請閱讀本節，以取得有關由變更記錄檔寫入的逗號分隔值 (CSV) 檔案的格式之資訊。

想像一下列與欄格式的變更記錄檔，例如試算表或資料庫表格。每「列」爲檔案中的每行。

變更記錄檔格式使用前兩列來進行自我說明。這兩列可一併用於定義「模式」；亦即表格中每個「儲存格」(列上逗號之間的值) 的邏輯名稱與邏輯類型。

第一列命名檔案中的屬性。第二列說明屬性值的類型。其他列表示變更事件的所有資料。

變更記錄檔以 Java UTF-8 格式進行編碼。

欄

檔案中的第一欄具有特殊的重要性。它會定義作業類型，例如，變更事件是否爲建立、修改或刪除動作。其名稱永遠爲 changeType，類型永遠爲 T (表示文字)。其值爲以下值之一：ADD、MOD 或 DEL。

每一欄應該準確具有一個唯一的項目識別碼 (主鍵)。一般爲檔案中的第二欄。

其他欄僅命名屬性。名稱來自於 [ChangeLog View] 表格中的 [Column Name] 值。

列

在定義檔案**模式**的前兩個標頭列之後，剩餘的列爲屬性的值。值以第一列中欄位的順序顯示。變更記錄檔套用自身份識別屬性，因此包含偵測到變更時所有已知的使用者資料。

而且，沒有表示空 (或未設定) 的特殊指示值。如果偵測到變更時，而值不存在，則變更記錄檔會寫入空字串。

根據檔案第二列指定的欄類型，對值進行編碼。支援的類型如下：

- T：文字
- B：二進位
- MT：多文字
- MB：多進位

文字值

文字值寫入爲字串，但有兩種例外：

- 如果值包含 , (逗號)，則 Identity Manager 會透過插入 \ (反斜線) 字元來退出值中的逗號。例如，如果 fullname 的值爲 Doe, John，則 Identity Manager 會將該值寫入爲
  Doe \,John。
- 如果值包含 \ (反斜線) 字元，則 Identity Manager 會另加一個 \ 來退出該字元。例如，如果 homedir 的值包含 C:\users\home，則 Identity Manager 會將 C:\\users\\home 寫入記錄。

文字值不能包含換行字元。如果檔案需要換行，則請使用二進位值類型。

二進位值

二進位值以 Base64 進行編碼。

多文字值

多文字值與文字值的寫入方式相似，但用逗號分隔並使用 [與] 括起來。

多進位值

多進位值與二進位值寫入方式相似 (以 Base64 編碼)，但也用逗號分隔並使用 [與] 括住。

格式範例

以下範例說明各種輸出格式。每個範例均遵循以下格式：

```
column1, column2, column3, column4
```

每個範例的欄 3 均顯示範例文字。

- 文字 (T) 資料在檔案中顯示爲字串：

  ```
  ADD,account0,some text data,column4
  ```

- 二進位 (B) 資料顯示爲 base64 編碼。

  ```
  ADD,account0,FGResWE23WDE==,column4
  ```

- 多文字 (MT) 顯示爲：

  ```
  ADD,account0,[one,two,three],column4
  ```

- 多文字 (MB) 顯示爲：

  ```
  ADD,account0,[FGResWE23WDE==,FGRCAFEBADE3sseGHSD],column4
  ```

備註 Base64 字母不包含 , (逗號)、[(左括號) 或] (右括號) 字元，或換行符號。

變更記錄檔名稱

檔案名稱遵循以下格式：

```
servername_User_timestamp.sequenceNumber.suffix
```

其中：

- *timestamp* 爲此記錄啓動或自動重建的時間。將具有相同時間戳記的檔案視爲**自動重建**。
- *sequenceNumber* 爲單增長數字，用來將自動重建分割爲檔案子集，並由位元、行或秒的最大數目控制。每個檔案子集稱爲一個**序列**檔案。
- *suffix* 爲變更記錄檔配置中定義的檔案副檔名，通常爲 `.csv`。

配置週轉與序列

這些可在變更記錄檔策略物件中定義，並從變更記錄檔參考。

範例

如果某策略將自動重建定義爲：

- 開始於上午 7:00
- 每天選轉 3 次，持續兩天

則將產生與如下類似的檔案名稱。(在其中每個週轉中，均有兩個序列檔案。)

```
myServer_User_20060101070000.1.csv
myServer_User_20060101070000.2.csv
myServer_User_20060101150000.1.csv
myServer_User_20060101150000.2.csv
myServer_User_20060101230000.1.csv
myServer_User_20060101230000.2.csv

myServer_User_20060102070000.1.csv
myServer_User_20060102070000.2.csv
myServer_User_20060102150000.1.csv
myServer_User_20060102150000.2.csv
myServer_User_20060102230000.1.csv
myServer_User_20060102230000.2.csv
```

1 月 1 日顯示 3 個週轉，間隔 8 小時，開始於 07:00:00。1 月 2 日 與之類似；僅對應於日期 (20060102) 的名稱部分有所不同。

寫入變更記錄檔程序檔

請閱讀本節，以取得有關變更記錄檔程序檔寫入器有用的資訊。

- 程序檔一般會連續執行，等待新資料、新檔案或在作業之間暫停，然後讀取檔案並將每行的變更套用至後端資源。
- 變更記錄檔支援刪除作業，但是只有 `accountId` 值將包含在 `DEL` 行中。
- 透過使用週轉與序列，可以決定程序檔執行的頻率。例如，如果您可以指定：
  - 在午夜啓動週轉，然後每晚根據前一週轉執行程序檔。
  - 每 4 小時週轉一次，從上午 8:00 開始，然後每四小時執行程序檔 (時間分別爲 8、12、16、20、24、4...)
  - 無週轉，但執行程序檔，從而當序列號溢滿時會讀取序列檔案。您可以控制序列號如何遞增；它可以是以大小爲基礎、以數字作業爲基礎或以時間爲基礎。
- 每個變更記錄檔都可以代表後端系統中的記錄。爲了使程序檔讀取記錄更加簡單，Identity Manager 總是將所有的資料寫入給定記錄，無論它是否變更。程序檔可能「盲目地」套用記錄中的資料。

  但是，其需要確保後端資源 (或程序檔) 可以 (特別是對於 `ADD` 與 `DEL`)：
  - 等冪處理此作業。(**等冪**指如果套用資料多於一次，則等於未進行任何作業。) 如果程序檔從開啓至結束共兩次讀取變更記錄檔，則資源中資料記錄的狀態在每次傳入後應該完全相同。
  - (最多) 執行一次。例如，如果資源對於增加與刪除動作無法進行等冪作業，則程序檔必須確保僅套用一次變更，透過僅讀取記錄項目一次或以其他方式追蹤其進度。
- 最好等待出現序列檔案，然後套用之前的檔案。例如，直到出現 .2 檔案後再套用 .1 檔案。當出現 .3 檔案時，再套用 .2 檔案。套用檔案後，請注意您在磁碟上進行這些作業。此方法可讓您避免使用諸如 `fstat` 或 `tail -f` 等呼叫。

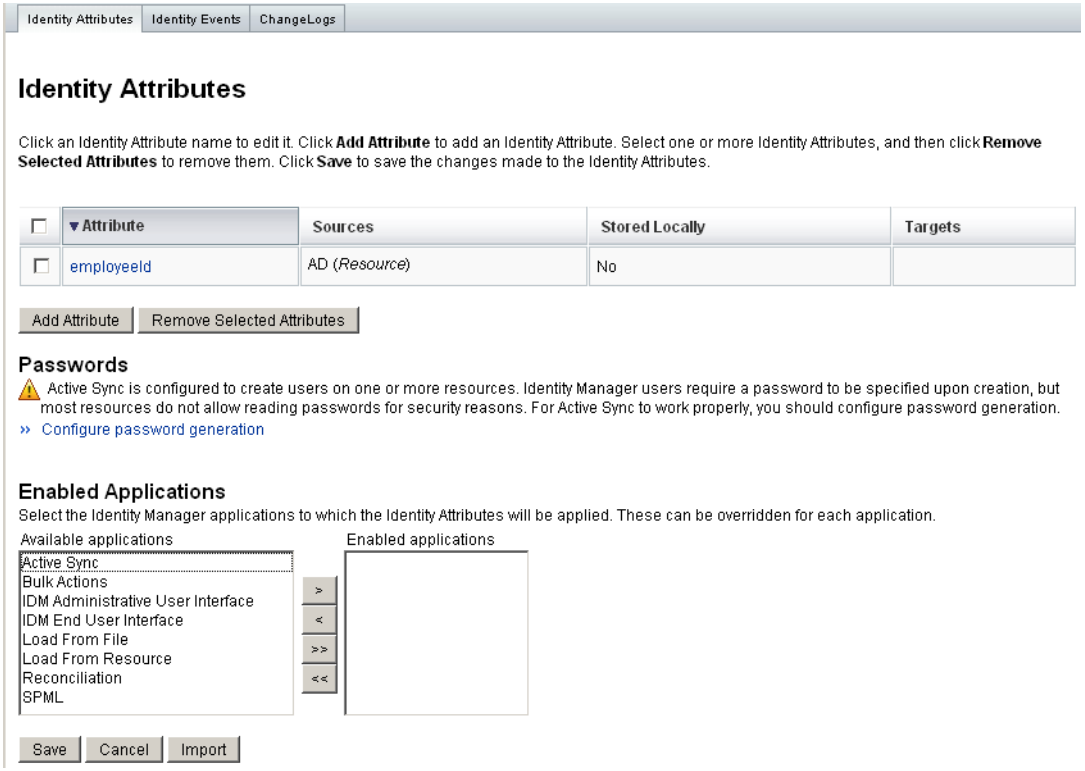
配置身份識別屬性和事件

您可以使用管理員介面的 [Meta View] 區域配置身份識別屬性和事件。請使用以下小節中的資訊和程序配置 Identity Manager 身份識別屬性和身份識別事件，以及選取將套用這些屬性和事件的 Identity Manager 系統應用程式。

處理身份識別屬性

若要配置身份識別屬性，請選取 **[MetaView]**，然後選取 **[Identity Attributes]**。螢幕將顯示 [Identity Attributes] 頁面。下圖爲此頁面的一個範例。

圖 4-7 在 [Meta View] 中配置 [Identity Attributes]



若要增加身份識別屬性，請按一下 **[Add Attribute]**。增加至清單後，透過在清單中按一下身份識別屬性名稱來編輯該屬性。若要移除一個或多個身份識別屬性，請選取要移除的屬性，然後按一下 **[Remove Selected Attributes]**。

您可以選取一個或多個要增加到屬性中或要從其中移除的回應。

您必須按一下 **[Save]**，才能執行該動作。

如果自從您上次修改身份識別屬性以後，資源已發生變更，則 [Identity Attributes] 頁面將顯示以下警告訊息 (圖 4-8)。按一下警告訊息中的 **[Configure the Identity Attributes from resource changes]** 以同化變更。

圖 4-8 [Resources Have Changed] 警告訊息

密碼

Active Sync 配置爲在一個或多個資源上建立使用者。Identity Manager 使用者需要在建立時指定一個密碼，但大多數資源出於安全性原因不允許讀取密碼。如果密碼產生尚未設定，請按一下 **[Configure password generation]**。

選取如何在身份識別使用者和透過 Active Sync 建立的其他資源帳號上設定密碼：

- **[Use default password]** — 選取此選項，然後輸入一個密碼。password.password 身份識別屬性將從此值設定使用者密碼。
- **[Use rule to generate password]** — 選取此選項可選取密碼產生要使用的規則。`password.password` 身份識別屬性使用所選的規則來產生密碼。
- **[Use Identity System Account Policy password generation]** — 選取此選項可以選取密碼產生要使用的策略。選取此選項會將 `waveset.assignedLhPolicy` 身份識別屬性設定爲所選的策略。如果所選的策略未配置爲產生密碼，並且您具有建立和修改策略所需的權限，則頁面會重新顯示其他選項，可以讓您建立策略副本或修改現有策略。

  此選項會根據爲 Identity 系統帳號策略配置的密碼策略產生隨機密碼。由於其依賴於隨機密碼產生，因此這是最安全的密碼產生選項。

選取應用程式

使用 [Enabled Applications] 區域來選取將套用身份識別屬性的 Identity 系統應用程式。從 [Available applications] 區域中選取一個或多個應用程式，然後將它們移至 [Enabled applications] 區域。您必須按一下 **[Save]**，才能執行該動作。

備註 若要使用變更記錄檔功能，您必須啓用 Active Sync 應用程式。如需更多資訊，請參閱第 199 頁的「Active Sync 配接卡」。

增加和編輯身份識別屬性

從 [Add Identity Attributes] 或 [Edit Identity Attributes] 頁面，請進行以下這些選取以增加或編輯身份識別屬性：

- **[Attribute Name]** — 選取或輸入屬性名稱。從提供的預設值 (來自資源模式對映項目、作業中的身份識別屬性與使用者擴充的屬性) 中進行選取；或在文字方塊中輸入值。
- **[Sources]** — 選取一個或多個來源，從中寫入此身份識別屬性的值。將按順序評估這些來源，並將身份識別屬性設定爲第一個非空值。
  - **[Resource]** — 該值來自於所選資源上已選取的屬性。
  - **[Rule]** — 該值來自於對所選規則的評估。
  - **[Constant]** — 該值設定爲提供的常數值。

  按一下 [+] (加號) 可增加新行以選取其他來源。按一下來源旁邊的 [-] (減號) 可將其刪除。若要對來源進行重新排序，請按一下箭頭，以在清單中上下移動來源。
- **[Attribute Properties]** — 使用此區域可指定身份識別屬性的特性設定。
  - **[How to set Identity Attribute]** — 選取以下某個選項可以指定 Identity Manager 將如何設定資源上的屬性值。
    - **[Set to value]** — 身份識別屬性的值爲所有目標上的授權設定值。選取此選項將導致由來源確定的值會置換使用者在表單中輸入的任何值。此選項是典型實作的適當設定。
    - **[Default value]** — 僅當目標上未設定值時設定屬性值。
    - **[Merge with value]** — 將值增加到現有值。系統將篩選出重複值。
  - **[Store attribute in IDM repository]** — 選取此選項，以將身份識別屬性儲存在本機的 Identity 系統儲存庫中。如果 Identity 系統使用者被授權儲存身份識別屬性，或者屬性可以處理查詢，則應該選取此選項。

- **[Set value on all assigned resources]** — 如果身份識別屬性將全域設定在支援此屬性的所有資源上，則選取此選項。

- **[Targets]** — 選取應該設定該身份識別屬性的目標資源。如果未定義目標，請按一下 **[Add Target]**。若要從清單中移除目標，請選取該目標，然後按一下 **[Remove Selected Targets]**。

  按一下 **[OK]** 可增加該身份識別屬性並返回至 [Identity Attributes] 頁面。必須在 [Identity Attributes] 頁面上按一下 **[Save]** 才能儲存增加的屬性。

增加目標資源

如果身份識別屬性僅用於變更記錄檔，則不必爲身份識別屬性設定目標。例如，如果您要使用變更記錄檔，還要使用標準的「輸入表單」推入資料 (透過 Active Sync)，則您可以這樣做。如果沒有目標，則 [MetaView] 將僅評估身份識別屬性的值；而不會在其他任何資源上設定這些屬性。

進行選取以增加應該設定身份識別屬性的目標資源：

- **[Target Resource]** — 選取應該設定所選身份識別屬性的目標資源。
- **[Target Attribute]** — 選取在目標資源上將接收其值的屬性名稱。
- **[Condition]** — 選取要執行的規則，以確定是否應該在此目標資源上設定所選的身份識別屬性。此規則應該返回 true 或 false 值。如果未設定條件，則對於選取的事件類型，會自動設定目標屬性。
- **Apply To:** — 選取事件類型，對於這些選取的事件類型，會在目標資源上設定選取的身份識別屬性。這些選取與條件共同確定是否設定目標屬性。

  按一下 **[OK]** 可以增加目標資源，並返回至 [Add Identity Attribute] 或 [Edit Identity Attribute] 頁面。

移除目標資源

若要移除一個或多個目標資源，請從清單中選取它們，然後按一下 **[Remove Selected Targets]**。

匯入身份識別屬性

使用匯入身份識別屬性功能，您可以選取一個或多個表單來匯入並寫入身份識別屬性值。Identity Manager 將分析匯入的表單值並對身份識別屬性進行「最佳猜測」；但是在匯入後編輯身份識別屬性是必要的。

進行這些匯入選取：

- **[Merge with existing Identity Attributes]** — 如果選取此選項，則 Identity Manager 會將匯入的值與現有的身份識別屬性合併。如果未選取，則會在匯入執行之前清除身份識別屬性。
- **[Forms to import]** — 從 [Available Forms] 區域中選取一個或多個表單來寫入身份識別屬性。

  按一下 **[Import]** 可匯入這些表單。顯示 [Identity Attributes] 頁面，其中會列出新的或合併的身份識別屬性。

  按一下 **[Save]** 可儲存身份識別屬性的變更。

備註 如果有需要校正的身份識別屬性條件，則 Identity Manager 將顯示 [Warning] 頁面，其中列出一個或多個警告。按一下 **[OK]** 可返回至 [Configure] 區域。

配置身份識別事件

您還可以配置由 Identity Manager 管理之資源的身份識別事件，以定義發生在這些資源上之事件的運作方式。身份識別事件中定義的運作方式在 Active Sync 期間用於確定事件的發生時間，並採取適當的動作回應該事件。

例如，您可以將身份識別事件配置爲在您的授權人力資源 (HR) 系統 (可觸發要刪除的身份識別使用者和其他所有資源帳號) 上偵測並回應刪除。

若要配置身份識別事件，請選取 **[MetaView]**，然後選取 **[Identity Events]** 標籤。在 [Identity Events] 頁面中，按一下 **[Add Event]** 並指定事件類型。您也可以透過選取 [Identity Events] 頁面中的事件並指定以下選項，來編輯身份識別事件。

- **[Event Type]** — 選取 [Delete]、[Enable] 或 [Disable] 可以指定您要配置的身份識別事件類型。
- **[Sources]** — 選取將套用身份識別事件的資源 (例如，AD 表示 Active Directory)。如果資源需要事件偵測規則以偵測事件並對事件做出回應 (因爲其不具有本機支援)，請在 **[determined by]** 欄位中選取規則。您可以增加和移除資源。
- **[Responses]** — 從 [Responses] 清單中選取回應，或按一下 **[Responses]** 可以增加回應 (如果未定義任何回應)。若要從選項清單中移除某回應，請選取該回應，然後按一下 **[Remove Selected Responses]**。

完成選取後請按一下 **[OK]**。

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 帳戶 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。

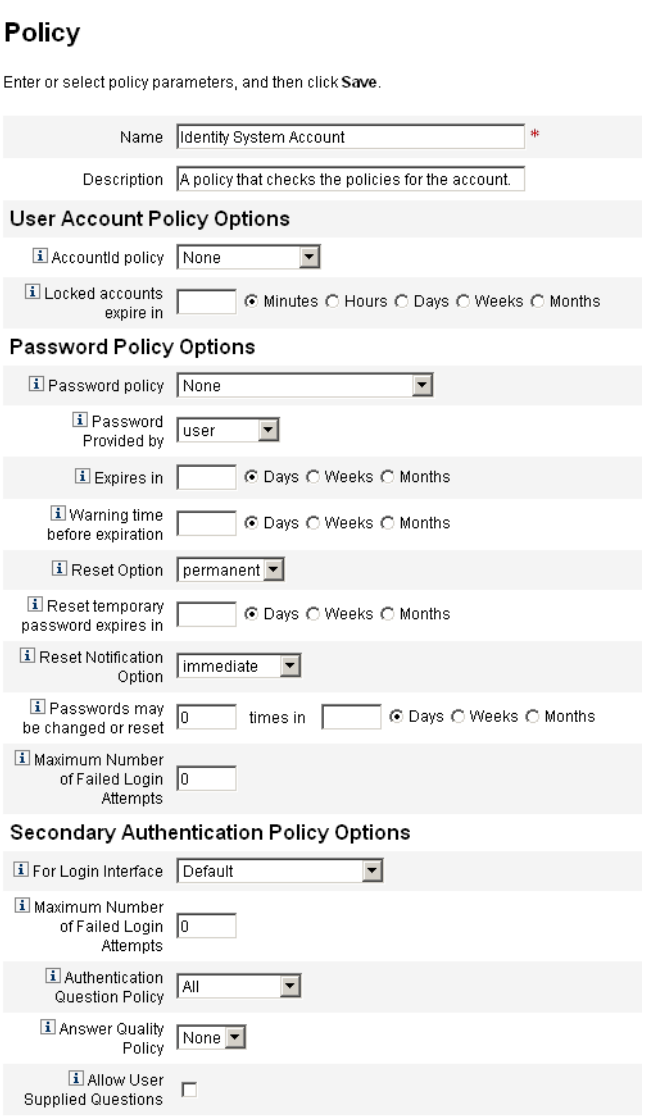
備註 Identity Manager 還提供了專門用於稽核使用者規範遵循的稽核策略。第 11 章「身份識別稽核」中論述了稽核策略

您可以在 [Policies] 頁面中建立並編輯 Identity Manager 使用者策略。在功能表列中，選取 **[Security]**，然後選取 **[Policies]**。在顯示的清單頁中，可以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及限制條件。透過 [Create Organization]、[Edit Organization]、[Create User] 和 [Edit User] 頁面，您可將 Identity 系統帳號策略 (如圖 4-9 所示) 指定給組織或使用者。

圖 4-9 Identity Manager 策略

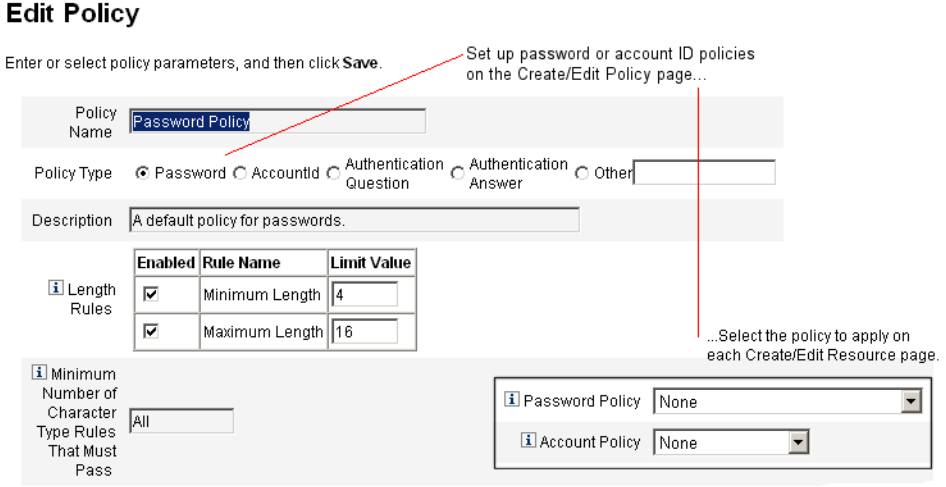


您可以設定或選取的選項包括：

- **[User policy options]** — 指定使用者在未能正確回答認證問題時，Identity Manager 應如何處理使用者帳戶
- **[Password policy options]** — 設定密碼過期、過期前的警告時間以及重設選項
- **[Authentication policy options]** — 確定如何向使用者顯示認證問題，使用者是否可以提供其自己的認證問題，並建立可以向使用者顯示的問題庫 (最多 10 項)。

- **[SPE System Account policies]** — 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 [Create Organization]、[Edit Organization]、[Create SPE User] 和 [Edit SPE User] 頁面，您可將這些策略指定給組織或使用者。
- **[String Quality Policies]** — 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 4-10 提供了一個範例。

圖 4-10 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：

- **[Length rules]** — 決定最小長度和最大長度。
- **[Character type rules]** — 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。
- **[Password re-use limits]** — 指定在目前密碼之前不能重複使用的密碼數。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。
- **[Prohibited words and attribute values]** — 指定不能 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

字典策略可使 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 [Administrator Interface] 密碼 [Edit Policy] 頁中的 [Not Contain Words] 選項來執行這份清單。)

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

請遵循下列步驟：

1. 在功能表列中，選取 **[Configure]**，然後選取 **[Policies]**。
2. 按一下 **[Configure Dictionary]** 顯示 [Dictionary Configuration] 頁。
3. 選取並輸入資料庫資訊：
    - **[Database Type]** — 選取要用來儲存字典的資料庫類型 (Oracle、DB2、SQLServer 或 MySQL)。
    - **[Host]** — 輸入正在執行資料庫的主機名稱。
    - **[User]** — 輸入連線至資料庫時使用的使用者名稱。
    - **[Password]** — 輸入連線至資料庫時使用的密碼。
    - **[Port]** — 輸入資料庫偵聽的連接埠。
    - **[Connection URL]** — 輸入連線時要使用的 URL。以下是可用的範本變數：
    - `%h` — 主機
    - `%p` — 連接埠
    - `%d` — 資料庫名稱
- **[Driver Class]** — 輸入與資料庫進行互動時要使用的 JDBC 驅動程式類別。
- **[Database Name]** — 輸入要載入字典的資料庫名稱。
- **[Dictionary Filename]** — 輸入載入字典時要使用的檔案名稱。

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

執行字典策略

從 Identity Manager 策略區執行字典策略。在 [Policies] 頁面中，按一下以編輯密碼策略。在 [Edit Policy] 頁面中，選取 [Check passwords against dictionary words] 選項。執行之後，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：

- **[Access Review Notice]** — 傳送使用者的存取權限需要加以檢閱的通知。必須補救或緩解存取策略的違規時，系統會傳送此通知。.
- **[Account Creation Approval]** — 將通知傳送給核准人，告知新帳號正在等待其核准。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。
- **[Account Creation Notification]** — 傳送已使用指定的特定角色建立帳號的通知。在 [Create Role」或 [Edit Role] 頁面的 [Notification recipients] 欄位中選取一或多位管理員時，系統將傳送此通知。
- **[Account Deletion Approval]** — 向核准人傳送通知，告知使用者帳號刪除動作正在等待核准。在 [Create Role」或 [Edit Role] 頁面的 [Notification recipients] 欄位中選取一或多位管理員時，系統將傳送此通知。
- **[Account Deletion Notification]** — 傳送已刪除帳號的通知。
- **[Account Update Notification]** — 將已更新帳號的通知傳送至指定的電子郵件地址或使用者帳號。
- **[Password Reset]** — 傳送重設 Identity Manager 密碼的通知。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。
- **[Password Synchronization Notice]** — 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。
- **[Password Synchronization Failure Notice]** — 通知使用者未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。
- **[Policy Violation Notice]** — 傳送發生帳號策略違規的通知。
- **[Reconcile Account Event]**、**[Reconcile Resource Event]**、**[Reconcile Summary]** — 分別從 [Notify Reconcile Response]、[Notify Reconcile Start] 和 [Notify Reconcile Finish] 預設工作流程呼叫。通知將依照每個工作流程中的配置傳送。
- **[Report]** — 將產生的報告傳送給指定收件者清單中的收件者。
- **[Request Resource]** — 將已請求資源的通知傳送給資源管理員。當管理員從 [Resources] 區域中請求資源時，系統會傳送此通知。
- **[Retry Notification]** — 傳送通知給管理員，說明對資源所進行的特定作業嘗試失敗達到指定的次數。

- **[Risk Analysis]** — 傳送風險分析報告。將一或多名電子郵件收件人指定爲資源掃描的部分時，系統將傳送此報告。
- **[Temporary Password Reset]** — 將已向帳號提供臨時密碼的通知傳送給使用者或角色核准人。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。

編輯電子郵件範本

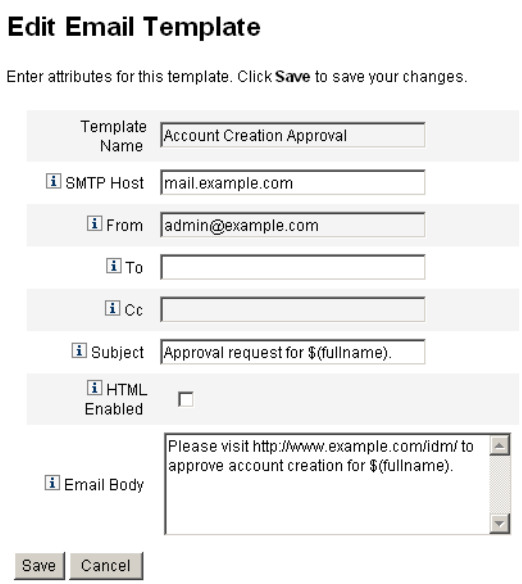
您可以自訂電子郵件範本以便爲收件者提供特定的指導，告知其如何完成作業或如何查看結果。例如，您可能要自訂 [Account Creation Approval] 範本，以透過增加以下訊息來將核准人導向至帳號核准頁面：

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 [Account Creation Approval] 範本用做範例，並執行以下程序：

1. 在功能表列中，選取 **[Configure]**。
2. 在 [Configure] 頁面中，選取 **[Email Templates]**。
3. 按一下以選取 [Account Creation Approval] 範本：

圖 4-11 編輯電子郵件範本



4. 輸入範本的詳細資訊：
   - 在 [SMTP Host] 欄位中，輸入 SMTP 伺服器名稱，以便傳送電子郵件通知。
   - 在 [From] 欄位中，自訂來源電子郵件地址。
   - 在 [To] 和 [Cc] 欄位中，指定將會接收電子郵件通知的一或多個電子郵件地址或 Identity Manager 帳號。
   - 在 [Email Body] 欄位中，自訂內容以提供指向您的 Identity Manager 位置的指標。
5. 按一下 **[Save]**。

您也可以使用 Identity Manager IDE 修改電子郵件範本。如需有關 IDE 的更多資訊，請參閱「Identity Manager Deployment Tools」。

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 [HTML Enabled] 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 4-3 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) — 使用者的完整名稱 $(role) — 使用者的角色
更新通知	$(fullname) — 使用者的完整名稱 $(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) — 使用者的完整名稱 $(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。配置稽核群組和事件需要 [Configure Audit] 管理權能。

若要配置稽核配置群組，請從功能表列中選取 **[Configure]**，然後選取 **[Audit]**。

[Audit Configuration] 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 [Edit Audit Configuration Group] 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 [Enable Audit] 核取方塊。取消選取該核取方塊可停用稽核系統。

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 [Actions] 欄中的項目從 **[Available]** 區域移至 **[Selected]** 區域，然後按一下 **[OK]**。

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 **[New]**。Identity Manager 會在頁面底部新增事件。從 [Object Type] 欄的清單中選取物件類型，然後將新物件類型的 [Actions] 欄中的一或多個項目從 [Available] 區域移至 [Selected] 區域。按一下 **[OK]** 可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 server settings]** — 透過從 [Resources] 區域建立 Remedy 資源來設定 Remedy 配置。在設定資源後，測試連線以確保啓用整合。

- **[Remedy template]** — 在設定 Remedy 資源後，定義 Remedy 範本。若要執行此作業，請選取 **[Configure]**，然後選取 **[Remedy Integration]**。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。若要執行此作業，請選取 **[Configure]**，然後選取 **[Servers]**。

若要編輯個別伺服器的設定，請選取 [Configure Servers] 頁面中清單內的伺服器。Identity Manager 會顯示 [Edit Server Settings] 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

依預設，調解器設定會顯示在 [Edit Server Settings] 頁面中。您可以接受預設值或透過取消選取 **[Use default]** 選項來指定值：

- **[Parallel Resource Limit]** — 指定調解器可以同時處理的最大資源數目。
- **[Minimum Worker Threads]** — 指定調解器會一直持續作用的處理執行緒數目。
- **[Maximum Worker Threads]** — 指定調解器可以使用的最大處理執行緒數目。調解器只會啓動工作負荷量需要的執行緒數目；這將限制執行緒數目。

排程程式設定

按一下 [Edit Server Settings] 頁上的 **[Scheduler]** 可以顯示排程程式選項。您可以接受預設值或取消選取 [Use] 預設選項來指定設定值：

- **[Scheduler Startup]** — 選取排程程式的啓動模式：
  - **[Automatic]** — 伺服器啓動時啓動。這是預設的啓動模式。
  - **[Manual]** — 伺服器啓動時啓動，但在手動啓動之前保持暫停狀態。

- **[Disabled]** — 伺服器啓動時不啓動。

- **[Tracing Enabled]** — 選取此選項即可啓動標準輸出的排程程式除錯追蹤。
- **[Maximum Concurrent Tasks]** — 選取此選項可指定排程程式將在任何一個時間執行的作業最大數目 (預設除外)。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。
- **[Task Restrictions]** — 指定可以在伺服器上執行的作業組合。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 **[Save]** 可儲存伺服器設定變更。

電子郵件範本伺服器設定

按一下 [Servers] 功能表中的 **[Email Templates]**，可以指定 [Default SMTP Server] 設定。

如果不使用預設，則可使用此選項，透過取消選取 **[Use Default]** 選項並輸入要使用的郵件伺服器，來指定預設電子郵件伺服器。您輸入的文字用於替代 [Email Templates] 中的 *smtpHost* 變數。

JMX

使用此設定可以啓用 JMX 叢集輪詢並配置輪詢執行緒的間隔。透過移至 Identity Manager 除錯頁面並按一下 **[Show MBean Info]** 按鈕，可以檢視已收集的 JMX 資料。

若要啓用 JMX 輪詢，請按一下 [Servers] 標籤上的 **[JMX]**，並選取以下選項：

- **[Enable 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 ([Use Default (false)])。

備註	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。

- **[Polling Interval (ms)]** — 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。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。

按一下 **[Save]** 可儲存伺服器設定變更。

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。若要編輯預設設定，請按一下 **[Edit Default Server Settings]**。[Default Server Settings] 頁面顯示與個別伺服器設定頁面一樣的選項。

您對每個預設伺服器設定所做的變更會傳遞至對應的個別伺服器設定，除非您取消選取該設定的 [Use] 預設選項。

按一下 **[Save]** 可儲存伺服器設定變更。

章節 5

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 管理員是擁有擴充 Identity Manager 特權的使用者。您可以建立 Identity Manager 管理員以管理：

- 使用者帳號
- 系統物件，例如角色與資源
- 組織

Identity Manager 以直接或間接指定下列項目的方式區別管理員與使用者：

- **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。
- **控制的組織**。被指定控制某組織後，管理員可以管理該組織中的物件，以及在階層中位於該組織以下的所有組織中的物件。

委託管理

在大多數公司中，具有欲執行管理工作的員工會擁有特定與不同的責任。多數情況下，管理員需要執行帳號管理作業，而這些作業對其他使用者或管理員而言是**不需設定的**，或者具有某些範圍限制。

例如，某管理員可能只負責建立 Identity Manager 使用者帳號。具有該有限責任範圍的管理員，不大可能需要有關其建立使用者帳號之資源的特定資訊，或有關系統內現有角色或組織的特定資訊。

Identity Manager 支援責任分離與此委託管理模式，方法是僅允許管理員檢視並管理特定的已定義範圍之內的物件。

Identity Manager 透過如下方法將個別系統活動委託給管理員進行管理：

- 提供對特定組織及這些組織中物件的有限控制
- 篩選 Identity Manager 使用者建立與編輯頁面的管理員檢視
- 以權能的形式給予管理員特定的工作責任

在設定新使用者帳號或編輯某使用者帳號時，您可以從 [Create User] 頁面爲使用者指定委託。

您也可以從 [Work Items] 標籤委託工作項目，例如要核准的請求。請參閱第 180 頁的「委託工作項目」，以取得詳細資訊。

建立管理員

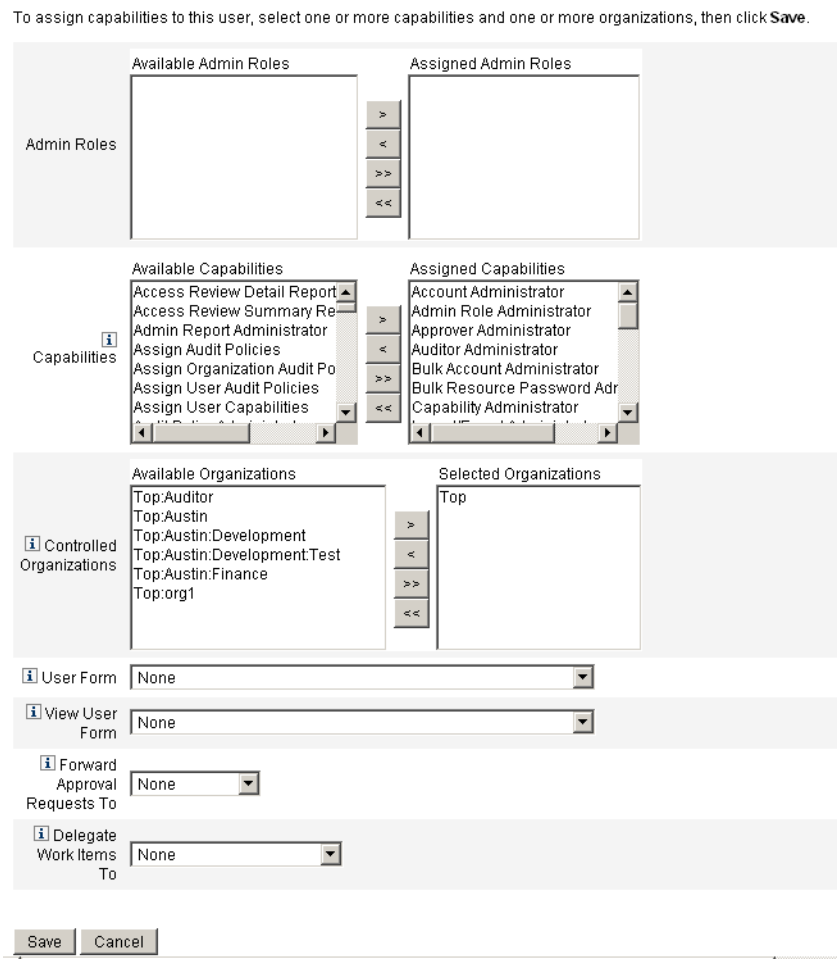
您可以透過延伸 Identity Manager 使用者的權能來建立 Identity Manager 管理員。建立或編輯使用者時，您可以給予他們管理控制權，方法是：

- 指定其可管理的組織
- 指定其管理組織中的權能
- 選取在建立與編輯 Identity Manager 使用者時將使用的表單 (若指定了允許其執行這些動作的權能)
- 選取接收等待核准請求的核准人 (若指定了允許其核准請求的權能)

若要授予使用者管理權限，請在功能表列中選取 **[Accounts]** 以移至 Identity Manager 的 [Accounts] 區域。對於新使用者，請從 [Create User] 頁面中選取 **[Security]** 標籤，以指定管理員屬性。

若要爲現有使用者指定管理員屬性，請從 [User Actions] 清單中選取 [Edit User Capabilities]，然後在 [Accounts] 清單中選取使用者並編輯該使用者的權能。開啓的安全性表單如下圖所示：

圖 5-1 [User Account Security] 頁面：指定管理員權限



選取一或多項以建立管理控制：

- **[Controlled Organizations]** — 選取一個或多個組織。管理員可控制所選組織或階層中其下任何組織的物件。其控制的範圍由其指定的權能進一步定義。您必須在此區域中進行選擇。
- **[Capabilities]** — 選取此管理員在其控制的組織中將擁有的一項或多項權能。如需有關 Identity Manager 權能的更多資訊或說明，請閱讀第 4 章「配置」。

- **[User Form]** — 選取此管理員在建立和編輯 Identity Manager 使用者時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。
- **[Forward Approval Requests To]** — 選取使用者，以將所有擱置的核准請求轉寄給該使用者。此管理員設定也可以在 [Approvals] 頁面中設定。
- **[Delegate Work Items To]** — 如果可用，使用此選項可指定對使用者帳號的委託。您可以指定您的 IDMManager、一個或多個已選取的使用者，也可以使用委託核准規則。

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：

- **[Organization]** — 當您建立組織時，您可以指定該組織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。
- **[Administrator]** — 當您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 4 章「配置」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。

管理員可以變更其他管理員的密碼，途徑有：

- **[Accounts] 區域** — 從清單中選取管理員，然後從 [User Actions] 清單中選取 [Change Password]。
- **[Edit User] 頁面** — 選取 **[Identity]** 表單標籤，然後輸入並確認新密碼。
- **[Passwords] 區域** — ，輸入管理員名稱，然後按一下 **[Change Password]**。

提示 輸入一個或多個字元，然後按一下 **[Find]** 以列出所有相符的項目。

管理員可以在 [Passwords] 區域變更其自己的密碼。選取 **[Passwords]**，然後選取 **[Change My Password]** 可以存取自助密碼欄位。

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。其他密碼限制可由設定於管理員資源的密碼策略來設定。

質疑管理員動作

您可以設定一個選項，要求管理員在處理特定帳號變更之前，提供他的 Identity Manager 登入密碼。如果密碼錯誤，則無法繼續執行帳號動作。

支援這個選項的 Identity Manager 頁有：

- 編輯使用者 (`account/modify.jsp`)
- 變更使用者密碼 (`admin/changeUserPassword.jsp`)
- 重設使用者密碼 (`admin/resetUserPassword.jsp`)

請按照以下章節中說明設定這些選項：

[Edit User Challenge] 選項

請按如下所示在 `account/modify.jsp` 頁面中設定此選項：

```
requestState.setOption(UserViewConstants.OP_REQUIRES_CHALLENGE, "email,
fullname, password");
```

其中，選項的值是一份以逗點分隔的清單，內含一個或多個使用者檢視屬性名稱：

- applications
- adminRoles
- assignedLhPolicy
- capabilities
- controlledOrganizations
- email
- firstname
- fullname
- lastname

- organization
- password
- resources
- roles

[Change User Password and Reset User Password Challenge] 選項

請按如下所示在 admin/changeUserPassword.jsp 與 admin/resetUserPassword 頁面中設定此選項：

```
requestState.setOption(UserViewConstants.OP_REQUIRES_CHALLENGE, "true");
```

其中，選項的值可以是 true 或 false。

變更認證問題的答案

使用 [Passwords] 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 **[Passwords]**，然後選取 **[Change My Answers]**。

如需有關認證的更多資訊，請參閱第 86 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
- Approvals

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做爲顯示名稱，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**給其他組織。

Identity Manager 管理員會另外指定，以**控制**組織。

建立組織

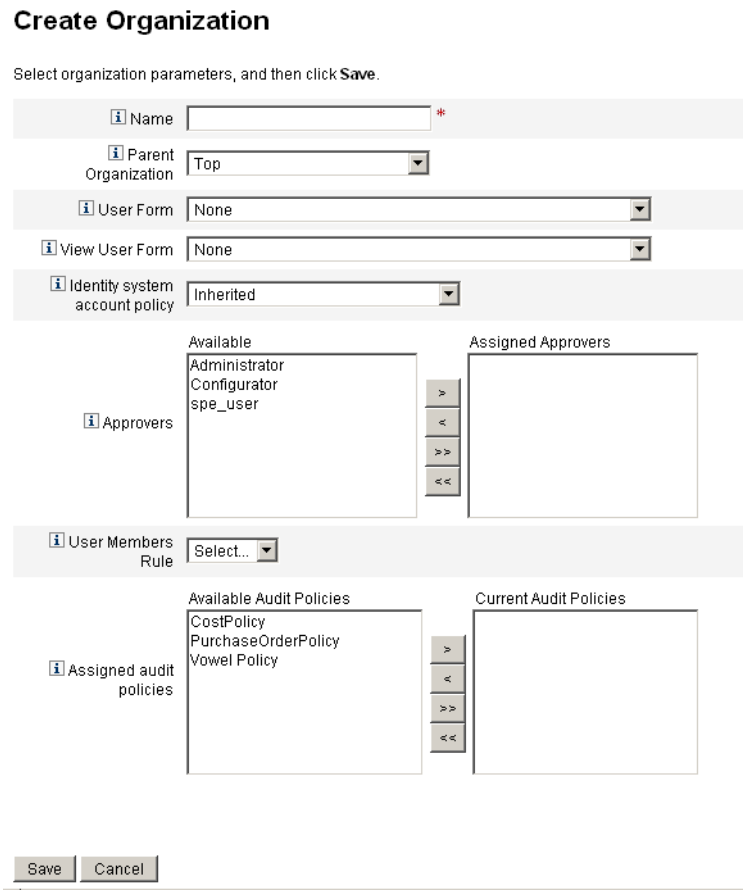
組織於 Identity Manager 帳號區域中建立。若要建立組織，請執行以下步驟：

1. 從功能表列中，選取 **[Accounts]**。
2. 從 [Accounts] 頁面的 [New Actions] 清單中，選取 **[New Organization]**。

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，然後從 [New Actions] 清單中選取 **[New Organization]**。

圖 5-2 將說明 [Create Organization] 螢幕。

圖 5-2 [Create Organization] 螢幕



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。組織成員資格由以下決定：

- **直接 (靜態) 指定** — 從 [Create User] 或 [Edit User] 頁面，將使用者直接指定給組織。(選取 **[Identity]** 表單標籤可顯示 [Organizations] 欄位。) 使用者必須直接指定給一個組織。
- **規則導向 (動態) 指定** — 藉由將評估時可傳回一組成員使用者的規則指定給組織，將使用者動態指定給組織。Identity Manager 將於以下情況評估使用者成員規則：

- 列出組織中的使用者時
- 尋找使用者 (透過 [Find Users] 頁面),包括搜尋具備使用者成員規則的組織中的使用者
- 請求使用者存取權，且目前管理員控制的組織具有使用者成員規則

從 [Create Organization] 頁面的 [User Members Rule] 欄位選擇使用者成員規則。圖 5-3 爲使用者成員規則的範例。

圖 5-3 建立組織：使用者成員規則選取

以下範例顯示了如何設定可以動態控制組織的使用者成員資格的使用者成員規則。

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

- 欲使某規則顯示在 [User Member Rule] 選項方塊中，其 `authType` 必須設定爲 `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` 會爲做爲 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`。

以下是使用者成員規則範例的語法範例。

代碼範例 5-1 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 [Create User] 或 [Edit User] 頁面指定一個或多個組織的管理控制。選取 **[Security]** 表單標籤可顯示 [Controlled Organizations] 欄位。

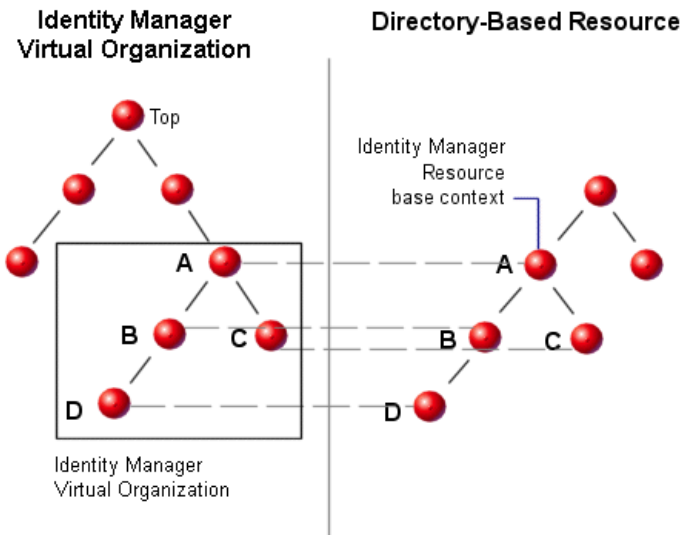
您也可以透過從 [Admin Roles] 欄位指定一個或多個管理角色，來指定組織的管理控制。

瞭解目錄結合與虛擬組織

目錄結合是一組階層相關的組織，它鏡射一組目錄資源的實際階層式容器。**目錄資源**透過利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射。目錄結合中的其餘虛擬組織爲頂層虛擬組織的**直接**或**間接**子系，而且還鏡射一個爲已定義資源的基底環境容器之子系的目錄資源容器。圖 5-4 說明了此結構。

圖 5-4 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。

您將目錄結合新增至 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，您可以隨時更新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

您可以在 Identity Manager 帳號區域中設定目錄結合：

1. 從 Identity Manager 功能表列中，選取 **[Accounts]**。
2. 在 [Accounts] 清單中，選取一個 Identity Manager 組織，然後在 [New Actions] 清單中，選取 [New Directory Junction]。

   您選取的組織將成爲設定的虛擬組織的父系組織。

   Identity Manager 顯示 [Create Directory Junction] 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 [Accounts] 清單中選取的組織；不過，您可以從清單中選取不同的父系組織。
   - **目錄資源** — 選取您要在虛擬組織中鏡射其結構的現有目錄之目錄資源。
   - **使用者表單** — 選取要套用至這個組織中的管理員的使用者表單。
   - **Identity Manager 帳號策略** — 選取策略或選取預設選項 (繼承的) 來繼承父系組織的策略。
   - **核准人** — 選取可以核准與這個組織相關的請求的管理員。

更新虛擬組織

此程序從選取的組織開始，向下更新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 [Organization Actions] 清單中，選取 [Refresh Organization]。

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 **[Delete]**。

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。

不是所有的 Identity Manager 使用者都需要爲其指定權能；只有那些將透過 Identity Manager 執行一個或多個管理動作的使用者才需要。例如，使用者要變更其密碼不需要指定的權能，但是要變更其他使用者的密碼則需要一個指定的權能。

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：

- **[Home]** 和 **[Help]** 標籤
- **[Passwords]** 標籤 (僅限 **[Change My Password]** 和 **[Change My Answers]** 子標籤)
- **Reports** (限於和管理員的特定責任相關的類型)

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

1. 在功能表列中，選取 **[Security]**。
2. 選取 **[Capabilities]** 標籤以顯示 Identity Manager 權能清單。

建立權能

若要建立權能，請按一下 **[New]**。命名新權能，然後選取要與此權能相關聯的權能、指定者和組織。您必須至少選取一個要爲其指定權能的組織。

編輯權能

若要編輯非保護的權能，請在清單中按一下滑鼠右鍵，然後選取 **[Edit]**。

您無法編輯內建權能，但是可以使用不同的名稱儲存它們以建立您自己的權能，或在您建立的權能中使用它們。

儲存並重新命名權能

若要**複製**權能 (以不同的名稱儲存權能以建立新權能)，請：

- 在清單中的權能上按一下滑鼠右鍵，然後選取 **[Save As]**。
- 輸入新名稱，然後按一下 **[OK]**。

您可以編輯新權能，即使複製的權能受到保護。

指定權能

從 [Create and Edit User] 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 [Security] 區域設定) 將權能指定給使用者。請參閱第 171 頁的「瞭解與管理管理員角色」，以取得詳細資訊。

權能階層

作業型權能位於下列功能性權能階層中：

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
    - 取消連結使用者
  - 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

- 連線權能
- 連線權能規則
- 連線控制的組織規則
- 連線組織

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
- Auditor 定期存取檢閱管理員
  - Auditor 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

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

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

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
  -
- 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

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

使用者帳號管理員

- 刪除使用者
- 密碼管理員
- 建立使用者
- 停用使用者
- 啓用使用者
- 匯入使用者
- 重新命名使用者
- 解除鎖定使用者
- 更新使用者

檢視組織

- 列出組織

檢視資源

- 列出資源

Waveset 管理員

權能定義

表 5-1 描述各個作業型權能，並列出每個權能可以存取的標籤與子標籤。這些權能按名稱的字母順序列出。

所有權能都允許使用者或管理員存取 **[Passwords]** > **[Change My Password]** 和 **[Change My Answers]** 標籤。

表 5-1 Identity Manager 權能說明

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	**[Reports]** > **[Run Reports]** 標籤，**[View Reports]** 標籤 — 僅 [Access Review Detail Reports] **[Reports]** > **[View Dashboards]**
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	**[Reports]** — 僅 [Access Review Summary Reports **[Reports]** > **[View Dashboards]**

表 5-1 Identity Manager 權能說明 (繼續)

權能	允許管理員 / 使用者：	可以存取這些標籤與子標籤：
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。	**[Accounts]** — **[List Accounts]**、**[Find Users]**、**[Extract to File]**、**[Load from File]**、**[Load from Resource]** 標籤
		[Passwords] — 所有子標籤
		[Work Items] — **[Approvals]** 子標籤
		[Tasks] — 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。	**[Reports]** — **[Manage Reports]**，**[Run Reports]** 子標籤 (僅 [Administrator Report])
管理員角色管理員	建立、編輯和刪除管理員角色。	**[Security]** — **[Admin Roles]** 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 [Default]**
指定稽核策略	為使用者帳號和組織指定稽核策略。	**[Accounts]** — [User Actions] 清單中的 **[Edit User Audit Policy]**。
		[Accounts] — **[Organization Actions] 清單中的 [Edit Organization Audit Policy]**。
指定組織稽核策略	僅為組織指定稽核策略。	**[Accounts]** — [Organization Actions] 清單中的 **[Edit Organization Audit Policy]**；**[List Accounts]** 標籤
指定使用者稽核策略	僅為使用者指定稽核策略。	**[Accounts]** — [User Actions] 清單中的 **[Edit User Audit Policy]**；**[Find Users]** 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)。	**[Accounts]** — **[List Accounts]** (僅 [Edit])，**[Find Users]** 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「啟用使用者」)。
稽核策略管理員	建立、修改和刪除稽核策略。	**[Compliance]** — **[Manage Policies]**
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」。	**[Reports]** — 僅 [Audit Policy Scan Report]
稽核報告管理員	建立、修改、刪除和執行稽核報告。	**[Reports]** — 僅 [Audit Report]
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」。	**[Reports]** — 僅 [Audited Attribute Report]
稽核記錄報告管理員	建立、修改、刪除和執行「稽核記錄報告」。	**[Reports]** — 僅 [AuditLog Report]
Auditor 存取掃描管理員	建立、編輯和刪除定期存取檢閱掃描	**[Compliance]** — **[Manage Access Scans]**

表 5-1 Identity Manager 權能說明 (繼續)

權能	允許管理員 / 使用者：	可以存取這些標籤與子標籤：
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。	**[Compliance]** — 所有子標籤 **[Reports]** — [Run Reports]、[View Reports] 和 [Manage Auditor Reports] **[Accounts]** — [Edit User Audit Policies] 和 [Edit Organization Audit Policies] 動作。
Auditor 驗證者	啟用組織安全性後，需要驗證其他使用者的驗證。	**僅 [Default]**
Auditor 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。	**[Compliance]** — **[Manage Access Scans]**、**[Access Review]** 子標籤
Auditor 修正者	補救、緩解和轉寄稽核策略違規。	**[Remediations]** — 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。	**[Reports]** — 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。	**[Accounts]** — **[List Accounts]**、**[Find Users]** 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。	**[Reports]** — 僅 [AuditPolicy Violation History Report]
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。	**[Accounts]** — 所有子標籤 **[Passwords]** — 所有子標籤 **[Approvals]** — 所有子標籤 **[Tasks]** — 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。	**[Accounts]** — **[List Accounts]**、**[Find Users]**、**[Launch Bulk Actions]** 子標籤。無法建立或刪除使用者。 **[Passwords]** — 所有子標籤 **[Approvals]** — 所有子標籤 **[Tasks]** — 所有子標籤
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。	**[Accounts]** — **[List Accounts]**、**[Find Users]**、**[Launch Bulk Actions]** 子標籤。無法建立、刪除或指定給使用者的權能。 **[Passwords]** — 所有子標籤 **[Tasks]** — 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)。	**[Accounts]** — **[List Accounts]** (僅 [Create])、**[Find Users]**、**[Launch Bulk Actions]** 子標籤 **[Tasks]** — 所有子標籤

表 5-1 Identity Manager 權能說明 (繼續)

權能	允許管理員 / 使用者：	可以存取這些標籤與子標籤：
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)。	**[Accounts]** — **[List Accounts]** (僅 [Create])、**[Find Users]**、**[Launch Bulk Actions]** 子標籤
		[Tasks] — 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)。	**[Accounts]** — **[List Accounts]** (僅 [Delete])、**[Find Users]**、**[Launch Bulk Actions]** 子標籤
		[Tasks] — 所有子標籤
批次取消佈建使用者	刪除並取消連結現有資源帳號 (對於個別使用者並使用批次作業)。	**[Accounts]** — **[List Accounts]** (僅 [Deprovision])、**[Find Users]**、**[Launch Bulk Actions]** 子標籤
		[Tasks] — 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)。	**[Accounts]** — **[List Accounts]** (僅 [Disable])、**[Find Users]**、**[Launch Bulk Actions]** 子標籤
		[Tasks] — 所有子標籤
批次啟用使用者	啟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)。	**[Accounts]** — **[List Accounts]** (僅 [Enable])、**[Find Users]**、**[Launch Bulk Actions]** 子標籤
		[Tasks] — 所有子標籤
批次取消指定使用者	取消指定並取消連結現有資源帳號 (對於個別使用者並使用批次作業)。	**[Accounts]** — **[List Accounts]** (僅 [Unassign])、**[Find Users]**、**[Launch Bulk Actions]** 子標籤
		[Tasks] — 所有子標籤
批次取消連結使用者	取消連結現有資源帳號 (對於個別使用者並使用批次作業)。	**[Accounts]** — **[List Accounts]** (僅 [Unlink])、**[Find Users]**、**[Launch Bulk Actions]** 子標籤
		[Tasks] — 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)。	**[Accounts]** — **[List Accounts]** (僅 [Update])、**[Find Users]**、**[Launch Bulk Actions]** 子標籤
		[Tasks] — 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。	**[Accounts]** — 所有子標籤
		[Passwords] — 所有子標籤
		[Tasks] — 所有子標籤
權能管理員	建立、修改和刪除權能。	**[Configure]** — **[Capabilities]** 子標籤

表 5-1 Identity Manager 權能說明 (繼續)

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	**[Accounts]** — 所有子標籤。無法刪除使用者。 **[Passwords]** — 所有子標籤 **[Approvals]** — 所有子標籤 **[Tasks]** — 所有子標籤 **[Reports]** — 在範圍內建立管理員與使用者報告、執行及編輯報告，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。	**[Tasks]** — **[Find Tasks]**、**[All Tasks]**、**[Run Tasks]** 子標籤 **[Resources]** — 對於 Active Sync 資源：[Edit] 動作功能表，[Edit Active Sync Parameters]
變更密碼管理員	變更使用者和資源帳號密碼。	**[Accounts]** — **[List Accounts]**、**[Find Users]** 子標籤 (僅限 [Change Password]) **[Passwords]** — 所有子標籤 **[Tasks]** — 所有子標籤。僅 [Export Password Scan] 作業 (從 **[Run Tasks]** 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。	**[Accounts]** — **[List Accounts]**、**[Find Users]** 子標籤 (僅限 [Change Password]；必須先驗證才能執行動作) **[Passwords]** — 所有子標籤 **[Tasks]** — 所有子標籤。僅 [Export Password Scan] 作業 (從 **[Run Tasks]** 子標籤)
變更資源密碼管理員	變更資源管理員帳號密碼。	**[Tasks]** — 所有子標籤 **[Resources]** — **[List Resources]** 子標籤。僅變更資源密碼 (從 [Actions] 功能表中的 **[Manage Connection] > [Change Password]**)
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	**[Accounts]** — **[List Accounts]**、**[Find Users]** 子標籤。無法建立、刪除或指定給使用者的權能。 **[Passwords]** — 所有子標籤 **[Tasks]** — 所有子標籤
配置稽核	配置系統中稽核的事件和配置群組。	**[Configure]** — **[Audit Events]** 子標籤

表 5-1 Identity Manager 權能說明 (繼續)

權能	允許管理員 / 使用者：	可以存取這些標籤與子標籤：
配置憑證	配置可信任的憑證和 CRL。	**[Security]** — **[Certificates]** 子標籤
控制 Active Sync 資源管理員	控制 Active Sync 資源狀態 (如開始、停止和更新)	**[Tasks]** — **[Find Tasks]**、**[All Tasks]**、**[Run Tasks]**
		[Resources] — 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	**[Accounts]** — **[List Accounts]** (僅 [Create])、**[Find Users]** 子標籤
		[Tasks] — 所有子標籤
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。	**[Accounts]** — **[List Accounts]** (僅 [Delete])、**[Find Users]** 子標籤
		[Tasks] — 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。	**[Accounts]** — **[List Accounts]** (僅 [Delete])、**[Find Users]** 子標籤
		[Tasks] — 所有子標籤
取消佈建使用者	刪除並取消連結現有的資源帳號。不包括批次處理作業。	**[Accounts]** — **[List Accounts]** (僅 [Deprovision])、**[Find Users]** 子標籤
		[Tasks] — 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	**[Accounts]** — **[List Accounts]** (僅 [Disable])、**[Find Users]** 子標籤
		[Tasks] — 所有子標籤
啟用使用者	啟用現有的使用者和資源帳號。不包括批次作業	**[Accounts]** — **[List Accounts]** (僅 [Enable])、**[Find Users]** 子標籤
		[Tasks] — 所有子標籤
匯入使用者	從定義的資源匯入使用者。	**[Accounts]** — **[Extract to File]**、**[Load from File]**、**[Load from Resource]** 子標籤
匯入 / 匯出管理員	匯入和匯出所有類型的物件。	**[Configure]** — **[Import Exchange File]** 子標籤
授權管理員	設定 Identity 系統產品授權	提供 `lh license` 指令存取。(此能力不提供非管理員介面標籤。)
登入管理員	編輯指定登入介面的一組登入模組。	**[Configure]** — **[Login]** 子標籤
中介檢視管理員	修改身份識別屬性配置	**[Meta View]** — **[Identity Attributes]** 標籤
組織管理員	建立、編輯和刪除組織。	**[Accounts]** — **[List Accounts]** 子標籤 (僅 [Edit Organizations]、[Create Organization]、[Edit Directory Junction]、[Create Directory Junction] 和 [Delete Organizations])

表 5-1 Identity Manager 權能說明 (繼續)

權能	允許管理員 / 使用者：	可以存取這些標籤與子標籤：
組織核准人	核准新組織請求。	**[Work Items]** — **[Approvals]** 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。	**[Reports]** — 僅 [Organization Violation History Report]
密碼管理員	變更和重設使用者與資源帳號密碼。	**[Accounts]** — **[List Accounts]** (僅限列出、變更及重設密碼)、**[Find Users]** 子標籤 **[Passwords]** — 所有子標籤 **[Tasks]** — 所有子標籤
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。	**[Accounts]** — **[List Accounts]** (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)、**[Find Users]** 子標籤 **[Passwords]** — 所有子標籤 **[Tasks]** — 所有子標籤
策略管理員	建立、編輯和刪除策略。	**[Configure]** — **[Policy]** 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」。	**[Reports]** — 僅 [Policy Summary Report]
調解管理員	編輯調解策略和控制調解作業。	**[Server Tasks]** — 所有子標籤 (檢視調解作業)。 **[Resources]** — **[List Resources]** 子標籤。
調解報告管理員	建立、編輯、刪除和執行調解報告。	**[Reports]** — **[Run Reports]** (僅 [Account Index Report])、**[Manage Reports]** 子標籤
調解請求管理員	管理調解請求。	**[Tasks]** — 所有子標籤 **[Resources]** — **[List Resources]** 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。	**[Tasks]** — 所有子標籤 (檢視作業，執行角色同步化)。 **[Configure]** — **[Remedy Integration]** 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。	**[Accounts]** — [List Accounts] 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。	**[Tasks]** — 所有子標籤 (檢視作業，執行角色同步化)。 **[Reports]** — 所有子標籤

表 5-1 Identity Manager 權能說明 (繼續)

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	重設使用者和資源帳號密碼。	**[Accounts]** — **[List Accounts]**、**[Find Users]** 子標籤 (僅限 [Reset Password])
		[Passwords] — 所有子標籤
		[Tasks] — 所有子標籤。僅 [Export Password Scan] 作業 (從 **[Run Tasks]** 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。	**[Accounts]** — **[List Accounts]**、**[Find Users]** 子標籤 (僅限 [Reset Password]；必須先驗證才能執行動作)
		[Passwords] — 所有子標籤
		[Tasks] — 所有子標籤。僅 [Export Password Scan] 作業 (從 **[Run Tasks]** 子標籤)
重設資源密碼管理員	重設資源管理員帳號密碼。	**[Tasks]** — **[Find Tasks]**、**[All Tasks]**、**[Run Tasks]** 子標籤
		[Resources] — **[List Resources]** 子標籤。僅重設資源密碼 (透過 [Actions] 功能表的 **[Manage Connection] --> 重設密碼**)
資源管理員	建立、修改和刪除資源。	**[Reports]** — 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。
		[Resources] — **[List Resources]** 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)。
資源群組管理員	建立、編輯和刪除資源群組。	**[Resources]** — **[List Resource Groups]** 子標籤
資源物件管理員	建立、修改和刪除資源物件。	**[Tasks]** — **[Find Tasks]**、**[All Tasks]**、**[Run Tasks]** 子標籤 (檢視涉及資源物件的作業)
		[Resources] — **[List Resources]** 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。	**[Tasks]** — **[Find Tasks]**、**[All Tasks]**、**[Run Tasks]** 子標籤
		[Resources] — **[List Resources]** 子標籤。僅變更資源密碼 (從 [Actions] 功能表中的 **[Manage Connection] > [Change Password]**)
資源報告管理員	建立、編輯、刪除和執行資源報告。	**[Reports]** — 所有子標籤 (僅限資源報告)

表 5-1 Identity Manager 權能說明 (繼續)

權能	允許管理員 / 使用者：	可以存取這些標籤與子標籤：
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。	**[Reports]** — 僅 [Resource Violation History Report]
風險分析管理員	建立、編輯、刪除和執行風險分析。	**[Risk Analysis]** — 所有子標籤
角色管理員	建立、修改和刪除角色。	**[Tasks]** — **[Find Tasks]**、**[All Tasks]**、**[Run Tasks]** 子標籤 (同步化角色)
		[Roles] — 所有子標籤
角色報告管理員	建立、編輯、刪除和執行資源報告。	**[Reports]** — 僅 [Role Report]
執行存取檢閱詳細資訊報告	執行存取檢閱詳細資訊報告	**[Reports]** — 僅 [Access Review Detail Report]
執行存取檢閱摘要報告	執行存取檢閱摘要報告	**[Reports]** — 僅 [Access Review Summary Report]
執行管理員報告	執行管理員報告。	**[Reports]** — 僅 [Admin Report]。
執行稽核策略掃描管理員	執行和管理稽核策略掃描報告	[Reports] — 僅 [Audit Policy Scan Report]
執行稽核策略掃描報告	執行稽核策略掃描報告。	**[Reports]** — 僅 [Audit Policy Scan Report]
執行稽核報告	執行稽核報告。	**[Reports]** — 僅 [AuditLog Report] 及 [Usage Report]
執行已稽核的屬性報告	執行「已稽核的屬性報告」。	**[Reports]** — 僅 [Audited Attribute Report]
		[Reports] > [View Dashboards]
執行 Auditor 報告	執行任何 Auditor 報告。	**[Reports]** — 任何 Auditor 報告
		[Reports] > [View Dashboards]
執行稽核記錄報告	執行「稽核記錄報告」。	**[Reports]** — 僅 [AuditLog Report]
執行稽核策略違規歷程記錄	執行「組織違規歷程記錄」報告。	**[Reports]** — 僅 [AuditPolicy Violation History Report]
		[Reports] > [View Dashboards]
執行策略摘要報告	執行「策略摘要報告」。	**[Reports]** — 僅 [Policy Summary Report]
執行組織違規歷程記錄	執行「組織違規歷程記錄」報告。	**[Reports]** — 僅 [Organization Violation History Report]
		[Reports] > [View Dashboards]
執行調解報告	執行調解報告。	**[Reports]** — 僅 [AuditLog Report] 及 [Usage Report]
執行資源報告	執行資源報告。	**[Reports]** — 僅 [AuditLog Report] 及 [Usage Report]

表 5-1 Identity Manager 權能說明 (繼續)

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。	**[Reports]** — 僅 [Resource Violation History Report]
執行風險分析	執行風險分析。	**[Reports]** — [Run Risk Analysis]、[View Risk Analysis] 子標籤
執行角色報告	執行角色報告。	**[Reports]** — 僅 [Role Report]
執行作業報告	執行作業報告。	**[Reports]** — 僅 [Task Report]
執行使用者存取報告	執行「詳細使用者報告」。	**[Reports]** — 僅 [User Access Report] **[Reports] > [View Dashboards]**
執行使用者報告	執行使用者報告。	**[Reports]** — 僅 [User Report]
執行違規摘要報告	執行「違規摘要」報告。	**[Reports]** — 僅 [Violation Summary Report] **[Reports] > [View Dashboards]**
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。	**[Accounts]** — **[List Accounts]** (刪除、建立、更新、編輯、變更及編輯密碼)、**[Find Users]** 子標籤 (稽核報告) **[Passwords]** — 所有子標籤 **[Tasks]** — **[Find Tasks]**、**[All Tasks]**、**[Run Tasks]** 子標籤 **[Reports]** — 所有子標籤 **[Resources]** — **[List Resources]** (列出及控制資源物件)。 **[Security]** — **[Policies]**、**[Login]** 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。	**[Report]** — 僅限對責任分離報告的所有動作
執行責任分離報告	執行責任分離報告	**[Reports]** — 僅 [Separation of Duties Report] **[Reports] > [View Dashboards]**
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。	**[Security]** — **[Admin Roles]** 標籤

表 5-1 Identity Manager 權能說明 (繼續)

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。	**[Accounts]** — **[Manage Service Provider Users]** 子標籤 **[Server Tasks] > [Service Provider Transactions]** 標籤 **[Reports] > [View Dashboards]** 標籤 **[Reports] > [Dashboard Configuration]** 標籤 **[Service Provider]** — 所有子標籤
「服務提供者」的建立使用者	為服務提供者 (企業外部網路) 使用者建立使用者帳號。	**[Accounts]** — **[Manage Service Provider Users]** 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。	**[Accounts]** — **[Manage Service Provider Users]** 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。	**[Accounts]** — **[Manage Service Provider Users]** 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。	**[Accounts] > [Manage Service Provider Users]** — 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。	**[Accounts]** — **[Manage Service Provider Users]** 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。	**[Security]** — **[Capabilities]** 子標籤
作業報告管理員	建立、編輯、刪除和執行作業報告。	**[Reports]** — 僅 [Task Report]。
取消指定使用者	取消指定並取消連結現有的資源帳號。不包括批次處理作業。	**[Accounts]** — **[List Accounts]** (僅 [Unassign])、**[Find Users]** 子標籤 **[Tasks]** — 所有子標籤
取消連結使用者	取消連結現有的資源帳號。不包括批次處理作業。	**[Accounts]** — **[List Accounts]** (僅 [Unlink])、**[Find Users]** 子標籤 **[Tasks]** — 所有子標籤
取消鎖定使用者	解除鎖定現有使用者支援解除鎖定的資源帳號。不包括批次處理作業。	**[Accounts]** — **[List Accounts]** (僅 [Unlock])，**[Find Users]** 子標籤 **[Tasks]** — **[Find Tasks]**、**[All Tasks]**、**[Run Tasks]** 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。	**[Accounts]** — 編輯和更新使用者 **[Tasks]** — 管理現有作業 (從 **[All Tasks]** 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	**[Reports]** — 僅 [User Access Report] **[Reports] > [View Dashboards]**

表 5-1 Identity Manager 權能說明 (繼續)

權能	允許管理員 / 使用者：	可以存取這些標籤與子標籤：
使用者帳號管理員	對使用者執行所有作業。	**[Accounts]** — **[List Accounts]**、**[Find Users]**、**[Extract to File]**、**[Load from File]**、**[Load from Resource]** 子標籤。無法指定使用者權能 (**[List Accounts]** 子標籤上的 **[Security]** 表單標籤)。 **[Tasks]** — **[Find Tasks]**、**[All Tasks]**、**[Run Tasks]** 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。	**[Reports]** — [Run User Report]。
檢視使用者	檢視個別使用者詳細資訊。	**[Accounts]** — 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。	**[Reports]** — 僅 [Violation Summary Report] **[Reports] > [View Dashboards]**
Waveset 管理員	執行系統範圍的作業，如修改系統配置物件。	**[Server Tasks]** — 所有子標籤。同步化角色、編輯來源配接器範本，並排程報告。 **[Reports]** — 所有子標籤 **[Resources]** — [List Resources] (僅列出，不允許變更動作) **[Configure]** — **[Audit]**、**[Email Templates]**、**[Form and Process Mappings]** 和 **[Servers]** 子標籤

瞭解與管理管理員角色

管理員角色可將權能和控制範圍或受管理組織的唯一集合指定給一個或多個管理員。可將多個管理員角色指定給一個管理員。這可讓管理員在一個控制範圍內具有一個權能集，而在另一個控制範圍內具有不同的權能集。

例如，對於指定了某管理員角色的管理員，該管理員角色可授予其建立和編輯屬於該管理員角色所指定受控制組織成員之使用者的權限。然而，指定給該管理員的其他管理員角色僅可授予其在該管理員角色所指定受控制組織中變更使用者密碼的權限。

建議將管理員角色用於授予管理員權限，而非直接將權能和受控制組織指定給使用者。管理員角色允許重複使用權能及範圍或控制配對，並可簡化大量使用者的管理員權限的管理工作。

可以直接或間接 (動態) 將權能或組織 (或二者) 指定給某個管理員角色：

- **直接** — 使用此方法，會將權能和 / 或受控制組織明確指定給管理員角色。例如您可將使用者報告管理員權能與 Top 受控制組織指定給某管理員角色。
- **動態 (間接)** — 此方法使用權能和受控制組織指定**規則**。每當已指定該管理員角色的管理員登入時，均會評估該規則，以根據認證管理員動態確定權能和 / 或受控制組織的明確集合。

  例如，當使用者登入時：

  - 如果其 Active Directory (AD) 使用者稱謂爲**管理者**，則該權能規則可能會傳回 [Account Administrator] 做爲要指定的權能。
  - 如果其 Active Directory (AD) 使用者部門爲**銷售**，則受控制組織規則可能傳回 [Marketing] 做爲要指定的受控制組織。

請參閱以下有關設定這些規則的重要資訊。

可以直接或間接 (動態) 將管理員角色指定給管理員：

- **直接** — 明確將管理員角色指定給管理員 (使用者帳號)。
- **間接 (動態)** — 使用管理員角色規則來指定管理員角色。Identity Manager 會在每次管理員登入時對該規則進行評估，以確定是否要將管理員角色指定給認證管理員。

  例如，當使用者登入時，如果其 Active Directory (AD) 使用者城市爲 `Austin` 並且州爲 `Texas`，則該規則可能傳回 `true`。這樣，便指定了管理員角色。

備註 可爲每個登入介面 (例如，使用者介面或管理員介面) 啓用或停用將管理員角色動態指定給使用者，方法是將系統配置屬性 `security.authz.checkDynamicallyAssignedAdminRolesAtLoginTo.`*`logininterface`* 設定爲 `true` 或 `false`。所有介面的預設均爲 false。

管理員角色規則

Identity Manager 提供了可用於建立管理員角色規則的範例規則。這些規則位於 Identity Manager 安裝目錄中的 `sample/adminRoleRules.xml`。表 5-2 提供了規則名稱以及您必須爲規則指定的 `authType`。

表 5-2 管理員角色範例規則

規則名稱	authType
受控制組織規則	ControlledOrganizationsRule
權能規則	CapabilitiesRule
已爲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範例規則的資訊，請參閱 「服務提供者管理」一章中第 414 頁的 「委託管理」。

使用者管理員角色

Identity Manager 包含內建管理員角色，名爲 「使用者管理員角色」。依預設，未向其指定權能或受控制組織。您無法將其刪除。此管理員角色在登入時即已指定給所有使用者 (一般使用者和管理員)，而與其登入的介面 (例如使用者介面、管理員介面、主控台介面或 IDE 介面) 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 414 頁的 「委託管理」。

您可以透過管理員介面編輯使用者管理員角色 (選取 **[Security]**，然後選取 **[Admin Roles]**)。

由於透過此管理員角色靜態指定的任何權能或控制的組織，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。

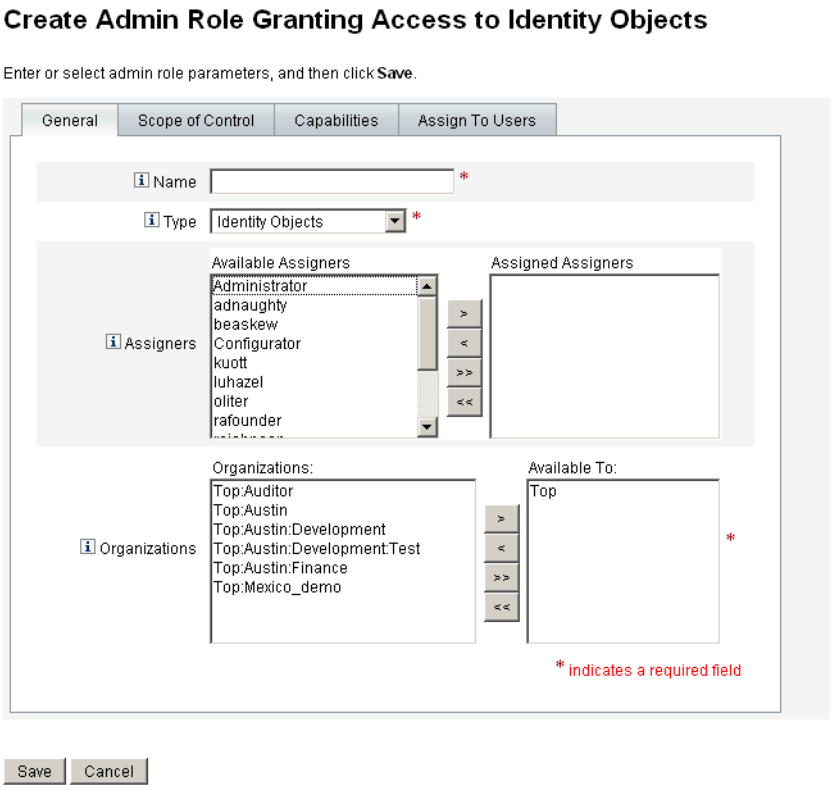
然而如果使用者應該要能在工作流程外 (也可能在工作流程內) 存取一個或多個物件，則利用使用者管理員角色動態指定權能和受控制組織的方式，就能讓這些物件有動態、精細的授權機制。

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 **[Security]**，然後按一下 **[Admin Roles]** 標籤。[Admin Roles] 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 **[New]** 可建立管理員角色。Identity Manager 會顯示 [Create Admin Role] 選項 (如圖 5-5 所示)。[Create Admin Role] 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 5-5 管理員角色建立頁面：[General] 標籤 :



[General] 標籤

可使用 [Create Admin Role] 或 [Edit Admin Role] 檢視的 [General] 標籤來指定管理員角色的以下基本特徵：

- **[Name]** — 此管理員角色的唯一名稱。

  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

- **[Type]** — 爲類型選取 **[Identity Objects]** 或 **[Service Provider Users]**。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 Objects]。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 [Service Provider Users]。

備註 如需有關建立管理員角色以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 414 頁的 「委託管理」。

- **[Assigners]** — 選取可以將此管理員角色指定給其他使用者的使用者。

  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 [Assign User Capabilities] 權能，請選取一個或多個使用者做爲 [Assigners]，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。

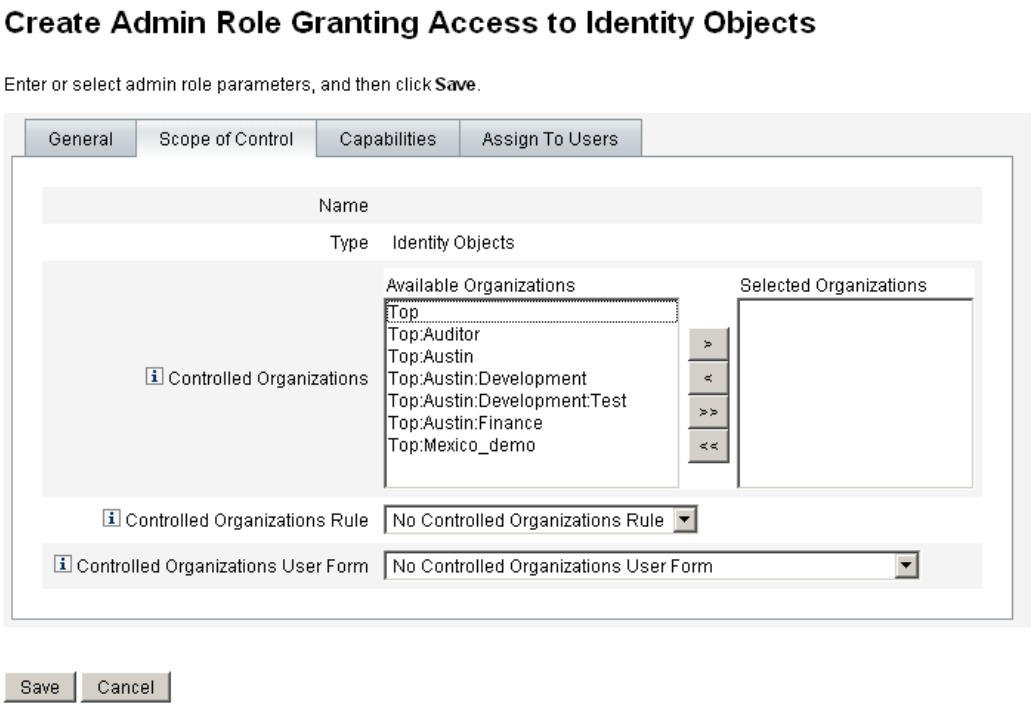
- **[Organizations]** — 選取可使用此管理員角色的一或多個組織。這是必填欄位。

  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

使用此標籤 (如圖 5-6 所示) 可指定此組織的成員可以管理的組織，或指定可確定該管理員角色之使用者所要管理組織的規則，以及爲該管理員角色選取使用者表單。

圖 5-6 建立管理員角色：控制範圍



- **[Controlled Organizations]** — 從 [Available Organizations] 清單中選取此管理員角色有權管理的組織。
- **[Controlled Organizations Rule]** — 爲已指定該管理員角色的使用者所要控制的零個或多個組織選取在使用者登入時要進行評估的規則。選取的規則必須具有 `ControlledOrganizationsRule` authType。依預設，不會選取任何受控制組織規則。
- **[Controlled Organizations User Form]** — 選取使用者表單，已指定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受控制組織的使用者時使用該表單。依預設，不會選取任何受控制組織使用者表單。

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 [Capabilities] 標籤上，可選取以下選項：

- **[Capabilities]** — 這些是管理員角色使用者所用有的對其受控制組織的特定權能 (管理權限)。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 [Assigned Capabilities] 清單。
- **[Capabilities Rule]** — 選取使用者登入時將評估的規則，將決定爲已指定該管理員角色的使用者授予的零個或多個權能之清單。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 [Create Admin Role] 或 [Edit Admin Role] 檢視中的 [Assign To Users] 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。
- 如果沒有將使用者表單直接或透過管理員角色間接指定給管理員，則會使用指定給管理員之成員組織的使用者表單 (從管理員的成員組織開始，直到 `Top` 的下一層級)。

- 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。

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 [Work Items] 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：

- **[Approvals]** — 對新帳號或帳號變更的核准請求。
- **[Attestations]** — 檢視並核准使用者權限的請求。
- **[Remediations]** — 修正或緩解使用者帳號策略違規的請求。
- **[Other]** — 標準類型的動作項目請求，但有一個類型除外，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，請按一下功能表列中的 **[Work Items]** 標籤。您可以存取您的工作項目以透過此標籤管理請求，或選取其中一種工作項目類型以列出對此類型的請求。

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 [Work Items] 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 [Work Items] 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。

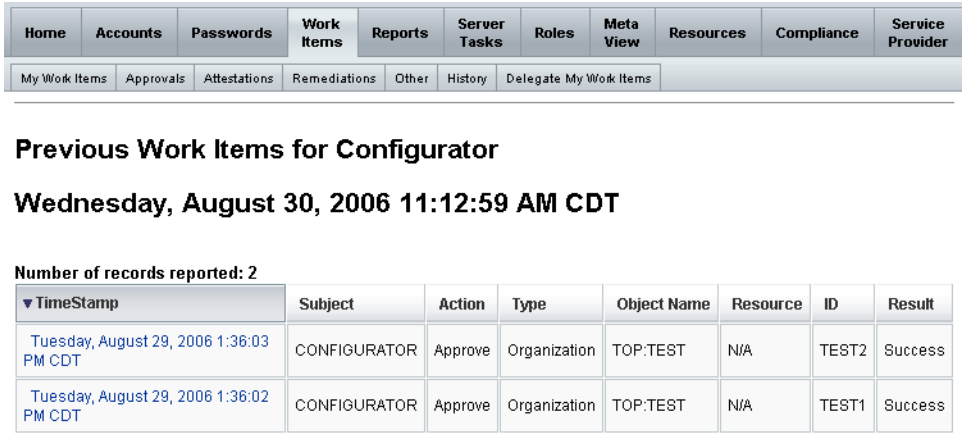
如需有關回應請求的更多資訊，請參閱以下主題：

- 第 180 頁的「帳號核准」
- 第 367 頁的「管理驗證責任」
- 第 348 頁的「修正與緩解」

檢視工作項目歷程記錄

使用 [Work Items] 區域中的 [History] 標籤可檢視先前工作項目動作的結果。圖 5-7 爲工作項目歷程記錄檢視範例。

圖 5-7 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。以下項目可用於委託工作項目：

- **[My Manager]** — 將工作項目請求委託給爲您帳號指定的管理員。
- **[Selected Users]** — 將工作項目請求委託給您從搜尋結果清單中選取的一個或多個使用者。
- **[Delegate Approvers Rule]** — 指定解析工作項目時要評估的規則。請從可用規則中選取規則。

若要停止委託工作項目，請在 [Delegate Work Items] 頁面中選取 **[None]**。

帳號核准

將使用者新增至 Identity Manager 系統時，指定爲新帳號**核准人**的管理員必須驗證帳號建立。Identity Manager 支援三個核准種類，並套用至以下 Identity Manager 物件：

- **[Organization]** — 若要將使用者帳號增加至組織，需要核准。
- **[Role]** — 若要將使用者帳號指定給角色，需要核准。
- **[Resource]** — 若要授予使用者帳號存取資源的權限，需要核准。

備註 您可以將 Identity Manager 配置爲數字簽名的核准。如需說明，請參閱第 183 頁的「配置數位簽署的核准」。

設定核准人

爲這些種類中的每一種設定核准人是可選作業，但建議執行這個作業。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。

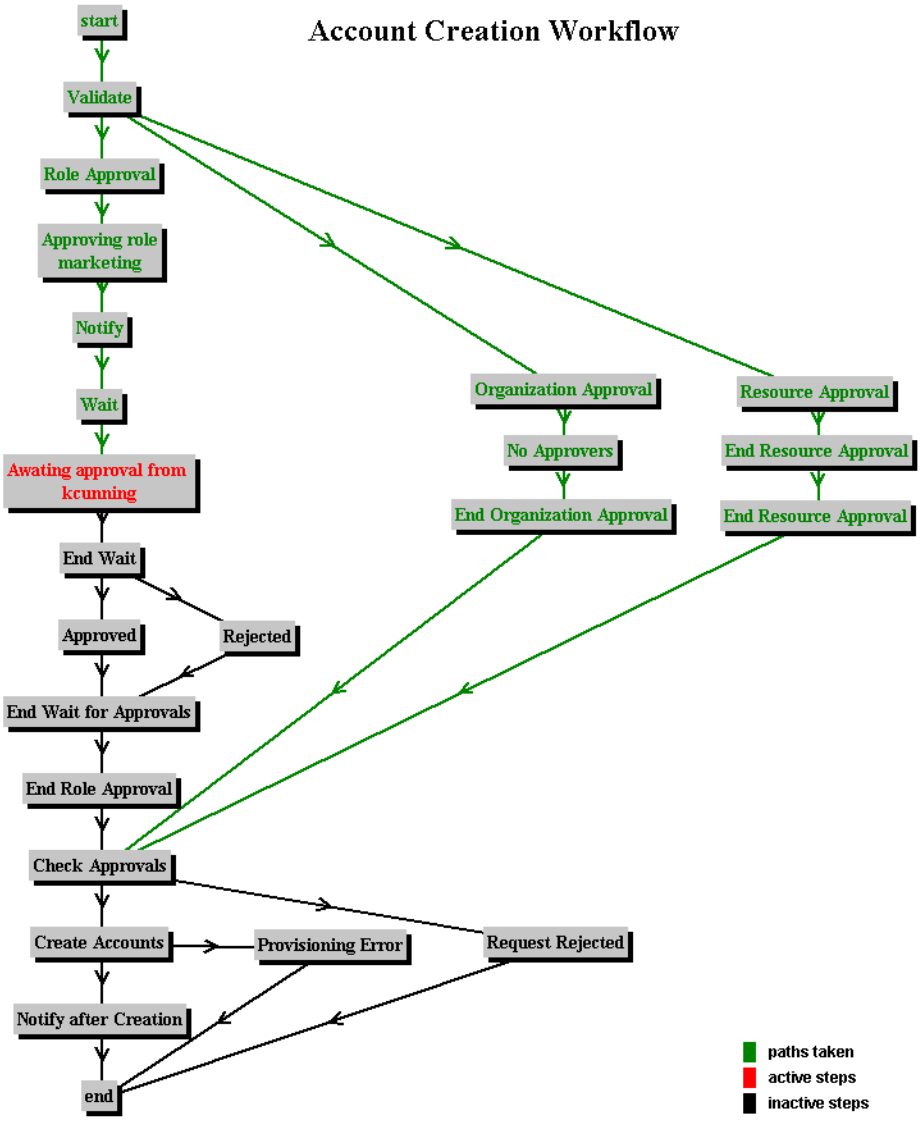
您可以將多個核准人指定給每個種類。因爲種類中只需要一次核准，您可以設定多個核准人以協助確保工作流程不會延遲或終止。若某個核准人無法使用，則其他核准人可以處理請求。核准僅適用於帳號設定。依預設，帳號更新與刪除不需要核准；然而，您可以自訂此程序，使其需要核准。

Identity Manager 會用一個工作流程圖來說明核准程序及帳號建立請求的狀態。您可以自訂工作流程，方法是使用 Identity Manager IDE 變更核准流程、擷取帳號刪除與擷取更新。

如需有關 IDE、工作流程以及變更核准工作流程之圖示範例的更多資訊，請參閱「Identity Manager Workflows, Forms, and Views」。

圖 5-8 說明了帳號建立工作流程，以及工作流程程序中適合進行核准的位置。

圖 5-8 帳號建立工作流程



Identity Manager 核准人既可核准也可拒絕核准請求。若要核准使用數位簽名的帳號，您必須先按照第 183 頁的 「配置數位簽署的核准」中的說明設定數位簽名。

您可以從 Identity Manager 介面的 [Work Items] 區域檢視擱置核准與管理核准。在 [Work Items] 頁面中，按一下 **[My Work Items]** 以檢視擱置核准。按一下 **[Approvals]** 標籤以管理核准。

簽署核准

遵循下列步驟來簽署核准。

1. 在 Identity Manager 管理員介面中，選取 **[Work Items]**。
2. 按一下 **[Approvals]** 標籤。
3. 從清單中選取一或多個核准。
4. 輸入核准註釋，然後按一下 **[Approve]**。

   Identity Manager 提示您並詢問是否信任該 Applet。
5. 按一下 **[Always]**。

   Identity Manager 將顯示一個註有日期的核准摘要。
6. 按 Enter 鍵或按一下 **[Browse]** 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 185 頁的 「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 185 頁的 「簽署核准的用戶端配置」程序中步驟 101 所述)。
8. 按一下 **[Sign]** 核准請求。

簽署後續核准

簽署核准之後，後續同意動作僅需輸入金鑰庫密碼並按一下 **[Sign]**。(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

使用以下資訊與程序來設定數位簽署的核准。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。

簽署核准的伺服器端配置

若要啓用伺服器端配置，請執行以下步驟：

1. 在系統配置中，設定 `security.nonrepudiation.signedApprovals=true`

2. 將您的認證機構 (CA) 的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. 請至 http://*IPAddress*/certsrv，並使用管理權限登入。

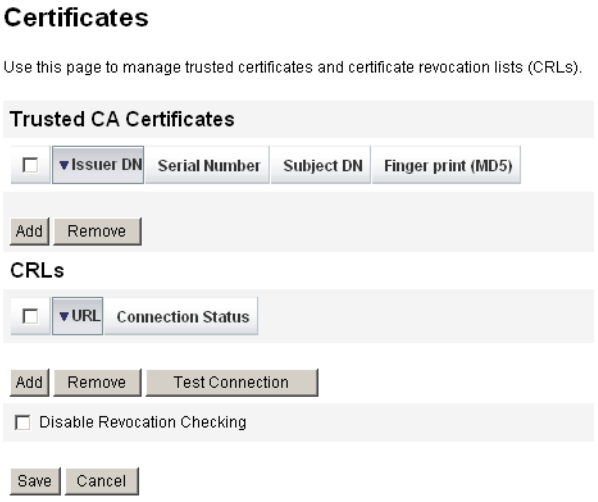
   b. 從清單中選取擷取 CA 憑證或憑證撤銷清單，然後按一下 **[Next]**。

   c. 下載並儲存 CA 憑證。

3. 將憑證增加至 Identity Manager 做爲可信任的憑證：

   a. 從管理員介面選取 **[Configure]**，然後選取 **[Certificates]**。Identity Manager 將顯示 [Certificates] 頁面。

圖 5-9 憑證



   b. 在 [Trusted CA Certificates] 區域中，按一下 **[Add]**。Identity Manager 將顯示 [Import Certificate] 頁面。

   c. 瀏覽至並選取可信任的憑證，然後按一下 **[Import]**。

      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 [Certificates] 頁面的 [CRLs] 區域中，按一下 **[Add]**。

   b. 輸入 CA 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 CRL 的 URL 可以爲 http 或 LDAP。
- 每個 CA 具有不同的 URL 來發行 CRL；您可以透過瀏覽 CA 憑證的 CRL 發佈點擴充來確定此位置。

5. 按一下 **[Test Connection]** 以驗證該 URL。
6. 按一下 **[Save]**。
7. 使用 jarsigner 簽署 applets/ts1.jar。

備註 請參閱 http://java.sun.com/j2se/1.4.2/docs/tooldocs/windows/jarsigner.html，以取得更多資訊。Identity Manager 隨附的 `ts1.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。

簽署核准的用戶端配置

若要啓用用戶端配置，請執行以下步驟：

先決條件

用戶系統必須執行 JRE 1.4 或更高版本的 Web 瀏覽器。

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，然後使用管理權限登入。
2. 選取 [Request a certificate]，然後按一下 **[Next]**。
3. 選取 [Advanced request]，然後按一下 **[Next]**。
4. 按 **[Next]**。
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 **[Submit]**，然後按一下 **[OK]**。

8. 按一下 **[Install this certificate]**。

9. 選取 **[Run]** — **> [mmc]** 以啓動 mmc。

10. 加入憑證快照：

    a. 選取 [Console] — >[Add/Remove Snap-in]。

    b. 按一下 **[Add...]**。

    c. 選取電腦帳號。

    d. 按 **[Next]**，然後按一下 **[Finish]**。

    e. 按一下 **[Close]**。

    f. 按一下 **[OK]**。

    g. 移至 **[Certificates]** — **> [Personal]** — **> [Certificates]**。

    h. 在 **[Administrator All Tasks]** — **> [Export]** 上按一下滑鼠右鍵。

    i. 按 **[Next]**。

    j. 按 **[Next]** 來確認匯出私密金鑰。

    k. 按 **[Next]**。

    l. 提供密碼，然後按 **[Next]**。

    m. 將 *CertificateLocation* 歸檔。

    n. 按 **[Next]**，然後按一下 **[Finish]**。按一下 **[OK]** 來確認。

備註 請記下您在用戶端配置的步驟 101 (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。

檢視作業事件簽名

遵循下列步驟來檢視 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 **[Reports]**。
2. 在 [Run Reports] 頁面上，從 [New...] 選項清單中選取 [AuditLog Report]。
3. 在 [Report Title] 欄位中，輸入標題 (例如「Approvals」)。
4. 在 [Organizations selection] 區域中，選取所有組織。
5. 選取 [Actions] 選項，然後選取 [Approve]。
6. 按一下 **[Save]** 儲存報告，並返回至 [Run Reports] 頁面。
7. 按一下 **[Run]** 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名資訊，其中包括：
    - 核發者
    - 主旨
    - 憑證序列號
    - 簽署的訊息
    - 簽名
    - 簽名演算法

委託核准

如果您具有核准人權能，則可以將未來的核准請求委託給一個或多個使用者 (受委託人) 達指定的時間長度。使用者無需核准人權能即可受委託。

委託功能僅適用於未來的核准請求。現有請求 ([Awaiting Approval] 標籤下列出的請求) 透過轉寄功能進行轉寄。

若要設定委託，請在 **[Approvals]** 區域中選取 **[Delegate My Approvals]** 標籤。

如果您具有任何指定的權能，其授予您對工作項目或工作項目的任何 authType 延伸 (包括 Approval、OrganizationApproval、ResourceApproval 以及 RoleApproval)，或者延伸工作項目或其 authType 之一的任何自訂子類型的委託權限，則您可以存取委託功能。

您也可以從 [Create User]/[Edit User]/[View User] 頁面的 [Security] 表單標籤，以及使用者介面主功能表委託核准。

受委託人可以在有效的委託期間代表您核准任何請求。委託的核准請求會包含受委託人的名稱。

請求的稽核記錄項目

如果已委託請求，則已核准和已拒絕之核准請求的稽核記錄項目會包含您 (委託人) 的名稱。當建立或修改使用者時，對使用者委託核准人資訊的變更將記錄在稽核記錄項目的詳細變更區段中。

資料同步化與載入

本章提供使用 Identity Manager 資料同步化與載入功能的資訊與程序。您將瞭解有關資料同步化工具 (探索、調解和同步化) 以及如何使用這些工具保持資料最新的資訊。

資料同步化工具：選哪一個好？

在選取適合執行作業的 Identity Manager 資料同步化工具時，請遵循以下指導原則。

表 6-1 要使用資料同步化工具的作業

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 配接卡 (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：

- **[Extract to File]** — 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。
- **[Load from File]** — 讀取檔案 (CSV 或 XML 格式) 中的帳號並將其載入 Identity Manager。
- **[Load from Resource]** — 合併其他兩個探索功能，擷取資源的帳號，然後將其直接載入 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。

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：

1. 從功能表列中，選取 **[Accounts]**，然後選取 **[Extract to File]**。
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 **[Download]**。Identity Manager 將顯示 [File Download] 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 (透過 Identity Manager 從資源擷取的帳號，或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

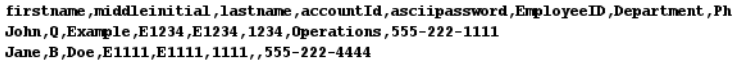
待載入的帳號通常在試算表中列出，並儲存爲逗號分隔值 (CSV) 格式，以便載入 Identity Manager 中。CSV 檔案內容必須遵循以下格式指導原則：

- **[Line 1]** — 列出每個欄位的欄標題或模式屬性 (以逗號分隔)。
- **[Lines 2 to end]** — 列出行 1 所定義的每個屬性的值 (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,Depart
ment,Phone
John,Q,Example,E1234,E1234,1234,Operations,555-222-1111
Jane,B,Doe,E1111,E1111,1111,,555-222-4444
```

圖 6-1 用於載入資料之正確格式化的 CSV 檔案範例



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：

1. 從功能表列中，選取 **[Accounts]**，然後選取 **[Load from File]**。

   Identity Manager 顯示 [Load from File] 頁面，讓您可以先指定載入選項後再繼續：

   - **[User Form]** — 當負載建立 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。
   - **[Account Correlation Rule]** — 帳號相互關聯規則會選取 Identity Manager 使用者，這些使用者可能是各個無主資源帳號的所有者。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。

- **[Account Confirmation Rule]** — 帳號確認規則會從相互關聯規則選取之可能所有者清單中排除任何非所有者。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 **[No Confirmation Rule]**，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。

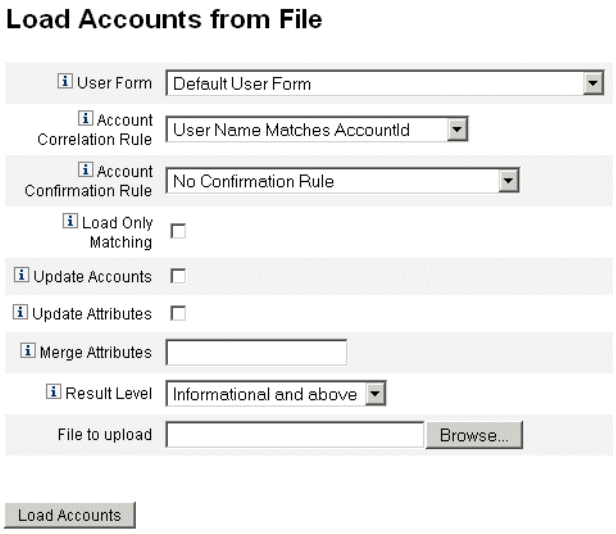
- **[Load Only Matching]** — 選取此選項可僅將符合現有 Identity Manager 使用者的帳號載入 Identity Manager 中。如果您選取此選項，載入時會捨棄所有不相符的資源帳號。
- **[Update Attributes]** — 選取此選項會將目前 Identity Manager 使用者屬性值替代爲載入帳號的屬性值。
- **[Merge Attributes]** — 輸入一或多個屬性名稱 (以逗號分隔),其值應進行合併 (排除重複項目) 而非覆寫。此選項僅能用於清單類型的屬性，如群組和郵件收件人清單。您還必須選取 [Update Attributes] 選項。
- **[Result Level]** — 選取一個臨界值，達到該臨界值時，載入程序便會記錄帳號的個別結果：
  - **[Errors only]** — 僅當載入帳號發生錯誤訊息時才記錄個別結果。
  - **[Warnings and errors]** — 載入帳號發生警告或錯誤訊息時記錄個別結果。
  - **[Informational and above]** — 記錄每個帳號的個別結果。這樣會導致載入過程執行得更慢。

2. 在 [File to Upload] 欄位中，指定要載入的檔案，然後按一下 **[Load Accounts]**。

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 6-2 說明了 [Load from File] 螢幕中的欄位和選項。

圖 6-2 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，請從功能表列中選取 **[Accounts]**，然後選取 **[Load from Resource]**。

Identity Manager 可讓您在繼續執行作業前先指定載入選項。[Load from Resource] 頁面中的載入選項及產生的動作與 [Load from File] 頁面的相同。

協調

使用調解功能可突顯 Identity Manager 中的資源帳號與資源中實際存在的帳號間的不一致狀況，並可定期進行帳號資料的關聯。

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 [Resources] 區域存取 Identity Manager 調解功能。[Resources] 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。

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：

1. 從功能表列中，選取 **[Resources]**。
2. 在 [Resources] 清單階層中，選取資源。
3. 從 [Resource Actions] 選項清單中，選取 **[Edit Reconciliation Policy]**。

Identity Manager 顯示 [Edit Reconciliation Policy] 頁面，您可以在其中選取如下策略：

- **[Reconciliation Server]** — 在叢集環境中，每個伺服器都可以執行調解。指定哪個 Identity Manager 伺服器將會對策略中的資源執行調解。
- **[Reconciliation Modes]** — 調解可在不同模式下執行，不同的模式會針對不同的品質進行最佳化處理：
  - **[Full reconciliation]** — 針對完整性進行最佳化處理，但速度會變慢。
  - **[Incremental reconciliation]** — 針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 **[Do not reconcile]** 可停用對目標資源的調解。

- **[Full Reconciliation Schedule]** — 如果啓用了完整模式調解，它會按固定的排程自動執行。指定應對策略中的資源執行完整式調解的頻率。選取 **[Inherit]** 選項可繼承更高層級策略中的指定排程。
- **[Incremental Reconciliation Schedule]** — 如果啓用了漸進式調解，它會按固定的排程自動執行。在策略中指定對資源執行增量調解的頻率。選取 **[Inherit]** 選項可繼承更高層級策略中的指定排程。

備註 並非所有資源都支援漸進式調解。

- **[Attribute-level Reconciliation]** — 可以配置調解，使其偵測出對帳號屬性進行的本機變更 (亦即，不是透過 Identity Manager 進行的變更)。指定調解時是否要偵測對 **[Reconciled Account Attributes]** 內所指定的屬性所做的原生變更。
- **[Account Correlation Rule]** — 帳號相互關聯規則會選取 Identity Manager 使用者，這些使用者可能是各個無主資源帳號的所有者。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。
- **[Account Confirmation Rule]** — 帳號確認規則會從相互關聯規則選取之可能所有者清單中排除任何非所有者。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 **[No Confirmation Rule]**，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。

- **[Proxy Administrator]** — 指定執行調解回應時所要使用的管理員。調解只能執行指定代理管理員允許執行的那些動作。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 [No Proxy Administrator] 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。

- **[Situation Options]** (與 [Response]) — 調解可識別幾種狀況類型。在 [Response] 欄中指定調解應採取的任何動作：

  - **[CONFIRMED]** — 預期的帳號已存在。
  - **[DELETED]** — 預期的帳號不存在。
  - **[FOUND]** — 調解程序在指定資源中找到了相符帳號。
  - **[MISSING]** — 在指定給使用者的資源上找不到相符帳號。
  - **[COLLISION]** — 將資源中的同一帳號指定給了兩個或兩個以上 Identity Manager 使用者。
  - **[UNASSIGNED]** — 調解程序在未指定給使用者的資源中找到了相符帳號。
  - **[UNMATCHED]** — 帳號與任何使用者均不相符。
  - **[DISPUTED]** — 帳號與一位以上的使用者相符。

  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)：

  - **[Create new Identity Manager user based on resource account]** — 執行資源帳號屬性的使用者表單以建立新的使用者。資源帳號不會隨任何變更而更新。
  - **[Create resource account for Identity Manager user]** — 重建缺少的資源帳號，運用使用者表單重新產生資源帳號屬性。
  - **[Delete resource account and Disable resource account]** — 刪除/停用資源上的帳號。
  - **[Link resource account to Identity Manager user and Unlink resource account from Identity Manager user]** — 增加或移除使用者的資源帳號指定。這不會執行任何表單的處理。

- **[Pre-reconciliation Workflow]** — 可以配置調解，使其在調解資源前先執行使用者特定的工作流程。指定調解應執行的工作流程。如果不要執行任何工作流程，請選取 [Do not run workflow]。

- **[Per-account Workflow]** — 可以配置調解，使其在回應資源帳號的狀況後執行使用者特定的工作流程。指定調解應執行的工作流程。如果不要執行任何工作流程，請選取 [Do not run workflow]。

- **[Post-reconciliation Workflow]** — 可以配置調解，使其在完成資源調解後執行使用者特定的工作流程。指定調解應執行的工作流程。如果不要執行任何工作流程，請選取 **[Do not run workflow]**。

按一下 **[Save]** 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：

- **[Reconciliation schedule]** — 您可在 [Edit Reconciliation Policy] 頁面上設定調解排程，該排程會按固定間隔執行調解。
- **[Immediate reconciliation]** — 立即執行調解。若要執行此動作，請在資源清單中選取資源，然後在 [Resource Actions] 清單中，選取以下選項之一：
  - 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，請選取資源，然後從 [Resource Actions] 清單中選取 **[Cancel Reconciliation]**。

檢視調解狀態

[Resources] 清單中的 [Status] 欄會呈報好幾種調解狀態情況。這些情況說明如下：

- **[unknown]** — 狀態不明。最近一次調解作業的結果無法使用。
- **[disabled]** — 調解已停用。
- **[failed]** — 最近一次的調解作業無法完成。
- **[success]** — 最近一次的調解順利完成。
- **[completed with errors]** — 最近一次的調解已完成，但完成時有錯誤發生。

備註 您必須更新此頁才能檢視狀態的變更 (資訊不會自動更新)。

可檢視每個資源帳號的詳細狀態資訊。在清單中選取資源，然後從 [Resource Actions] 清單中選取 **[View Reconciliation Status]**。

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

若要搜尋帳號索引，請從 [Resource Actions] 清單中選取 **[Search Account Index]**。

選取搜尋類型，然後輸入或選取搜尋屬性。按一下 **[Search]** 尋找符合所有搜尋條件的帳號。

- **[Resource account name]** — 選取此選項，選取一個修飾鍵 (開頭爲、包含或是)，然後輸入部分或完整的帳號名稱。
- **[Resource is one of]** — 選取此選項，然後從清單中選取一個或多個資源，以便尋找位於指定資源上的已調解帳號。
- **[Owner]** — 選取這個選項，選取一個修飾鍵 (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。
- **[Situation is one of]** — 選取此選項，然後從清單中選取一個或多個狀況，以便在指定狀況中尋找已調解的帳號。

按一下 **[Search]** 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 **[Limit results to]** 欄位中指定數目。預設限制爲前 1000 個找到的帳號。

按一下 **[Reset Query]** 以清除頁面重新進行選擇。

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。若要執行此動作，請選取 **[Resources]**，然後選取 **[Examine Account Index]**。

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 [Change index view] 清單中選擇一個檢視。

使用帳號

若要使用資源中的帳號，請選取 **[Group by resource]** 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。按一下資源旁邊的 + 號或 - 號，以顯示 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。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 **[Group by user]** 索引檢視。在此檢視中，Identity Manager 使用者和組織會以與 [Accounts List] 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。使用者帳號及 Identity Manager 已知的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。

Active Sync 配接卡

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。

您可以透過使用 [Meta View]，或透過在資源同步化策略中指定 [Input Form] (適用於適當目標物件類型)，來配置將資源屬性變更匯入 Identity Manager 的方式。

使用 [Meta View] 可指定資料更新的方式，以及指定要爲 Active Sync 應用程式啓用的身份識別屬性。如需有關配置身份識別屬性的更多資訊，請參閱第 120 頁的「配置身份識別屬性和事件」。

繼續下一小節以配置同步化。

配置同步化

Identity Manager 使用同步化策略來啓用資源的同步化。若要配置同步化，請在 [Resources] 標籤上選取您想要配置同步化的資源，然後從 [Resource Actions] 清單中選取 **[Edit Synchronization Policy]**。

編輯同步化策略

在 [Edit Synchronization Policy] 頁面中指定以下選項，以配置同步化：

- **[Target Object Type]** — 選取要套用策略的使用者類型，[Identity Manager Users] 或 [Service Provider Edition Users]。

備註	在服務提供者實作中，您必須將同步化策略 (將 [Service Provider Edition Users] 指定爲物件類型) 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 13 章 「服務提供者管理」

- **[Scheduling Settings]** — 使用此區段可指定啓動方法和輪詢排程。

  [Startup Type] 可以爲 [Manual]、[Automatic]、[Automatic with Failover] 或 [Disabled]：

  - **[Automatic] 或 [Automatic with failover]** — 當 Identity 系統啓動時，啓動授權來源。
  - **[Manual]** — 需要管理員啓動授權來源。
  - **[Disabled]** — 停用資源。

  使用 **[Start Date]** 和 **[Start Time]** 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：

  - 在 2005 年 7 月 18 日 (週二) 配置資源的 「使用中的同步化」
  - 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 日開始輪詢 (下個週一)。

如果未指定開始日期或時間，則資源會立即輪詢。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。

- **[Resource Specific Settings]** — 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。
- **[Common Settings]** — 爲以下資料同步化活動指定一般設定：
  - **[Proxy Administrator]** — 選取負責處理更新的管理員。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。
  - **[Input Form]** — 選取要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。
  - **[Rules]** — 您可以指定資料同步化程序期間要使用的規則：
    - **[Process Rule]** — 選取此規則可指定要針對每個內送帳號執行的處理規則。此選擇將置換所有其他選項。如果您指定一個處理規則，則不論資源上的其他設定爲何，皆會針對每一列執行此處理程序。可以是程序名稱，也可以是評估程序名稱的規則。
    - **[Correlation Rule]** — 選取相互關聯規則，以置換資源調解策略中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。
    - **[Confirmation Rule]** — 選取確認規則，以置換資源調解策略中指定的確認規則。
    - **[Resolve Process Rule]** — 選取此規則可指定當資料輸入之記錄有多個相符項目時，所要執行的作業定義名稱。此處理過程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。
    - **[Delete Rule]** — 選取將針對每個內送使用者更新進行評估的規則 (傳回 true 或 false)，以確定是否要執行刪除作業。
- **[Create Unmatched Accounts]** — 啓用此選項 (true) 後，配接卡將嘗試建立在 Identity Manager 系統中找不到的帳號。如果未啓用，配接卡將透過 [Resolve Process Rule] 傳回的程序來執行帳號。
- **[Logging Settings]** — 指定以下記錄選項的值：
  - **[Maximum Log Archives]** — 如果此值大於零，將會保留最近的 N 個記錄檔。如果此值爲零，將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。

- **[Maximum Active Log Age]** — 超過此段期間之後，將歸檔現用的記錄。如果時間爲零，則不會執行定期封存。如果 [Maximum Log Archives] 爲零，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。此有效期間標準的評估與 [Maximum Log File Size] 中所指定的標準無關。

  輸入數字，然後選取時間單位 (日、小時、分鐘、月、秒或週)。預設單位是日。

- **[Log File Path]** — 輸入要在其中建立現用與封存記錄檔案的目錄路徑。記錄檔案名稱的開頭將會是資源名稱。

- **[Maximum Log file Size]** — 以位元組爲單位輸入現用記錄檔案的最大值。當現用記錄檔案達到最大限制時，就會被封存起來。如果 [Maximum Log Archives] 爲零，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。此大小標準的評估與 [Maximum Active Log Age] 中所指定的有效期間標準無關。

- **[Log Level]** — 輸入記錄的層級：

  - 0 — 不記錄
  - 1 — 錯誤
  - 2 — 資訊
  - 3 — 詳細的
  - 4 — 除錯

按一下 **[Save]** 儲存資源的策略設定。

編輯 Active Sync 配接卡

編輯 Active Sync 配接卡之前，請停止同步化。從 [Edit Synchronization Policy] 頁面，選取 **[Disabled]** 做爲 Identity Manager 使用者的 **[Startup Type]**，對於服務提供者使用者，請取消選取 **[Enable Synchronization]** 選項。將出現一則警告訊息，指出已停用使用中的同步化。

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 配接卡效能

由於同步化是背景作業，所以 ActiveSync 配接卡配置會影響伺服器效能。調校 ActiveSync 配接卡效能要進行下列作業：

- 變更輪詢間隔
- 指定將執行配接卡的主機
- 啓動與停止
- 配接卡記錄

透過資源清單管理 Active Sync 配接卡。選取 Active Sync 配接卡，然後從 [Resource Actions] 清單的 *[Synchronization]* 區段中存取啓動、停止與狀態更新控制動作。

變更輪詢間隔

輪詢間隔決定 Active Sync 配接卡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，如果配接器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。有些配接卡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。

指定將執行配接卡的主機

若要指定將執行配接卡的主機，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 配接卡之機器的主機名稱。配接卡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 [Configure] 標籤檢視伺服器清單。

  或者

- 設定 `sources.hosts=localhost`。透過此設定，配接卡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 配接卡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 配接卡。若要啓動或停止 Active Sync 配接卡，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 152 頁的「權能類別」。

如果將配接卡設定爲自動，當應用程式伺服器重新啓動時，配接卡也會重新啓動。當您啓動配接器時，它會立刻執行並在指定的輪詢間隔來臨時執行。如果您停止配接器，下次配接器在檢查到停止旗標時便會停止。

配接卡記錄

配接卡記錄擷取有關配接卡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。配接器記錄在除錯問題與監視配接器程序進度時非常有用。

每個配接器各有其記錄檔案、路徑和記錄層級。您可以在 [Synchronization Policy] 的 [Logging] 區段爲適當的使用者類型 (Identity Manager 或服務提供者) 指定這些值。

刪除配接器記錄

僅當停止配接卡後，才能刪除配接卡記錄。多數情況下，請在刪除記錄前製作記錄副本做爲歸檔之用。

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：

- **[Reports]** — 使用此區域定義、執行、刪除和下載報告。您也可以管理排程的報告。
- **[Tasks]** — 定義報告後，您就可以移至 [Tasks] 區域以排定和處理報告作業。

報告

大多數與報告相關的作業都是在 [Run Reports] 頁面中執行的，在該頁面中您可以完成以下報告作業：

- 建立、修改和刪除報告
- 執行報告
- 下載報告資訊以便在其他應用程式 (如 StarOffice) 中使用。

若要檢視此頁面，請從功能表列中選取 **[Reports]**。螢幕將顯示 **[Run Reports]** 頁面，其中顯示了可用報告的清單。

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

圖 7-1 爲 [Run Reports] 頁面的範例。

圖 7-1 [Run Reports] 選取

使用下列方法之一開始定義報告：

- 建立報告。
- 選取要修改的報告，然後以新名稱儲存 (也稱爲報告複製)。

建立報告

若要建立報告，請使用以下步驟：

1. 從功能表列中，選取 **[Reports]**。
2. 選取報告種類：**[Identity Manager Reports]** 或 **[Auditor Reports]**，然後從 **[New]** 選項清單中選取報告類型。

Identity Manager 會顯示 [Define a Report] 頁面，您可在其中選取並儲存建立報告時要用的選項。

複製報告

若要複製報告，請從清單中選取一個報告。輸入新報告名稱並選擇性地調整報告參數，然後按一下 **[Save]** 將報告以新名稱儲存。

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信人。當您選取此選項時，頁面會更新並提示您輸入電子郵件收件者。輸入一或多位收信人，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：

- **[Attach CSV Format]** — 以逗號分隔值 (CVS) 格式附加報告結果。
- **[Attach PDF Format]** — 以可移植文件格式 (PDF) 附加報告結果。

執行報告

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 **[Run]** 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 **[Save]** 以儲存報告。一旦儲存後，您就可以從 [Run Reports] 頁面 (報告清單) 來執行此報告

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：

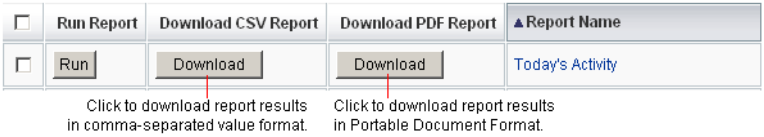
- **[Reports] > [Run Reports]** — 可讓您立即執行儲存的報告。在報告清單中，按一下 **[Run]**。Identity Manager 會執行報告，然後以摘要和明細形式顯示結果。
- **[Tasks] > [Schedule Tasks]** — 排定要執行的報告作業。選取報告作業後，您便可設定報告頻率及選項。您還可以調整特定的報告詳細資訊 (像在 [Define a Report] 頁面的 [Reports] 區域中那樣)。

下載報告資料

從 [Run Reports] 頁面的以下其中一欄中，按一下 **[Download]**：

- **[Download CSV Report]** — 以 CSV 格式下載報告輸出。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。
- **[Download PDF Report]** — 以可移植文件格式下載報告輸出，這種格式可使用 Adobe Reader 檢視。

圖 7-2 下載報告



配置報告輸出的字型

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。

若要配置報告字型選項，請按一下 **[Reports]**，然後選取 **[Configure]**。可使用以下選項：

- **PDF 報告選項**
  - **[PDF Font Name]** — 選取在產生 PDF 報告時要使用的字型。依預設，僅顯示適用於所有 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。

    可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 [Embed Font in PDF Documents] 選項。
  - **[Embed Font in PDF Documents]** — 選擇此選項可在產生的 PDF 報告中內嵌字型定義。這將確定在任何 PDF 檢視器中都可以檢視報告。

備註 內嵌字型會極大地增加文件的大小。

- **[CSV Report Options]** — 選取產生報告時所要使用的字元集。

按一下 **[Save]** 可儲存報告配置選項。

報告類型

Identity Manager 提供了數種報告類型：

- Auditor
- 稽核記錄
- 即時
- 摘要
- 系統記錄檔
- 使用情況

可透過以下一種或兩種報告種類來存取這些報告：

- Identity Manager 報告
- Auditor 報告

Auditor

Auditor 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。如需有關稽核策略和 Auditor 報告的更多資訊，請參閱第 11 章「身份識別稽核」

Identity Manager 提供以下 Auditor 報告：

- 存取檢閱報告
- 稽核策略掃描
- 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
- 違規摘要報告
- 責任分離報告

若要定義 Auditor 報告，請在 [Run Reports] 頁面中選取 **[Auditor Reports]** 選項，然後從 [Auditor Reports] 清單中選取報告。如需有關 Auditor 報告的更多資訊，請參閱「使用 Auditor 報告」。

稽核記錄

稽核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 **[Configure]**，然後選取 **[Audit]**。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 134 頁的「配置稽核群組和稽核事件」。

您可以從 [Run Reports] 頁面的報告選項清單中選取 [AuditLog Report]，以執行該報告。[Identity Manager Reports] 和 [Auditor Reports] 種類均包含此報告。

您設定與儲存報告參數後，請即從 [Run Reports] 清單頁面中執行報告。按一下 **[Run]** 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。

即時

即時報告直接輪詢資源以報告即時資訊。即時報告包括：

- **[Resource Group]** — 概述群組屬性，包括使用者的成員身份。
- **[Resource Status]** — 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。
- **[Resource User]** — 列示使用者資源帳號和帳號屬性。

若要定義即時報告，請從 [Run Reports] 頁面的 **[Identity Manager Reports]** 清單中選取一個報告選項。

您設定與儲存報告參數後，請即從 [Run Reports] 清單頁面中執行報告。按一下 **[Run]** 可產生一個包含與已儲存條件相符之所有結果的報告。

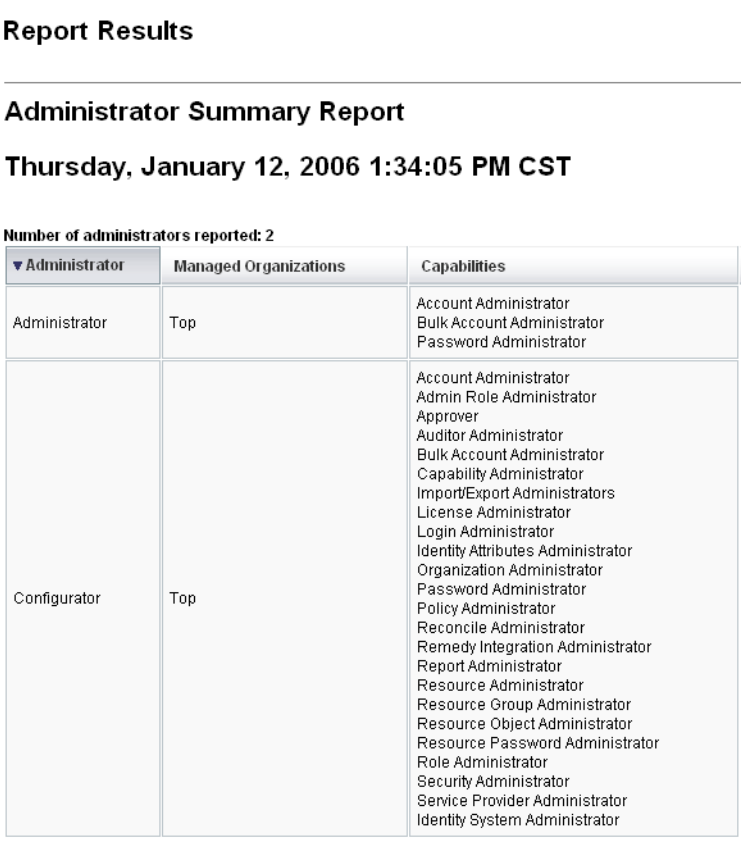
摘要報告

摘要報告類型包括 **[Identity Manager Reports]** 清單中的以下報告：

- **[Account Index]** — 根據調解狀況報告選取的資源帳號。
- **[Administrator]** — 檢視 Identity Manager 管理員、管理員管理的組織以及指定的權能。定義管理員報告時，您可以依組織選取要包括的管理員。
- **[Admin Role]** — 列示指定給管理員角色的使用者。
- **[Role]** — 概述 Identity Manager 角色以及關聯資源。定義角色報告時，您可以依相關組織選取要包括的角色。
- **[Task]** — 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。
- **[User]** — 檢視使用者、爲其指定的角色及其可以存取的資源。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。
- **[User Question]** — 允許管理員尋找沒有回答最低數目的認證問題的使用者，此數目按其帳號策略需求指定。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。

如下圖所示，管理員報告列示了 Identity Manager 管理員、管理員管理的組織及其指定的權能和管理員角色。

圖 7-3 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

系統記錄檔

系統記錄檔報告顯示儲存庫中記錄的系統訊息和錯誤。設定此報告時，可以指定包含或排除：

- 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 Report] 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 [Recent Systems Messages] 報告中的特定項目，請編輯該報告並選取 **[Event]** 欄位，然後輸入請求的 Syslog ID 並按一下 **[Run]**。

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，請從 [Run Reports] 頁面的報告選項清單中選取 **[SystemLog Report]**。

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或表格摘要。您可以透過圓餅圖、長條圖或表格形式顯示輸出。

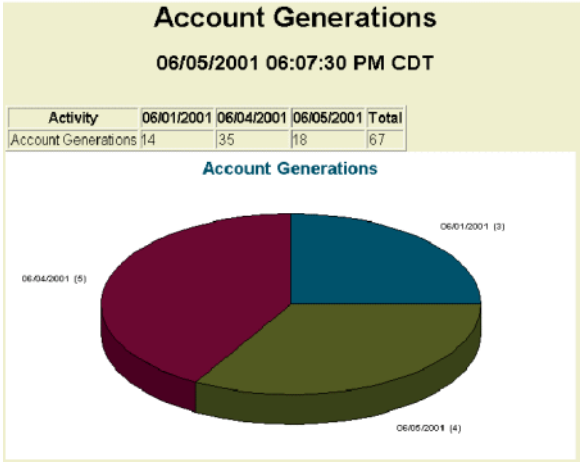
若要定義使用情況報告，請從 [Run Reports] 清單頁面的報告選項清單中選取 **[Usage Report]**。

您設定與儲存報告參數後，請即從 [Run Reports] 清單頁面中執行報告。

使用情況報告圖表

在下圖中，上方的表格顯示報告包含的事件。下方的圖表以圖形化格式來顯示同樣的資訊。當您將滑鼠指標移至圖表上的各個部分時，便會出現該部分所代表的值。

圖 7-4 使用情況報告 (產生的使用者帳號)



您可以處理圓餅圖的部份以反白顯示它們。按一下滑鼠右鍵並按住某個資料片，然後將它拖離中心，使它看起來與其他資料片分開。可以對圖表的一或多個部份執行同樣的動作。爲了獲得最佳的控制，請在中心附近按一下該資料片；如此可讓您將它拖曳到距離其他資料片更遠的位置。

也可以將圓餅圖旋轉到想要的檢視畫面。按一下並按住接近圖表邊緣之處，然後將滑鼠向左右移動即可旋轉檢視畫面。

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、Windows NT 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，並可使用 [Business Process Editor] 對其進行修改。如需有關配置 Identity Manager 表單的更多資訊，請參閱「Identity Manager Workflows, Forms, and Views」。

若要建立風險分析報告，請按一下功能表列中的 **[Risk Analysis]**，然後從 [New] 選項清單中選取一個報告。

您可以將報告限制爲只掃描選取的資源；視資源類型，可以掃描下列類型的帳號：

- 已停用、到期、非作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

定義後，您就可以將風險分析報告排程爲以指定間隔執行。

1. 按一下 **[Schedule Tasks]**，然後選取要執行的報告。
2. 在 [Create Task Schedule] 頁面中，輸入名稱與排程資訊，然後選擇性調整其他風險分析選擇。
3. 按一下 **[Save]** 以儲存排程。

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。面板可讓您快速存取系統資源和場所異常，以瞭解歷史效能趨勢 (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隔離問題。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活動和手動活動。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 222 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 [Configure Reports] 頁面的 [Tracked Event Configuration] 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 **[Enable event collection]** 可以啓用追蹤事件配置。

可爲事件集合指定以下選項：

- **[Time Zone]** — 此選項設定記錄追蹤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。

- **[Time Scales to collect]** — 此選項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。

系統會將追蹤事件資料儲存相當長的一段時間，以便詳細檢視系統的目前狀況並瞭解長期趨勢。

以下時間範圍可以使用。依預設全部選取。請取消選取不需要的收集間隔。

- 10 鏃間隔
- 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。

使用圖形

您可以執行以下與圖形相關的活動：

- 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。如果未收集適當的資料，則某些不使用範例資料的範例圖形可能顯示爲空白。

1. 按一下功能表列中的 **[Reports]**。
2. 按一下 **[Dashboard Graphs]**。

   所有已定義的圖形均會列出。
3. 按一下所需圖形名稱。
4. 如果需要，按一下 **[Pause refresh]** 以暫停面板更新。按一下 **[Resume]** 以更新檢視。

備註 對於包含許多圖形的面板，有時暫停更新直到初始載入所有圖形是很有幫助的。

5. 如有需要，請按一下 **[Refresh now]** 以強制執行立即更新。
6. 按一下 **[Done]** 以返回 [Dashboard Graphs] 清單頁面。

備註 如果有任何圖形顯示錯誤訊息，請使用除錯頁面在系統配置物件中設定 `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 **[Please include this text script if reporting a problem]** 連結擷取圖形程序檔。報告問題時應包含此圖形程序檔。

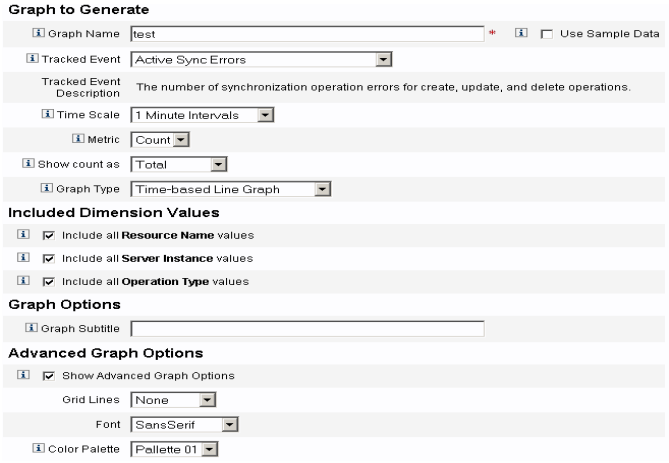
建立圖形

使用以下程序可建立新的面板圖形：

1. 按一下功能表列中的 **[Reports]**。
2. 按一下 **[Dashboard Graphs]**。

   所有已定義的圖形均會列出。
3. 按一下 **[New]**。圖 7-5 說明了 [Edit Graph] 頁面。

圖 7-5 編輯圖形



要產生的圖形

4. 輸入 **[Graph Name]**。因爲會依名稱將圖形增加至面板，所以請選擇唯一的、有意義的名稱。

5. 如有需要，請選取 **[Use Sample Data]**。

   啓用此選項可以預覽具有範例資料的圖形。範例資料選項僅供您熟悉系統之用。由於並非所有追蹤的事件均具有範例資料，所以此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。

6. 從清單中選取所需類型的 **[Tracked Event]**。

   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。

7. 從清單中選取 **[Time Scale]**。

   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。

8. 從清單中選取 **[Metric]**。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：

   - [Count] — 在該時間間隔內事件發生的總次數
   - [Average] — 在該時間間隔內事件值的算術平均值
   - [Maximum] — 在該時間間隔內的最大事件值
   - [Minimum] — 在該時間間隔內的最小事件值
   - [Histogram] — 在該時間間隔內各個事件值範圍的獨立計數

9. 從清單中選取 **[Show count as]**。

   圖形計數顯示爲原始總數或按不同時間比例進行劃分。

10. 從清單中選取 **[Graph Type]**。

    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。

基本尺寸

11. 如果需要，請從清單中選取以下選項：

    - **[Resource Name]**。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。
    - **[Server Instance]**。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。
    - **[Operation Type]**。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。

圖形選項

12. 如果需要，請爲 **[Graph Subtitle]** 輸入內容

    這會在圖形的主標題下產生一個子標題。

進階圖形選項

13. 如有需要，選取 **[Advanced Graph Options]**。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

14. 按一下 **[Save]** 以建立圖形。

編輯圖形

可透過選取 [Reports] 標籤，然後從 **[Dashboard Graphs]** 清單中選取圖形名稱來編輯圖形。

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徵進行編輯：

- **[Graph Name]** — 圖形將依名稱增加至面板。
- **[Registry]** — 指定登錄中定義的**追蹤事件說明**。目前選項包括：SAMPLE、SPE (服務提供者) 和 IDM。
- **[Tracked Event]** — 系統特徵 (如記憶體使用率) 或事件彙集 (如資源作業)，其之前的值會以可視圖形或圖表追蹤和顯示。
- **[Time Scale]** — 控制彙集資料的頻率以及保留資料的頻率。
- **[Metric]** — 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。
- **[Graph type]** — 控制追蹤事件資料的顯示方式 (例如，線形圖或長條圖)。
- **[Included Dimension Values]** — 如果選取此選項，則所有尺寸值都會包含在圖形中。
- **[Graph Subtitle]** — 如果需要，在圖形的主標題下輸入子標題。
- **[Advanced Graph Options]** — 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 **[Save]**。

刪除圖形

透過從 **[Dashboard Graphs]** 清單中選取圖形，然後按一下 **[Delete]** 可刪除圖形。

備註 刪除圖形會從包含該圖形的所有面板中自動將其移除，而不會發出警告。

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 222 頁的「建立面板」，以取得說明。

您可在 [Reports] 功能表中的以下區域使用面板。

您可以從 Identity Manager 介面的 **[Reports]** 區域檢視現有面板。按一下 [View Dashboards]，**[Dashboard Graphs]** 以列出目前定義的面板，然後按一下您要檢視的面板旁邊的 **[Display]**。

備註 對於包含許多圖形的面板，有時暫停更新直到初始載入所有圖形是很有幫助的。

按一下 **[Pause]** 可暫停面板更新，而按一下 **[Refresh]** 可更新檢視。

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，請執行以下程序：

1. 按一下功能表列中的 **[Reports]**。
2. 按一下 **[View Dashboards]**。

3. 按一下 **[New]**。
4. 輸入新面板的名稱。
5. 輸入新面板摘要。
6. 從清單中選取更新率，以秒、分鐘或小時爲單位。

備註 將更新率設定爲少於 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 **[Remove Graph(s)]**。
9. 按一下 **[Save]**。

編輯面板

使用建立面板中說明的程序來編輯面板 (選取 [New] 除外)，選取要修改的面板並編輯以下屬性：

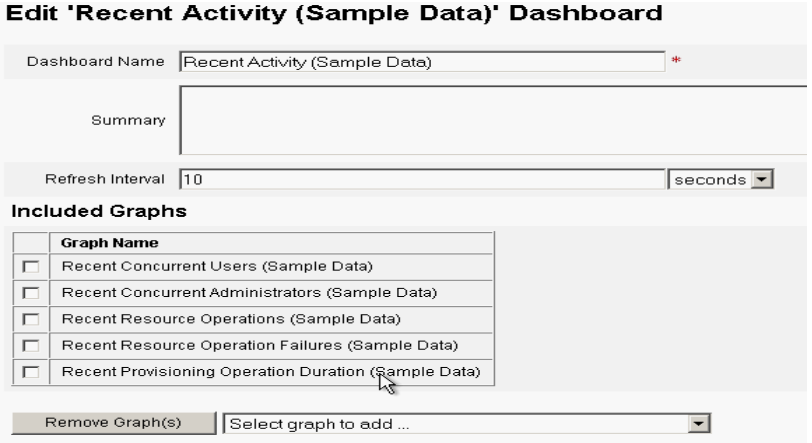
- 面板的名稱。
- 新面板摘要。
- 清單中的更新率，以秒、分鐘或小時爲單位。
- 增加或移除與面板關聯的圖形。

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 7-6 說明了範例面板編輯頁面。

圖 7-6 編輯面板



刪除面板

若要刪除 [Service Provider] 面板，請從 [Service Provider] 區域按一下 **[Manage Dashboards]**，然後選取需要的面板並按一下 **[Delete]**。

備註 使用此程序並不會移除面板中包含的圖形。請使用 [Manage Dashboard Graphs] 頁面刪除圖形 (請參閱 「刪除圖形」)。

搜尋作業事件

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，需要將其寫入作業事件永久性存放區。

備註 使用 [Edit Transaction Configuration] 頁面 (請參閱 「作業事件管理」)，管理員可以控制保存作業事件的時間。例如，即使在第一次嘗作業事件之前，也可以立即保留它們。

[Search Transactions] 頁面可讓您搜尋作業事件永久性存放區中的作業事件。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，以防止進一步的嘗試。

若要搜尋作業事件，請：

1. 登入至 Identity Manager。
2. 按一下功能表列中的 **[Service Provider]**。
3. 按一下 **[Search Transations]**。

   螢幕將顯示 **[Search Conditions]** 頁面。

備註 搜尋僅傳回符合在其下方所選**所有**條件的作業事件。這與 Identity Manager 中的 **[Accounts] -> [Find Users]** 頁面類似。

4. 如有需要，選取 **[User Name]**。

   此選項可讓您搜尋僅適用於具有您輸入的**帳號 ID** 之使用者的作業事件。

備註 如果您已在 Service Provider Edition [Transaction Configuration] 頁面配置了任何自訂的可查詢使用者屬性，則這些屬性將顯示在這裡。例如，您可以選擇根據 [Last Name] 或 [Full Name] (如果這些屬性已配置爲自訂的可查詢使用者屬性)。

5. 如有需要，選取按 **[Type]** 搜尋。

   此選項可讓您搜尋所選類型的作業事件。
6. 如有需要，選取按 **[State]** 搜尋。

   此選項可讓您搜尋處於以下所選狀態的作業事件：

   - **[Unattempted]**，作業事件尚未嘗試。
   - **[Pending retry]**，作業事件已嘗試一次或多次，已發生一個或多個錯誤，以及已排定重試達到爲個別資源配置的重試限制。
   - **[Success]**，作業事件已成功完成。
   - **[Failure]**，作業事件已完成，但發生一次或多次失敗。
7. 如有需要，選取按 **[Attempts]** 搜尋。

   此選項可讓您依據作業事件被嘗試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。
8. 如有需要，選取按 **[Submitted]** 搜尋。

   此選項可讓您依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。

9. 如有需要，選取按 **[Completed]** 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。

10. 如有需要，選取按 **[Cancelled Status]** 搜尋。

    此選項可讓您依據作業事件是否已取消來搜尋作業事件。

11. 如有需要，選取按 **[Transaction ID]** 搜尋。

    此選項可讓您依據作業事件的唯一 ID 來搜尋作業事件。使用此選項可依據您輸入的 ID 值來尋找作業事件，該 ID 值顯示在所有稽核記錄中。

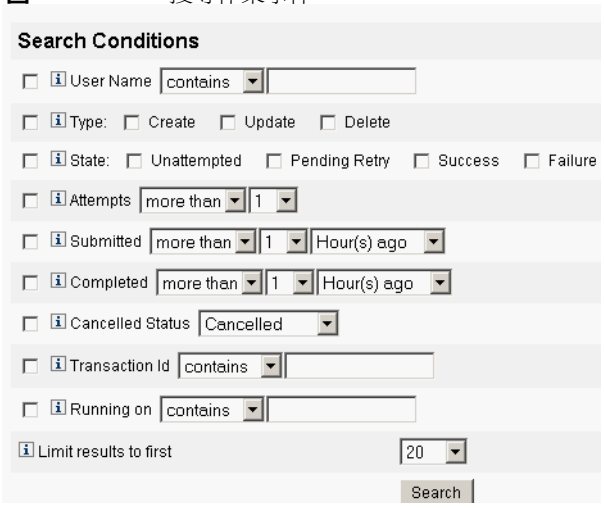
12. 如有需要，選取按 **[Running On]** (伺服器名稱) 搜尋。

    此選項可讓您依據執行作業事件的 Service Provider Edition 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。

13. 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。即使有更多的結果可用，也不會做任何指示。

圖 7-7 搜尋作業事件



14. 按一下 **[Search]**。

    螢幕上將顯示搜尋結果。

15. 如有需要，按一下結果頁面底部的 **[Download All Matched Transactions]**。這會將結果儲存爲 XML 格式的檔案。

備註 您可以取消搜尋結果中傳回的作業事件。選取結果表格中的作業事件，然後按一下 **[Cancel Selected]**。您無法取消已完成或已取消的作業事件。

作業範本

Identity Manager **作業範本**可讓您使用管理員介面來配置某些工作流程運作方式，做爲編寫自訂工作流程的替代方法。

本章中的以下主題說明了如何使您的系統可以使用作業範本，以及如何使用作業範本來配置工作流程運作方式：

啟用作業範本

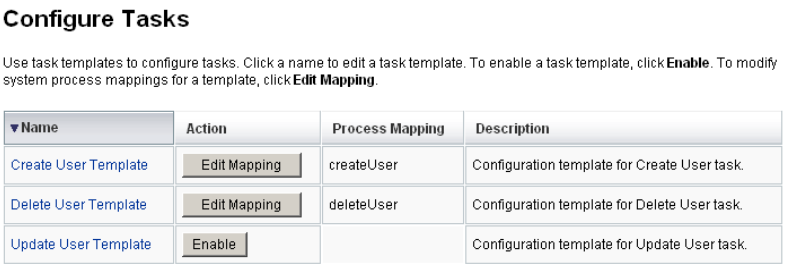
Identity Manager 提供了以下您可配置的作業範本：

- **[Create User Template]** — 配置建立使用者作業的特性。
- **[Delete User Template]** — 配置刪除使用者作業的特性。
- **[Update User Template]** — 配置更新使用者作業的特性。

在使用作業範本之前，您必須對映作業範本程序。若要對映程序類型，請使用以下程序：

1. 從 Identity Manager 管理員介面中選取 **[Tasks]**，然後選取 **[Configure Tasks]**。圖 8-1 顯示了 [Configure Tasks] 頁面。

圖 8-1 配置作業



[Configure Tasks] 頁面包含一個表格，其中具有以下欄：

- **[Name]** — 提供 [Create User Templates]、[Delete User Templates] 和 [Update User Templates] 的連結。
- **[Action]** — 包含以下按鈕之一：
  - **[Enable]** — 如果您尚未啓用範本，則顯示此按鈕。
  - **[Edit Mapping]** — 啓用範本之後會顯示此按鈕。

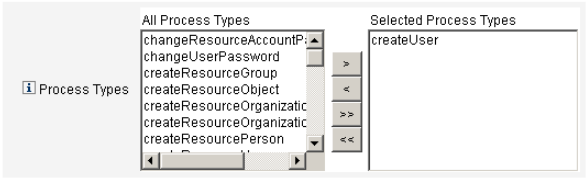
啓用和編輯程序對映的程序是一樣的。

- **[Process Mapping]** — 列出每個範本對映的程序類型。
- **[Description]** — 提供每個範本的簡短描述。

2. 按一下 **[Enable]** 以開啓範本的 [Edit Process Mappings] 頁面。

   例如，對於 [Create User Template]，會顯示以下頁面 (圖 8-2)：

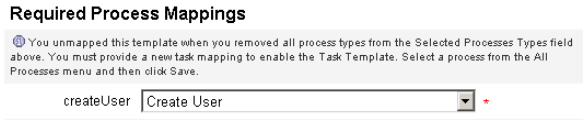
圖 8-2 [編輯程序對映] 頁面



備註 預設程序類型 (在此情況下，爲 createUser) 會自動顯示在 [Selected Process Types] 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 [Selected Process Types] 清單中移除程序類型，但未選取替代的程序類型，則將顯示 [Required Process Mappings] 區段，指示您選取一個新的作業對映。

圖 8-3 [Required Process Mappings] 區段



3. 按一下 **[Save]** 可對映選取的程序類型並返回到 [Configure Tasks] 頁面。

備註 重新顯示 [Configure Tasks] 頁面後，**[Edit Mapping]** 按鈕將替代 **[Enable]** 按鈕，而且程序名稱將列在 [Process Mapping] 欄中。

圖 8-4 更新的 [Configure Tasks] 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 **[Configure] > [Form and Process Mappings]**，以驗證對映。顯示 [Configure Form and Process Mappings] 頁面後，向下捲動到 [Process Mappings] 表，並驗證以下程序類型已對映到該表中顯示的 [Process Name Mapped To] 項目。

Process Name Mapped To	Process Type
createUser	Create User Template
deleteUser	Delete User Template
updateUser	Update User Template

  如果成功啓用範本，則 [Process Name Mapped To] 項目應該均包含文字 *Template*。

- 如果在 **[Process Name Mapped To]** 欄中鍵入**範本** (如表中所示)，則您還可以直接從 [Form and Process Mapping] 頁面對映這些程序類型。

成功對映範本程序類型後，可以配置該作業範本。

配置作業範本

若要配置不同的作業範本，請遵循以下步驟：

1. 在 [Task Template] 表中選取一個 [Name] 連結。將顯示以下頁面之一：
   - **[Edit Task Template Create User Template]** — 開啓此頁面可編輯用於建立新使用者帳號的範本。
   - **[Edit Task] Template Delete User Template** — 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。
   - **[Edit Task Template Update User Template]** — 開啓此頁面可編輯用於更新現有使用者資訊的範本。

   每個 [Edit Task Template] 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 8-1 [Task Template] 標籤

標籤名稱	用途	範本
General (**預設標籤**)	使您可以定義作業名稱在 [Home] 和 [Account] 頁面上的作業列中以及 [Tasks] 頁面的作業實例表中如何顯示。	僅 [Create User Task Template] 和 [Update User Task Template]
	讓您可以指定如何刪除 / 取消佈建使用者帳號	僅 [Delete User Template]
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
Approvals	讓您可以按類型啟用或停用核准、定義附加核准人、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。	所有範本
Provisioning	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 [Create User Task Template] 和 [Update User Task Template]
Sunrise and Sunset	讓您可以在指定日期 / 時間之前暫停建立作業 (*sunrise*) 或在指定日期 / 時間之前暫停刪除作業 (*sunset*)。	僅 [Create User Task Template]
Data Transformations	讓您可以配置在佈建期間如何變換使用者資料。	僅 [Create User Task Template] 和 [Update User Task Template]

2. 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 234 頁的「配置 [General] 標籤」
   - 第 236 頁的「配置 [Notification] 標籤」
   - 第 241 頁的「配置 [Approvals] 標籤」
   - 第 254 頁的「配置 [Audit] 標籤」
   - 第 256 頁的「配置 [Provisioning] 標籤」
   - 第 257 頁的「配置 [Sunrise and Sunset] 標籤」
   - 第 262 頁的「配置 [Data Transformations] 標籤」

3. 您配置完這些範本後，請按一下 **[Save]** 按鈕以儲存您的變更。

配置 [General] 標籤

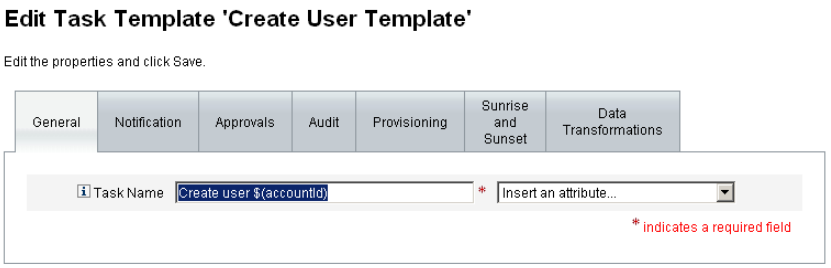
本節提供配置 [General] 標籤的說明。

備註 對於 [Create User Template] 和 [Update User Template]，[Edit Task Template] 頁面是相同的，因此在一節中說明如何配置標籤。

對於 [Create User Template] 或 [Update User Template]

依預設，開啓 [Edit Task Template Create User Template] 或 [Edit Task Template Update User Template] 後，會顯示 [General] 標籤頁面。此頁面由 [Task Name] 文字欄位和功能表組成，如下圖所示。

圖 8-5 [General] 標籤：Create User Template



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考。

若要變更預設作業名稱，請執行以下步驟：

1. 在 **[Task Name]** 欄位鍵入名稱。

   您可以編輯或完全替代預設的作業名稱。

2. **[Task Name]** 功能表會提供目前爲與此範本配置的作業相關聯的視圖而定義的屬性清單。從功能表中選取一個屬性 (**可選擇**)。

   Identity Manager 會將該屬性名稱附加到 [Task Name] 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 **[Save]** ，以儲存變更並返回到 [Configure Tasks] 頁面。

- 在 [Home] 和 [Accounts] 標籤的底部，Identity Manager 作業列中，將顯示新的作業名稱。
- 按一下 **[Cancel]**，以放棄變更並返回到 [Configure Tasks] 頁面。

對於 [Delete User Template]

開啓 [Edit Task Template Delete User Template] 後，依預設會顯示 [General] 標籤頁面。

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 **[Delete Identity Manager Account]** 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：
   - **[Never]** — 啓用此按鈕可以防止帳號被刪除。
   - **[Only if user has no linked accounts after deprovisioning]** — 啓用此按鈕，則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。
   - **[Always]** — 啓用此按鈕，可以始終允許刪除使用者帳號，即使仍然存在指定的資源帳號。
2. 使用 **[Resource Accounts Deprovisioning]** 方塊來控制**所有**資源帳號的資源帳號取消佈建作業，如下所示：
   - **[Delete All]** — 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。
   - **[Unassign All]** — 啓用此方塊可以取消指定該使用者的所有資源帳號。無法刪除資源帳號。
   - **[Unlink All]** — 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 [Individual Resource Accounts Deprovisioning] 表中的運作方式。

---

3. 使用 **[Individual Resource Accounts Deprovisioning]** 方塊，可以對使用者取消佈建進行更細致的操作 (與 [Resource Accounts Deprovisioning] 相比)，如下所述：
   - **[Delete]** — 啓用此方塊，可以刪除資源中代表該使用者的帳號。

- **[Unassign]** — 啓用此方塊，該使用者將不再直接指定到資源。無法刪除資源帳號。
- **[Unlink]** — 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 **[Individual Resource Accounts Deprovisioning]** 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。

4. 完成後，您可以
   - 選取其他標籤繼續編輯該範本。
   - 按一下 **[Save]** ，以儲存變更並返回到 [Configure Tasks] 頁面。
   - 按一下 **[Cancel]**，以放棄變更並返回到 [Configure Tasks] 頁面。

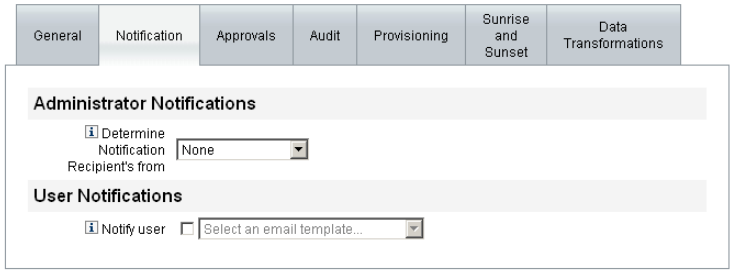
配置 [Notification] 標籤

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 [Notification] 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。

下圖顯示 [Create User Template] 的 [Notification] 頁面。

圖 8-6 [Notification] 標籤 Create User Template



若要指定 Identity Manager 如何確定通知收件者，請遵循以下程序：

1. 完成 [Administrator Notifications] 區段。
2. 完成 [User Notifications] 區段。
3. 完成後，您可以
   - 選取其他標籤繼續編輯該範本。
   - 按一下 **[Save]** ，以儲存變更並返回到 [Configure Tasks] 頁面。
   - 按一下 **[Cancel]**，以放棄變更並返回到 [Configure Tasks] 頁面。

配置管理員通知

從 **[Determine Notification Recipients from]** 功能表中選取一個選項，以確定通知管理員收件者的方法。

- **[None]** (預設) — 不通知任何管理員。
- **[Attribute]** — 選取此選項可從使用者視圖中指定的屬性中導出通知收件者的帳號 ID。繼續執行第 238 頁的「透過屬性指定收件者」。
- **[Rule]** — 選取此選項可以透過評估特定規則，來導出通知收件者的帳戶 ID。繼續執行第 238 頁的「透過規則指定收件者」。
- **[Query]** — 選取此選項可以透過查詢特定資源，來導出通知收件者的帳戶 ID。繼續執行第 239 頁的「透過查詢指定收件者」。
- **[Administrator List]** — 選取此選項可以從清單明確選擇通知收件者。繼續執行第 240 頁的「從管理員清單指定收件者」。

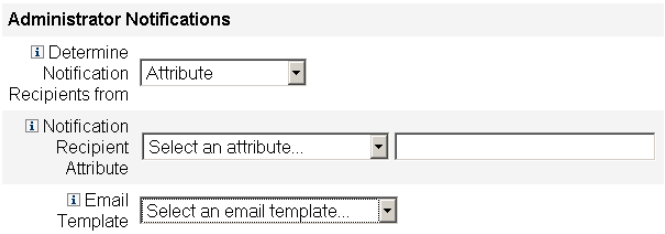
透過屬性指定收件者

若要從指定屬性導出通知收件者帳號 ID，請使用以下步驟：

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 **[Determine Notification Recipients from]** 功能表中選取 **[Attribute]**，將顯示以下新選項：

   圖 8-7 Administrator Notifications:Attribute

   - **[Notification Recipient Attribute]** — 提供用於確定收件者帳號 ID 的屬性清單 (目前爲與此範本配置的作業相關聯的視圖而定義)。
   - **[Email Template]** — 提供電子郵件範本的清單。

2. 從 **[Notification Recipient Attribute]** 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 **[Email Template]** 功能表中選取範本，以指定管理員之通知電子郵件的格式。

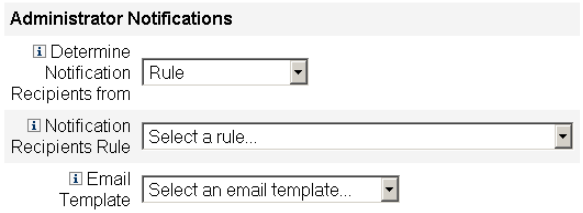
透過規則指定收件者

若要從指定規則導出通知收件者帳號 ID，請使用以下步驟：

備註	評估之後，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 **[Determine Notification Recipients from]** 功能表中選取 **[Rule]**，將會在 [Notification] 表單中顯示以下新選項：

圖 8-8 Administrator Notifications:Rule



- **[Notification Recipient Rule]** — 提供目前爲您的系統定義的規則清單，評估之後，它會傳回收件者的帳號 ID。
- **[Email Template]** — 提供電子郵件範本的清單。

2. 從 **[Notification Recipient Rule]** 功能表中選取規則。
3. 從 **[Email Template]** 功能表中選取範本，以指定管理員之通知電子郵件的格式。

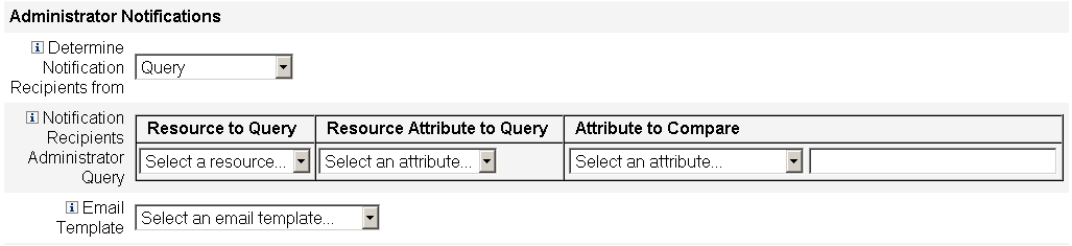
透過查詢指定收件者

備註 目前僅支援 LDAP 和 Active Directory 資源查詢。

若要透過查詢指定資源導出通知收件者帳號 ID，請使用以下步驟：

1. 從 **[Determine Notification Recipients from]** 功能表中選取 **[Query]**，將會在 [Notification] 表單中顯示以下新選項，如圖 8-9 中所示：

圖 8-9 Administrator Notifications:Query



- **[Notification Recipient Administrator Query]** — 提供包含以下功能表的表格，可用來建構查詢：

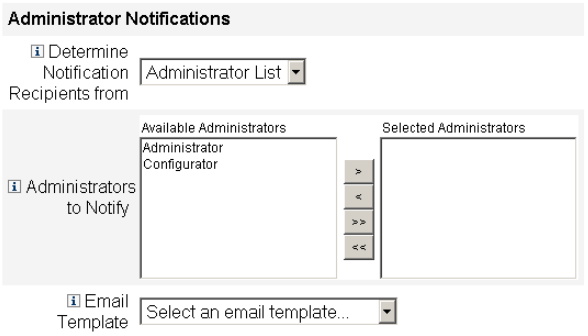
- **[Resource to Query]** — 提供目前爲系統定義的資源清單。
- **[Resource Attribute to Query]** — 提供目前爲系統定義的資源屬性清單。
- **[Attribute to Compare]** — 提供目前爲系統定義的屬性清單。
- **[Email Template]** — 提供電子郵件範本的清單。

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 **[Email Template]** 功能表中選取範本，以指定管理員之通知電子郵件的格式。

從管理員清單指定收件者

從 **[Determine Notification Recipients from]** 功能表中選取 **[Administrators List]**，將會在 [Notification] 表單中顯示以下新選項：

圖 8-10 Administrator Notifications: Administrators List



- **[Administrators to Notify]** — 提供選取工具和可用管理員的清單。
- **[Email Template]** — 提供電子郵件範本的清單。

4. 在 [Available Administrators] 清單中選取一個或多個管理員，然後使用 > 按鈕或 >> 按鈕將所選名稱移至 [Selected Administrators] 清單中。
5. 從 **[Email Template]** 功能表中選取範本，以指定管理員之通知電子郵件的格式。

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。

若要通知使用者被建立、更新或刪除，請啓用 **[Notify user]** 核取方塊 (如圖 8-11 所示)，然後從清單中選取電子郵件範本。

圖 8-11 指定電子郵件範本

配置 [Approvals] 標籤

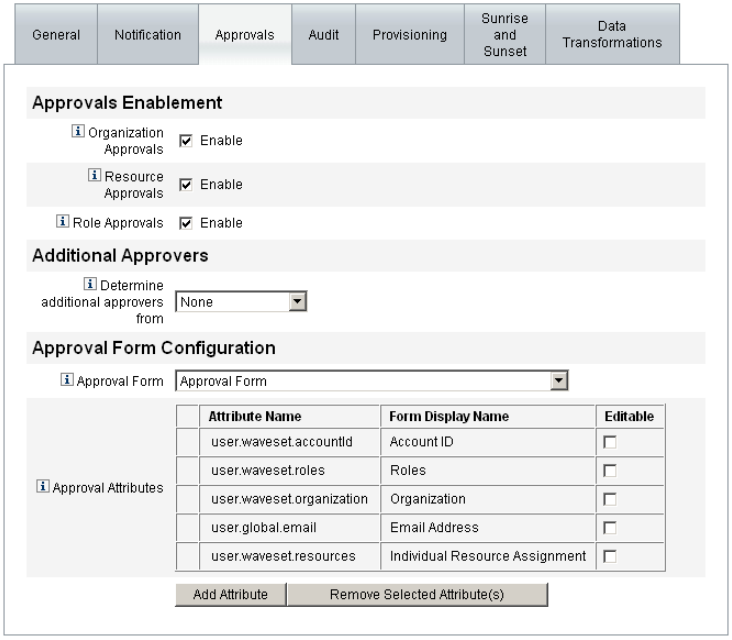
您可以使用 [Approvals] 標籤指定附加核准人，並在 Identity Manager 執行建立、刪除或更新使用者作業之前指定作業核准表單的屬性。

以前，需要與特定機構、資源或角色相關聯的管理員核准某些作業才能執行。Identity Manager 也允許您指定**附加核准人**，即需要核准該作業的附加管理員。

備註 如果您爲工作流程配置附加核准人，則需要取得原有核准人**和**範本中指定的任何附加核准人的核准。

下圖說明了初始 [Approvals] 頁面管理使用者介面。

圖 8-12 [Approvals] 標籤 Create User Template



若要配置核准，請使用以下步驟：

1. 完成 [Approvals Enablement] 區段 (請參閱第 243 頁的「啓用核准」)。
2. 完成 [Additional Approvers] 區段 (請參閱第 243 頁的「指定附加核准人」)。
3. 完成 [Approval Form Configuration] 區段 (僅 [Create User Template] 和 [Update User Template]) (請參閱第 251 頁的「配置核准表單」)。
4. 您配置完 [Approvals] 標籤後，可以
   - 選取其他標籤繼續編輯該範本。
   - 按一下 **[Save]** ，以儲存變更並返回到 [Configure Tasks] 頁面。
   - 按一下 **[Cancel]**，以放棄變更並返回到 [Configure Tasks] 頁面。

啟用核准

使用以下 **[Approvals Enablement]** 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，這些核取方塊對於 [Create User Template] 和 [Update User Template] 已啓用，但對於 [Delete User Template] 已**停用**。

- **[Organization Approvals]** — 啓用此核取方塊可以要求所有配置的組織核准人進行核准。
- **[Resource Approvals]** — 啓用此核取方塊可以要求所有配置的資源核准人進行核准。
- **[Role Approvals]** — 啓用此核取方塊可以要求所有配置的角色核准人進行核准。

指定附加核准人

使用 **[Determine additional approvers from]** 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。此功能表上的選項包括：

表 8-2 [Determine additional approvers from] 功能表選項

選項	說明
None (預設)	執行作業不需要附加核准人。
Attribute	核准人的帳號 ID 是從使用者的視圖中指定的屬性中導出的。
Rule	透過評估指定的規則，導出收件者的帳號 ID。
Query	透過查詢特定資源，導出收件者的帳號 ID。
Administrator List	從清單明確選擇核准人。

如果選取這些選項中的任何一個 (除了 **[None]**)，則管理使用者介面中都將顯示附加選項。配置這些選項的說明從第 243 頁開始。

使用以下各章節提供的說明來指定確定附加核准人的方法。

- 透過屬性 (第 244 頁)

- 透過規則 (第 245 頁)
- 透過查詢 (第 246 頁)
- 透過管理員清單 (第 247 頁)

透過屬性

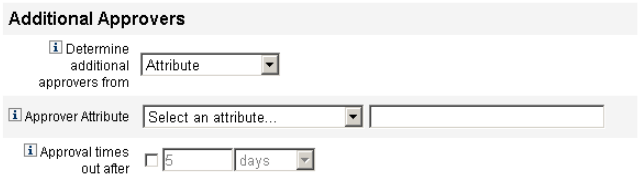
若要透過屬性確定附加核准人，

1. 從 **[Determine additional approvers from]** 功能表選取 **[Attribute]**。

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 8-13 附加核准人：屬性



- **[Approver Attribute]** — 提供用於確定核准人帳號 ID 的屬性清單 (目前爲與此範本配置的作業相關聯的視圖而定義)。
- **Approval times out after** — 提供指定核准逾時的方法。

備註 **[Approval times out after]** 設定會影響初始核准和提升的核准。

2. 使用 **[Approver Attribute]** 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。
   - 如果您要指定逾時時間期間，則請繼續閱讀第 248 頁的 「配置核准逾時」，以取得說明。
   - 如果您不想指定逾時期間，則可以繼續執行第 251 頁的 「配置核准表單」，或儲存變更並繼續配置其他標籤。

透過規則

若要從指定規則導出核准收件者帳號 ID，請使用以下步驟：

1. 從 **[Determine additional approvers from]** 功能表選取 **[Rule]**。

備註 評估之後，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 8-14 附加核准人：規則

- **[Approver Rule]** — 提供目前爲您的系統定義的規則清單，評估之後，它會傳回收件者的帳號 ID。
- **[Approval times out after]** — 提供指定核准逾時的方法。

備註 **[Approval times out after]** 設定會影響初始核准和提升的核准。

2. 從 **[Approver Rule]** 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。
   - 如果您要指定逾時時間期間，則請繼續閱讀第 248 頁的「配置核准逾時」，以取得說明。
   - 如果您不想指定逾時期間，則可以繼續執行第 251 頁的「配置核准表單」，或儲存變更並繼續配置其他標籤。

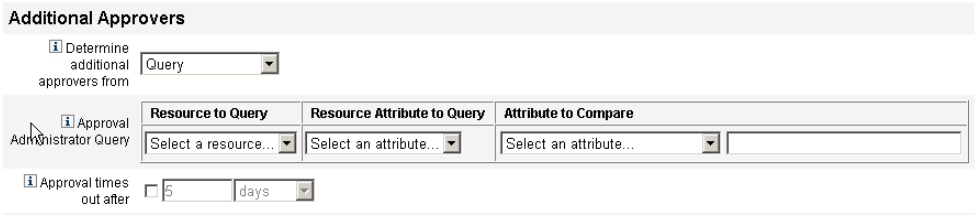
透過查詢

備註 目前僅支援 LDAP 和 Active Directory 資源查詢。

若要透過查詢指定資源導出核准人帳號 ID，請使用以下步驟：

1. 從 **[Determine additional approvers from]** 功能表中選取 **[Query]**，將會顯示以下新選項：

圖 8-15 附加核准人：查詢



- **[Approval Administrator Query]** — 提供包含以下功能表的表格，可用來建構查詢：
  - **[Resource to Query]** — 提供目前爲系統定義的資源清單。
  - **[Resource Attribute to Query]** — 提供目前爲系統定義的資源屬性清單。
  - **[Attribute to Compare]** — 提供目前爲系統定義的屬性清單。
- **[Approval times out after]** — 提供指定核准逾時的方法。

備註 **[Approval times out after]** 設定會影響初始核准和提升的核准。

2. 如下所示，建構一個查詢：
   a. 從 **[Resource to Query]** 功能表中選取資源。
   b. 從 **[Resource Attribute to Query]** 和 **[Attribute to Compare]** 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。
   - 如果您要指定逾時時間期間，則請繼續閱讀第 248 頁的「配置核准逾時」，以取得說明。

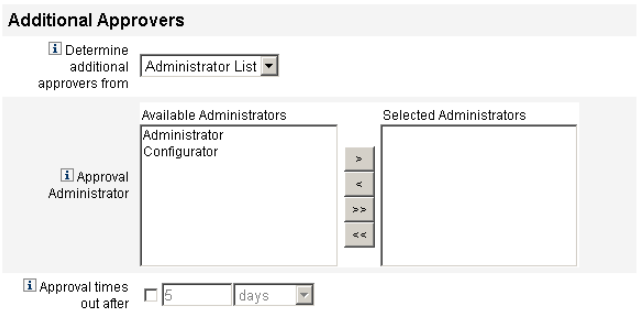
- 如果您不想指定逾時期間，則可以繼續執行第 251 頁的「配置核准表單」，或儲存變更並繼續配置其他標籤。

透過管理員清單

若要從管理員清單中明確選擇附加核准人，

1. 從 **[Determine additional approvers from]** 功能表中選取 **[Administrators List]**，將會顯示以下新選項：

圖 8-16 附加核准人：管理員清單



- **[Administrators to Notify]** — 提供選取工具和可用管理員的清單。
- **[Approval Form]** — 提供附加核准人可以用於核准或拒絕核准人請求的使用者表單之清單。
- **[Approval times out after]** — 提供指定核准逾時的方法。

備註 **[Approval times out after]** 設定會影響初始核准和提升的核准。

2. 在 [Available Administrators] 清單中選取一個或多個管理員，然後使用 > 按鈕或 >> 按鈕將所選名稱移至 [Selected Administrators] 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。
   - 如果您要指定逾時時間期間，則請繼續閱讀第 248 頁的「配置核准逾時」，以取得說明。
   - 如果您不想指定逾時期間，則可以繼續執行第 251 頁的「配置核准表單」，或儲存變更並繼續配置其他標籤。

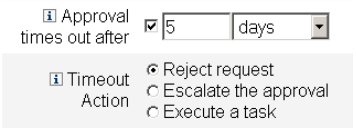
配置核准逾時

若要配置核准逾時，

1. 啓用該核取方塊。

   旁邊的文字欄位和功能表變爲可使用狀態，並顯示 **[Timeout Action]** 按鈕，如下圖中所示。

圖 8-17 [Approval Timeout] 選項



2. 使用 **[Approval times out after]** 文字欄位和功能表可以指定逾時期間，如下所示：

   a. 從功能表中選取 [seconds]、[minutes]、[hours] 或 [days]。

   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 **[Approval times out after]** 設定會影響初始核准和提升的核准。

3. 啓用以下 **[Timeout Action]** 按鈕之一，以指定核准逾時後應執行的作業：

   - **[Reject Request]** — 如果請求在指定的逾時時間期間之前沒有被核准，Identity Manager 將自動拒絕該請求。
   - **[Escalate the approval]** — 如果請求在指定的逾時時間期間之前沒有被核准，Identity Manager 將自動將該請求提升至其他核准人。

     啓用此按鈕後，將顯示新的選項，因爲您必須指定 Identity Manager 將如何爲提升核准確定核准人。繼續閱讀第 249 頁的「提升核准」，以取得說明。
   - **[Execute a task]** — 如果核准請求在指定的逾時時間期間之前沒有被核准，Identity Manager 將自動執行替代作業。

     啓用此按鈕，並顯示 **[Approval Timeout Task]** 功能表後，您可以指定在核准請求逾時後要執行的作業。繼續閱讀第 251 頁的「執行作業」，以取得說明。

提升核准

啓用 [Timeout Action] **[Escalate the approval]** 按鈕後，**[Determine escalation approvers from]** 功能表將如下顯示：

圖 8-18 [Determine Escalation Approvers From] 功能表

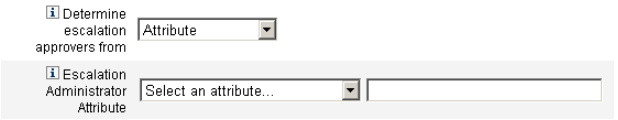
從此功能表中選取以下選項之一來指定如何爲提升核准確定核准人。

- **[Attribute]** — 從新使用者的視圖中指定的屬性中確定核准人的帳號 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。

  顯示 **[Escalation Administrator Attribute]** 功能表時，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 8-19 [Escalation Administrator Attribute] 功能表

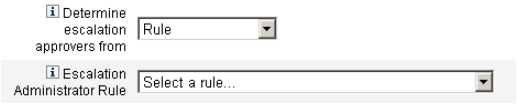
  

- **[Rule]** — 透過評估指定的規則，確定核准人帳號 ID。

  備註 評估之後，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。

  顯示 **[Escalation Administrator Rule]** 功能表時，從清單中選取規則。

  圖 8-20 [Escalation Administrator Rule] 功能表

- **[Query]** — 透過查詢特定資源，確定核准人帳號 ID。

  顯示 **[Escalation Administrator Query]** 功能表時，如下所示建構查詢：

  a. 從 **[Resource to Query]** 功能表中選取資源。

  b. 從 **[Resource Attribute to Query]** 功能表中選取屬性。

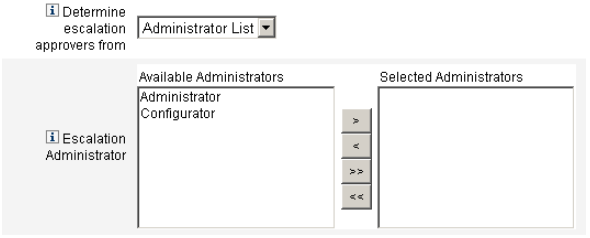
  c. 從 **[Attribute to Compare]** 功能表中選取屬性。

圖 8-21 [Escalation Administrator Query] 功能表

- **[Administrator List]** (預設) — 從清單中明確選擇核准人。

  顯示 **[Escalation Administrator]** 選取工具後，如下選取核准人：

圖 8-22 [Escalation Administrator] 選取工具



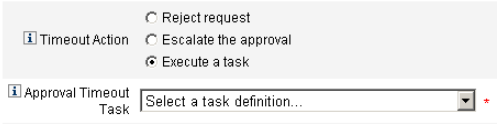
  a. 從 **[Available Administrators]** 清單中，選取一個或多個管理員名稱。

  b. 使用 > 按鈕或 >> 按鈕將這些名稱移到 **[Selected Administrators]** 清單中。

執行作業

啓用逾時動作 **[Execute a task]** 按鈕後，**[Approval Timeout Task]** 功能表將顯示如下：

圖 8-23 [Approval Timeout Task] 功能表



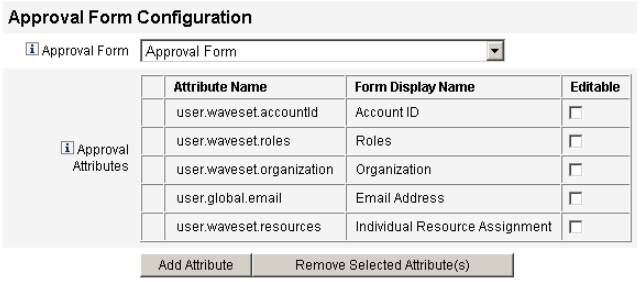
指定核准請求逾時後要執行的作業。例如，您可以允許請求者向管理員傳送說明請求或傳送報告。

配置核准表單

備註 [Delete User Template] 不包含 [Approval Form Configuration] 區段。您僅可以爲 [Create User Template] 和 [Update User Template] 配置此區段。

您可以使用 [Approval Form Configuration] 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 8-24 核准表單配置



依預設，[Approval Attributes] 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 [Approval Attributes] 表格中指定的表單屬性。

若要爲附加核准人配置核准表單：

1. 從 **[Approval Form]** 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 **[Approval Attributes]** 表格的 **[Editable]** 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，則核准者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` 屬性做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 **[Add Attribute]** 或 **[Remove Selected Attribute(s)]** 按鈕，以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。
   - 若要將屬性增加到表單，請參閱第 253 頁的 「增加屬性」。
   - 若要從表單中移除屬性，請參閱第 253 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。

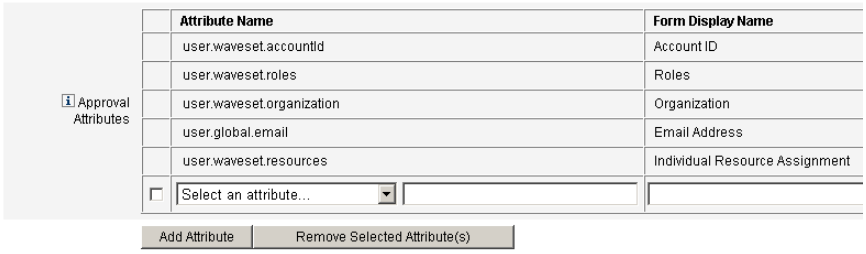
增加屬性

將屬性增加到核准表單

1. 按一下 [Approval Attributes] 表格下的 **[Add Attribute]** 按鈕。

   在 [Approval Attributes] 表格中，**[Attribute name]** 功能表將變爲可使用狀態，如下圖中所示：

圖 8-25 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，且屬性的預設顯示名稱將顯示在 [Form Display Name] 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 **[Editable]** 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。

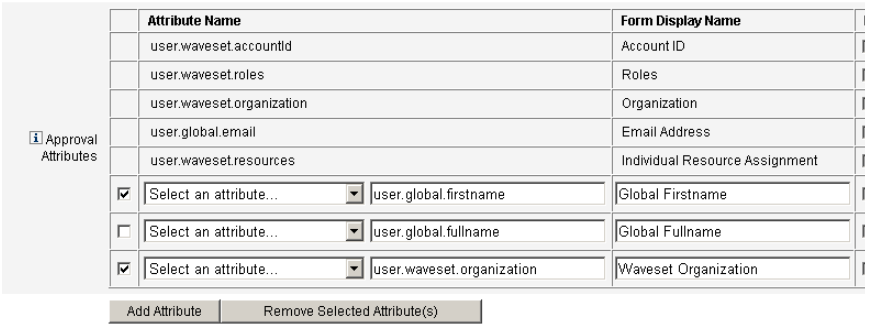
若要從核准表單移除屬性，請使用以下步驟：

1. 啓用 [Approval Attributes] 表最左欄中的一個或多個核取方塊。

2. 按一下 **[Remove Selected Attribute(s)]** 按鈕，可以立即移除從 [Approval Attributes] 表中選取的屬性。

   例如，如果按一下 **[Remove Selected Attribute(s)]** 按鈕，則 `user.global.firstname` 和 `user.waveset.organization` 將從下表移除。

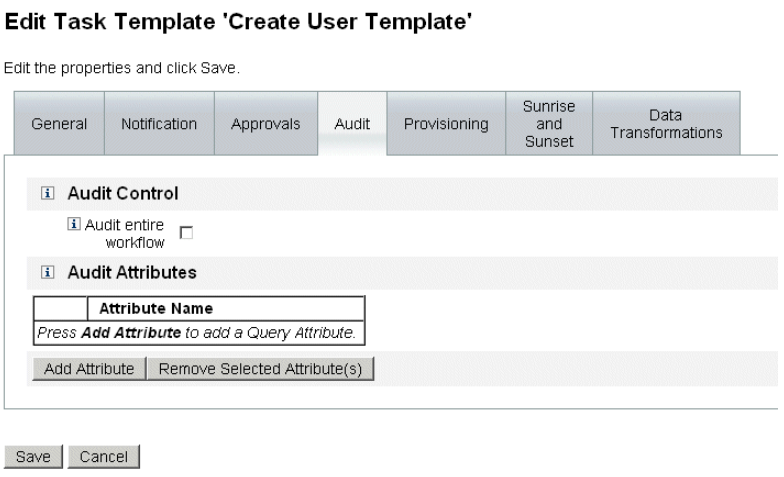
圖 8-26 移除核准屬性



配置 [Audit] 標籤

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 [Audit] 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 8-27 稽核建立使用者範本



若要從使用者範本的 [Audit] 標籤配置稽核，請：

1. 啓用 **[Audit entire workflow]** 核取方塊以啓動工作流程稽核功能。
2. 按一下 **[Add Attribute]** 按鈕 (在 [Audit Attributes] 區段中)，以選取您要記錄的屬性以進行報告。
3. **[Select an attribute]** 功能表顯示在 [Audit Attributes] 表中後，從清單中選取屬性。

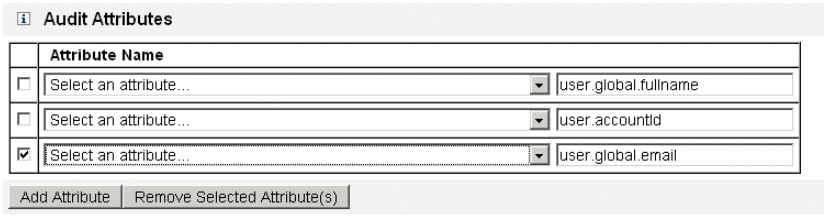
   屬性名稱將顯示在旁邊的文字欄位中。

圖 8-28 增加屬性

若要從 [Audit Attributes] 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 8-29 移除 user.global.email 屬性



2. 按一下 **[Remove Selected Attribute(s)]** 按鈕。

您配置完此標籤後，可以

- 選取其他標籤繼續編輯範本。
- 按一下 **[Save]** ，以儲存變更並返回到 [Configure Tasks] 頁面。
- 按一下 **[Cancel]**，以放棄變更並返回到 [Configure Tasks] 頁面。

配置 [Provisioning] 標籤

備註 此標籤僅對 [Create User Template] 和 [Update User Template] 可用。

您可以使用 [Provisioning] 標籤來配置與佈建相關的以下選項：

圖 8-30 [Provisioning] 標籤：Create User Template

- **[Provision in the background]** — 啓用此核取方塊可以在背景中執行建立、刪除或更新作業，而非同步執行作業。

  在背景中佈建可讓您在執行作業時繼續在 Identity Manager 中工作。

- **[Add Retry link to the task result]** — 啓用此核取方塊可以在作業執行中產生佈建錯誤時，將 **[Retry]** 連結增加到使用者介面。**[Retry]** 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。

您配置完 [Provisioning] 標籤後，可以

- 選取其他標籤繼續編輯範本。
- 按一下 **[Save]** ，以儲存變更並返回到 [Configure Tasks] 頁面。
- 按一下 **[Cancel]**，以放棄變更並返回到 [Configure Tasks] 頁面。

配置 [Sunrise and Sunset] 標籤

備註 此標籤僅對 [Create User Template] 可用。

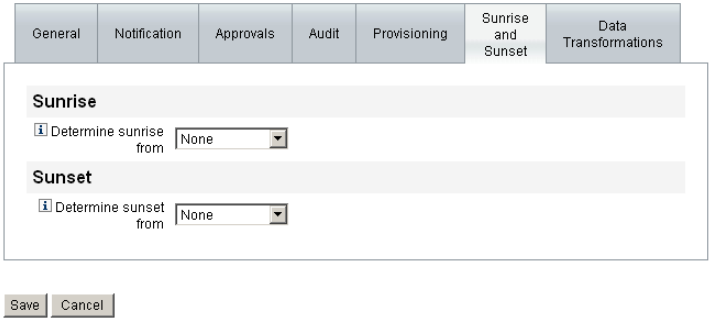
您可以使用 [Sunrise and Sunset] 標籤，來選取確定以下動作之發生時間和日期的方法。

- 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 8-31 說明了 [Sunrise and Sunset] 標籤上的設定。

圖 8-31 [Sunrise and Sunset] 標籤：Create User Template



下面的主題提供了配置 [Sunrise and Sunset] 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。

若要配置生效，請執行以下程序：

1. 從 **[Determine sunrise from]** 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。
    - **[Specifying a Time]** — 將佈建延遲到未來的指定時間。繼續閱讀第 258 頁，以取得說明。

- **[Specifying a Date]** — 將佈建延遲到未來的指定日曆日期。繼續閱讀第 259 頁，以取得說明。
- **[Specifying an Attribute]** — 根據使用者視圖中的屬性，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。

  繼續閱讀第 259 頁，以取得說明。
- **[Specifying a Rule]** — 根據評估後產生日期 / 時間字串的規則延遲取消佈建。同指定屬性時一樣，您可以指定資料將遵循的日期格式。

  繼續閱讀第 260 頁，以取得說明。

備註 **[Determine sunrise from]** 功能表預設爲 **[None]** 選項，允許立即進行佈建。

2. 從 **[Work Item Owner]** 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 [Approvals] 標籤中可用。

3. 配置完生效後，您可以
   - 選取其他標籤繼續編輯 [Create User Template]。
   - 按一下 **[Save]** ，以儲存變更並返回到 [Configure Tasks] 頁面。
   - 按一下 **[Cancel]**，以放棄變更並返回到 [Configure Tasks] 頁面。

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 **[Determine sunrise from]** 功能表選取 **[Specified time]**。
2. 當新的文字欄位和功能表顯示在 **[Determine sunrise from]** 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 8-32 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 **[Determine sunrise from]** 功能表選取 **[Specified day]**。
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 8-33 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來確定佈建日期和時間，請執行以下步驟：

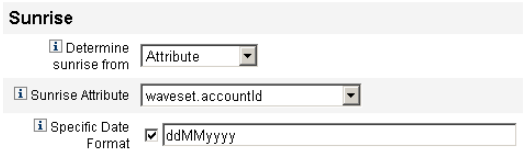
1. 從 **[Determine sunrise from]** 功能表中選取 **[Attribute]** ，以下選項將變爲可使用狀態：
   - **[Sunrise Attribute]** 功能表 — 提供目前爲與此範本配置的作業相關聯的視圖而定義的屬性清單。
   - **[Specific Date Format]** 核取方塊和功能表 — 讓您可以指定屬性值的日期格式字串 (如有必要)。

備註	若您未啓用 **[Specific Date Format]** 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 **[Sunrise Attribute]** 功能表中選取屬性。
3. 如有必要，啓用 **[Specific Date Format]** 核取方塊，並在 **[Specific Date Format]** 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 8-34 透過屬性佈建新使用者



指定規則

若要透過評估指定的規則來確定佈建日期和時間，請執行以下步驟：

1. 從 **[Determine sunrise from]** 功能表中選取 **[Rule]** ，以下選項將變爲可使用狀態：
   - **[Sunrise Rule]** 功能表 — 提供目前爲系統定義的規則清單。
   - **[Specific Date Format]** 核取方塊和功能表 — 讓您可以指定規則傳回值的日期格式字串 (如有必要)。

備註 若您未啓用 **[Specific Date Format]** 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 **[Sunrise Rule]** 功能表中選取規則。
3. 如有必要，啓用 **[Specific Date Format]** 核取方塊，並在 **[Specific Date Format]** 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 8-35 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 **[Sunset Task]** 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，請執行以下程序：

1. 使用 **[Determine sunset from]** 功能表指定用於確定進行取消佈建時間的方法：

備註	**[Determine sunset from]** 功能表預設爲 **[None]** 選項，允許立即進行取消佈建。

   - **[Specified time]** — 將取消佈建延遲到指定的未來時間。請參閱第 258 頁的「指定時間」，以取得說明。
   - **[Specified date]** — 將取消佈建延遲到指定的未來行事曆日期。請參閱第 259 頁的「指定日期」，以取得說明。
   - **[Attribute]** — 根據使用者帳號資料中的屬性，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。

     請參閱第 259 頁的「指定屬性」，以取得說明。
   - **[Rule]** — 根據評估後產生日期 / 時間字串的規則延遲取消佈建。同指定屬性時一樣，您可以指定資料將遵循的日期格式。

     請參閱第 260 頁的「指定規則」，以取得說明。
2. 使用 **[Sunset Task]** 功能表，指定作業以在指定的日期和時間取消佈建使用者。
3. 您配置完此標籤後，可以
   - 選取其他標籤繼續編輯範本。
   - 按一下 **[Save]** ，以儲存變更並返回到 [Configure Tasks] 頁面。
   - 按一下 **[Cancel]**，以放棄變更並返回到 [Configure Tasks] 頁面。

配置 [Data Transformations] 標籤

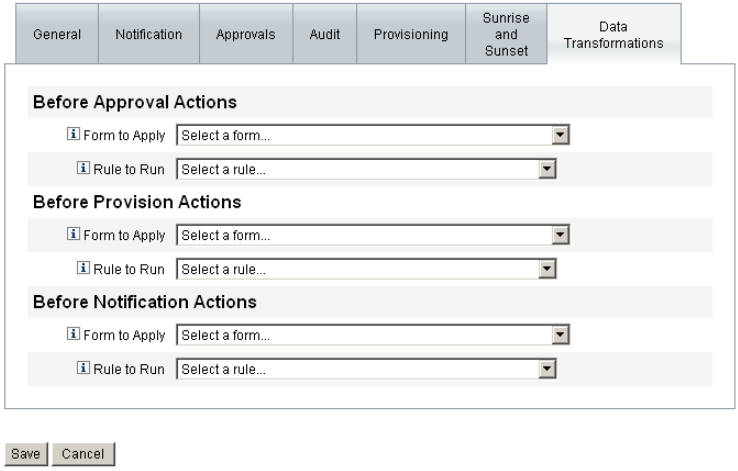
備註 此標籤僅對 [Create User Template] 和 [Update User Template] 可用。

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 [Data Transformations] 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 [Data Transformations] 標籤後，將顯示以下頁面：

圖 8-36 [Data Transformations] 標籤：Create User Template



此頁面包括以下區段：

- **[Before Approval Actions]** — 如果您要在將核准請求傳送到指定核准人之前變換使用者帳號資料，則配置此區段的選項。
- **[Before Provision Actions]** — 如果您要在佈建動作之前變換使用者帳號資料，則配置此區段的選項。
- **[Before Notification Actions]** — 如果您要在將通知傳送到指定收件者之前變換使用者帳號資料，則配置此區段的選項。

您可以在每個區段中配置以下選項：

- **[Form to Apply]** 功能表 — 提供目前爲系統配置的表單清單。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。
- **[Rule to Run]** 功能表 — 提供目前爲系統配置的規則清單。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。

您配置完此標籤後，可以

- 選取其他標籤繼續編輯範本。
- 按一下 **[Save]** ，以儲存變更並返回到 [Configure Tasks] 頁面。
- 按一下 **[Cancel]**，以放棄變更並返回到 [Configure Tasks] 頁面。

章節 9

PasswordSync

本章說明了 Sun Java™ System Identity Manager PasswordSync 功能，該功能使 Windows 用戶端可以變更其在 Windows Active Directory 和 Windows NT 網域中的密碼，從而使變更與 Identity Manager 同步。

資訊組織如下：

什麼是 PasswordSync？

PasswordSync 功能可以使在 Windows Active Directory 和 Windows NT 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。必須在將與 Identity Manager 同步之網域中的每個網域控制器上安裝 PasswordSync。必須將 PasswordSync 與 Identity Manager 分開安裝。

在網域控制器上安裝 PasswordSync 後，該控制器將與做爲 Java Messaging Service (JMS) 用戶端代理伺服器的 Servlet 進行通訊。而該 Servlet 與啓用 JMS 的訊息佇列進行通訊。JMS 偵聽程式資源配接器將從佇列中移除訊息，並使用工作流程作業處理密碼變更。密碼將在使用者的所有指定資源中更新，並且 SMTP 伺服器將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	密碼變更必須將要轉寄的變更請求的本機密碼策略傳送至 Identity Manager 伺服器以實現同步化。如果提議的密碼變更不遵循本機密碼策略，則 ADSI 將顯示錯誤對話方塊，並且不向 Identity Manager 傳送任何同步化資料。

安裝前注意事項

只能在 Windows 2000、Windows 2003 和 Windows NT 網域控制器上安裝 PasswordSync 功能。您必須在將與 Identity Manager 同步的網域中的每個網域控制器上安裝 PasswordSync。

PasswordSync 需要具有與 JMS 伺服器的連結性。如需有關 JMS 系統需求的更多資訊，請參閱「Sun Java™ System Identity Manager 資源參照」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安裝 Microsoft .NET 1.1 或更高版本
- 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，您必須安裝 Microsoft .NET 1.1 或更高版本的 Framework。如果您使用 Windows 2003 網域控制器，則依預設安裝此 Framework。如果您使用 Windows 2000 或 Windows NT 網域控制器，則可以從 Microsoft 下載中心下載此工具組：

http://www.microsoft.com/downloads

備註

- Microsoft .NET 1.1 Framework 需要 Internet Explorer 5.01 或更高版本。Internet Explorer 5.0 (隨附於 Windows 2000 SP4) 無法滿足需要。
- 在 [Keywords] 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。

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。

安裝 PasswordSync

以下程序說明了如何安裝 PasswordSync 配置應用程式。

備註 您必須在將與 Identity Manager 同步的網域中的每個網域控制器上安裝 PasswordSync。

1. 在 Identity Manager 安裝媒體中，按一下 `pwsync\IdmPwSync.msi` 圖示。將顯示歡迎視窗。

   安裝精靈提供了以下瀏覽按鈕：

   - **[Cancel]**：按一下可隨時結束精靈，而不儲存任何變更。
   - **[Back]**：按一下可返回前一個對話方塊。
   - **[Next]**：按一下可進入下一個對話方塊。

2. 請閱讀歡迎螢幕上提供的資訊，然後按 [Next] 以顯示 [Choose Setup Type PasswordSync Configuration] 視窗。
   PasswordSync 安裝

3. 按一下 [Typical] 或 [Complete] 以安裝完整的 PasswordSync 套裝軟體，或按一下 [Custom] 以控制要安裝套裝軟體的哪些部分。

4. 按一下 [Install] 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 [Finish] 以完成安裝程序。

   請確定選取 [Launch Configuration Application]，以便可以開始配置 Password Sync。請參閱 「第 268 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 9-1 說明了安裝在每個網域控制器上的檔案。

表 9-1 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
%$INSTALL_DIR$%\DotNetWrapper.dll	處理 .NET SOAP 通訊的 DLL
%$INSTALL_DIR$%\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。

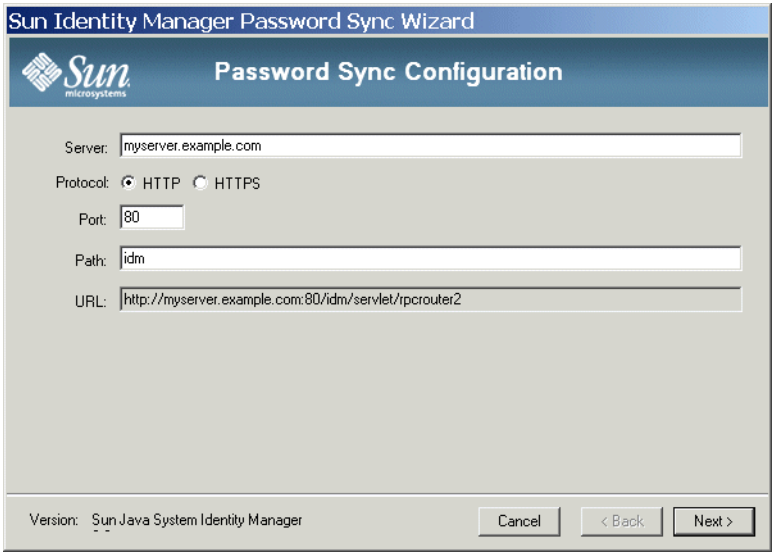
執行以下步驟來配置 PasswordSync

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 Java System Identity Manager PasswordSync > [Configuration] 中。

   螢幕上將顯示 [PasswordSync Configuration] 對話方塊 (請參閱圖 9-1)。

圖 9-1 PasswordSync Configuration] 對話方塊

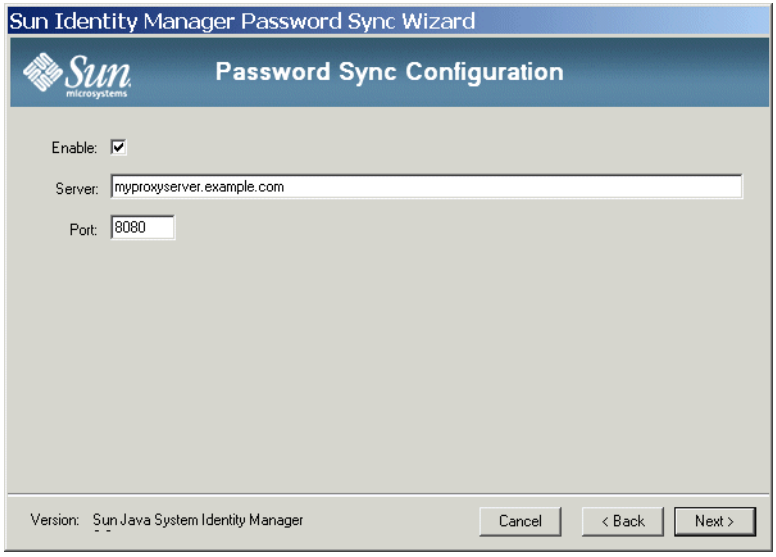


依需要編輯以下欄位。

- **[Server]** 必須用安裝 Identity Manager 的完全合格的主機名稱或 IP 位址替代。
- **[Protocol]** 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。
- **[Path]** 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 [Next] 以顯示代理伺服器配置頁面 (圖 9-2)。

圖 9-2 代理伺服器對話方塊

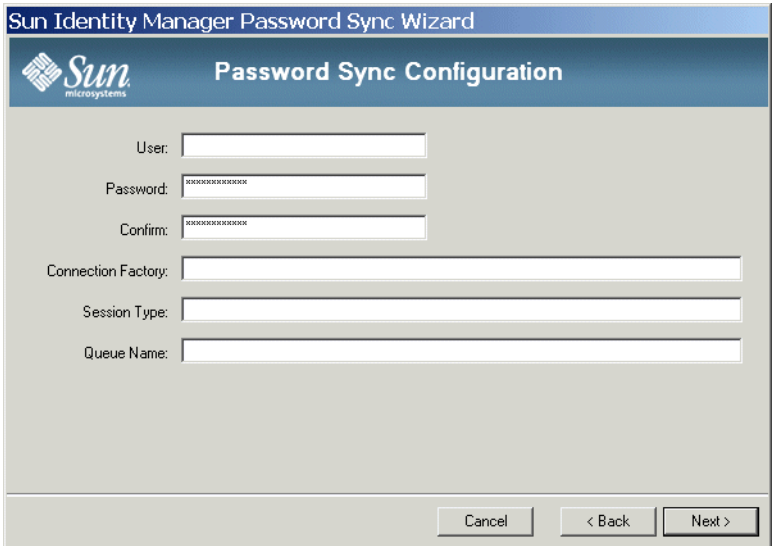


依需要編輯以下欄位。

- 如果需要代理伺服器，則按一下 [Enable]。
- **[Server]** 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 [Next] 以顯示 JMS 設定對話方塊 (圖 9-3)。

圖 9-3 JMS 設定對話方塊

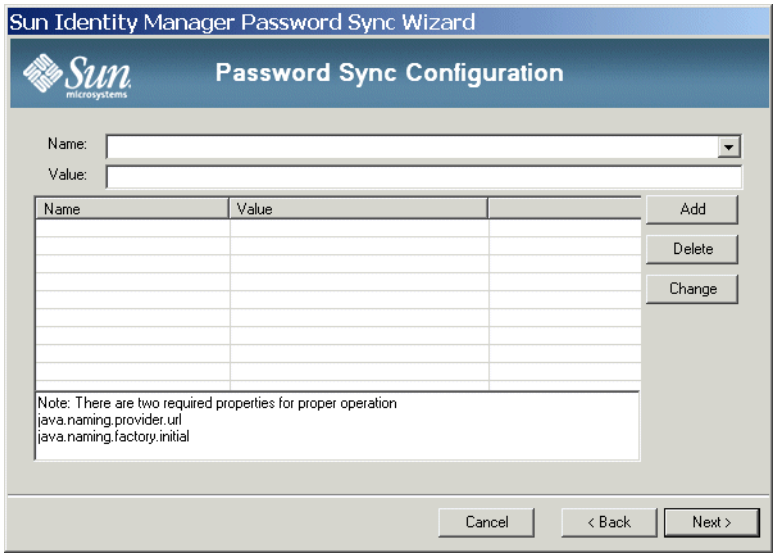


依需要編輯以下欄位。

- **[User]** 指定在佇列中置入新訊息的 JMS 使用者名稱。
- **[Password]** 和 **[Confirm]** 指定 JMS 使用者的密碼。
- **[Connection Factory]** 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 **[Session Type]** 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]`。
- **[Queue Name]** 指定密碼同步化事件的目標查詢名稱。

4. 按 [Next] 以顯示 JMS 特性對話方塊 (圖 9-4)。

圖 9-4 JMS 特性對話方塊



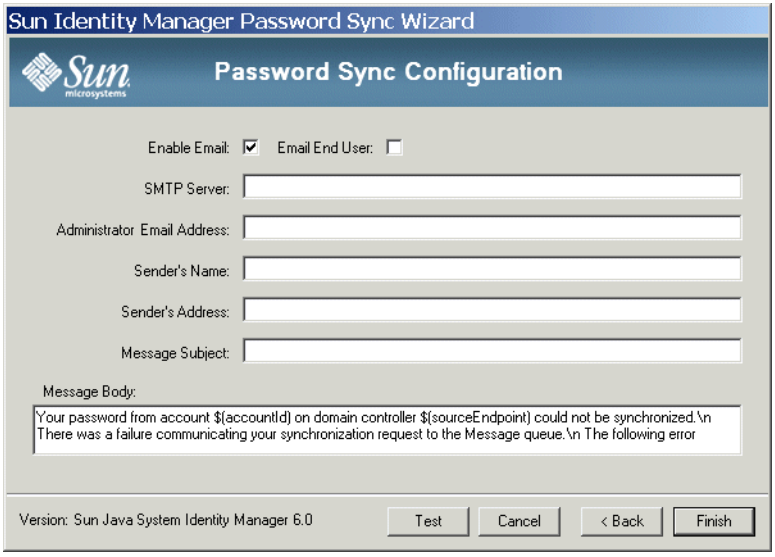
JMS 特性對話方塊可讓您定義用於建置初始 JNDI 環境的特性集。必須定義以下名稱 / 值對：

- `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的類別名稱 (包括套裝軟體)。

[Name] 下拉式功能表包含 `java.naming` 套裝軟體中的類別清單。選取類別或鍵入類型名稱，然後在 [Value] 欄位中輸入其對應的值。

5. 按 [Next] 以顯示電子郵件對話方塊 (圖 9-5)。

圖 9-5 電子郵件對話方塊



透過 [Email] 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 **[Enable Email]** 以啓用該功能。如果使用者要接收通知，請選取 **[Email End User]**。否則，將僅通知管理員。
- **[SMTP Server]** 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。
- **[Administrator Email Address]** 是用於傳送通知的電子郵件位址。
- **[Sender's Name]** 是寄件者的「易記名稱」。
- **[Sender's Address]** 是寄件者的電子郵件地址。
- **[Message Subject]** 指定所有通知的主旨行
- **[Message Body]** 指定通知的文字。

  郵件內文可能包含以下變數。

  - `$(accountId)` — 嘗試變更密碼的使用者的帳號 ID。
  - `$(sourceEndpoint)` — 安裝密碼提示程式的網域控制器的主機名稱，有助於找到出現故障的電腦。

- `$(errorMessage)` — 說明所發生之錯誤的錯誤訊息。

6. 按一下 [Finish] 以儲存變更。

如果再次執行配置應用程式，則螢幕上將顯示一組標籤，而非精靈。如果您希望將應用程式顯示爲精靈，請從指令行輸入以下指令：

`C:\`*InstallDir*`\Configure.exe -wizard`

對 PasswordSync 執行除錯

本節提供了有關尋找診斷 PasswordSync 問題時需要的資訊以及使用配置工具啓用追蹤的詳細資訊。還列出了對 PasswordSync 執行除錯或啓用配置工具無法實作的功能時可能需要的登錄機碼。

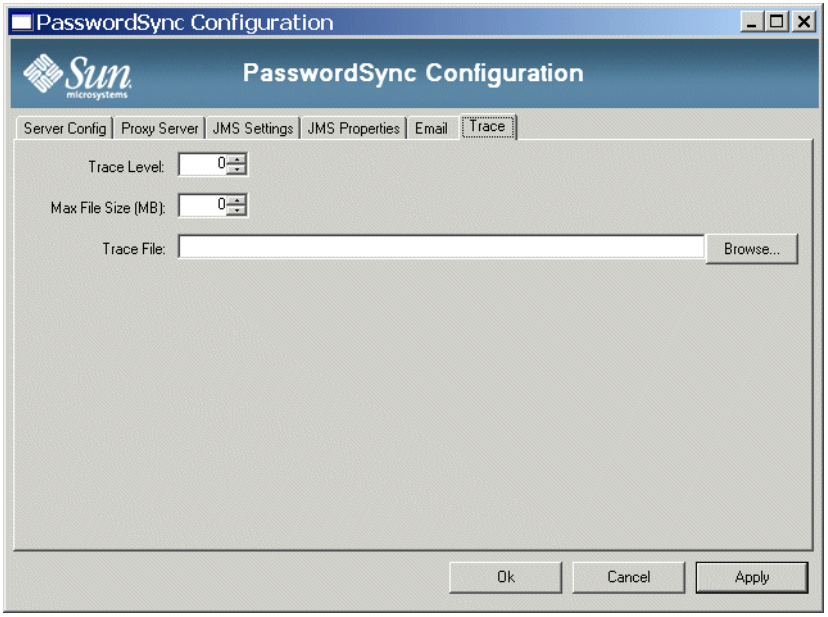
錯誤記錄

PasswordSync 會將所有故障寫入 Windows 事件檢視器。錯誤記錄項目的來源名稱是 *PasswordSync*。

追蹤記錄

首次執行配置工具時，精靈並不包含用於配置追蹤的面板。然而，以後每次啓動該工具時都會顯示 [Trace] 標籤 (圖 9-6)。

圖 9-6 [Trace] 標籤



[Trace Level] 欄位指定寫入追蹤記錄時 PasswordSync 將提供的詳細資訊層級。值 0 表示已關閉追蹤，而值 4 表示提供最多詳細資訊。

當追蹤檔案超過 [Max File Size (MB)] 欄位中指定的大小時，PasswordSync 會將檔案移至附加了 `.bk` 的基準名稱中。例如，如果將追蹤檔案設定爲 `C:\logs\pwicsvc.log`，並將追蹤層級設定爲 100 MB，則當追蹤檔案超過 100 MB 時，PasswordSync 會將該檔案重新命名爲 `C:\logs\pwicsvc.log.bk`，並將新資料寫入新的 `C:\logs\pwicsvc.log file` 中。

登錄機碼

您可以使用 Windows 登錄編輯器編輯表 9-2 中列出的登錄機碼。這些機碼位於：

`HKEY_LOCAL_MACHINE\SOFTWARE\Waveset\Lighthouse\PasswordSync`

此位置也會顯示其他機碼，但這些機碼可以使用配置工具進行編輯。

表 9-2 登錄機碼

機碼名稱	類型	說明
allowInvalidCerts	REG_DWORD	如果設定為 1，則該機碼將在 .NET 用戶端上設定以下旗標： • SECURITY_FLAG_IGNORE_UNKNOWN_CA • INTERNET_FLAG_IGNORE_CERT_CN_INVALID • INTERNET_FLAG_IGNORE_CERT_DATE_INVALID 結果，用戶端將容許過期或具有無效 CN 或主機名稱的憑證。這僅適用於使用 SSL 的情況。 在測試環境 (大多數憑證從無效的憑證授權單位 (CA) 產生) 中進行除錯時，該設定非常有用。 預設為 0。
clientConnectionFlags	REG_DWORD	將傳送至 .NET SOAP 用戶端的可選連線標幟。 預設為 0。
clientSecurityFlags	REG_DWORD	可傳送至 .NET SOAP 用戶端的可選安全標幟。 預設為 0。
installdir	REG_SZ	安裝 PasswordSync 應用程式的目錄。
soapClientTimeout	REG_DWORD	出現故障之前 SOAP 用戶端與 Identity Manager 伺服器的通訊逾時 (以毫秒為單位)。

解除安裝 PasswordSync

若要解除安裝 PasswordSync 應用程式，請至 Windows [控制台] 並選取 [新增 / 移除程式]。然後選取 [Sun Java System Identity Manager PasswordSync] 並按一下 [移除]。

備註 也可以透過載入 Identity Manager 安裝媒體並按一下 `pwsync\IdmPwSync.msi` 圖示來解除安裝 (或重新安裝) PasswordSync。

必須重新啓動系統才能完成該程序。

部署 PasswordSync

若要部署 PasswordSync，您必須在 Identity Manager 中執行以下動作：

- 配置 JMS 偵聽程式配接器
- 實作同步化使用者密碼工作流程
- 設定通知

配置 JMS 偵聽程式配接器

網域控制器間接將訊息置入佇列中後，必須將資源配接器配置爲接受這些訊息。您必須建立 JMS 偵聽程式資源配接器並對其進行配置以與佇列通訊。請參閱「Sun Java™ System Identity Manager 資源參照」以取得有關設定該配接卡的更多資訊。

您必須配置以下資源參數：

- **Destination Type** — 通常將該值設定爲 [Queue]。因爲有一個訂閱者而有多個潛在發佈者，所以主題通常不相關。
- **Initial context JNDI properties** — 該文字方塊定義用於建置初始 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 服務之電腦的 URI。
  - `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的類別名稱 (包括套裝軟體)。

  可能需要定義其他特性。特性和值清單應與配置應用程式的 JMS 設定頁面上指定的特性和值相符。
- **JNDI Name of Connection factory** — 在 JMS 伺服器中定義的連線工廠的名稱。
- **User** 與 **Password** — 從佇列中請求新事件的管理員的帳號名稱和密碼。
- **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。

實作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接受來自 JMS 偵聽程式配接卡的每個請求，出庫使用 ChangeUserPassword 檢視器，然後再將 ChangeUserPassword 檢視器入庫納管。完成簽入後，工作流程將反覆運算所有資源帳號並選取除來源資源以外的所有資源。Identity Manager 將使用電子郵件通知使用者所有資源上的密碼變更是否成功。

如果您要預設實作同步化使用者密碼工作流程，請將其指定爲 JMS 偵聽程式配接器實例的程序規則。可以在配接器的 Active Sync 精靈中指定程序規則。

如果您要修改預設的同步化使用者密碼工作流程，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 Java™ System Identity Manager 工作流程、表單與檢視」。

設定通知

Identity Manager 提供了 [Password Synchronization Notice] 和 [Password Synchronization Failure Notice] 電子郵件範本。這些範本可通知使用者在多個資源之間變更密碼的嘗試是否成功。

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。請參閱第 130 頁的「自訂電子郵件範本」。

使用 Sun JMS 伺服器配置 PasswordSync

Identity Manager 提供了 JMS 偵聽程式配接卡，可以使密碼變更事件在 JMS 訊息伺服器上形成佇列，以提高穩定性並保證傳送品質。

備註 請參閱「Sun Java™ System Identity Manager 資源參照」以取得有關此配接卡的更多資訊。

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。資訊組織如下：

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 Java™ System Identity Manager 6.0 2005Q4M3
- 在 Suse Linux 10.0 上執行的 MySQL 4.1.13
- Tomcat 5.0.28 running on Suse Linux 10.0
- 在 Suse Linux 10.0 上執行的 Sun Java™ System Message Queue 3.6 SP3 2005Q4
- 在 Suse Linux 10.0 上執行的 Sun Java™ System Directory Server 5.2 SP4
- Java 1.4.2

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)

解決方案簡介

分析在 Windows PasswordSync 解決方案中起作用的所有元件時，將發生以下情況：

1. 使用者變更其工作站上的密碼時，PasswordSync 會向目前的 Active Directory 網域控制器傳送密碼修改，而 Identity Manager 密碼擷取 dll (位於網域控制器上) 會擷取明文密碼。
2. 密碼擷取 dll 向 Identity Manager SOAP 請求處理程式發出 SOAP 請求。

   此 SOAP 請求中封裝有使用者 ID、已加密的密碼以及必要的 JMS 配置資訊。例如，

代碼範例 9-1 SOAP 請求範例

```
POST /idm/servlet/rpcrouter2 HTTP/1.0
Accept:text/*
SOAPAction:"urn:lighthouse"
Content-Type:text/xml; charset=utf-8
User-Agent:VCSoapClient
Host: 192.168.1.4:8080
Content-Length: 1154
Connection:Keep-Alive
Pragma:no-cache
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
   xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
<soap:Body soap:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<snp:queuePasswordUpdate xmlns:snp="urn:lighthouse">
<userEmailAddress xsi:nil="1"/>
<resourceAccountId>CN=John Smith,OU=people,DC=org,DC=local</resourceAccountId>
<resourceAccountGUID>b4e1c14b79d3a949a618a607dde7784d</resourceAccountGUID>
<password>zkpS8qcIJkVBWa/Frp+JqA==</password>
<accounts xsi:nil="1"/>
<resourcename xsi:nil="1"/>
<resourcetype>Windows Active Directory</resourcetype>
<clientEndpoint>W2003EE</clientEndpoint>
<jmsUser>guest</jmsUser>
```

代碼範例 9-1 SOAP 請求範例 (繼續)

```
<jmsPassword>guest</jmsPassword>
<queueName>cn=pwsyncDestination</queueName>
<connectionFactory>cn=pwsyncFactory</connectionFactory>
<sessionType>LOCAL</sessionType>
<JNDIProperties>java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory;java.naming.
   provider.url=ldap://gwenig.coopsrccom:389/ou=sunmq,dc=coopsrc,dc=com</JNDIProperties>
<singleResult>true</singleResult>
</snp:queuePasswordUpdate>
</soap:Body>
</soap:Envelope>
```

3. SOAP 處理程式接收請求並使用請求中包含的 JMS 參數啓動與 JMS Message Queue 代理程式的連線。然後 SOAP 處理程式傳送包含使用者 ID 和已加密密碼的訊息 (與稍後要討論的一些其他參數一起)。

   例如，Message Queue 代理程式上的 SOAP 處理程式會傳送類似以下內容的訊息 (屬於 *MapMessage* 類型)：

   代碼範例 9-2 SOAP 處理程式訊息

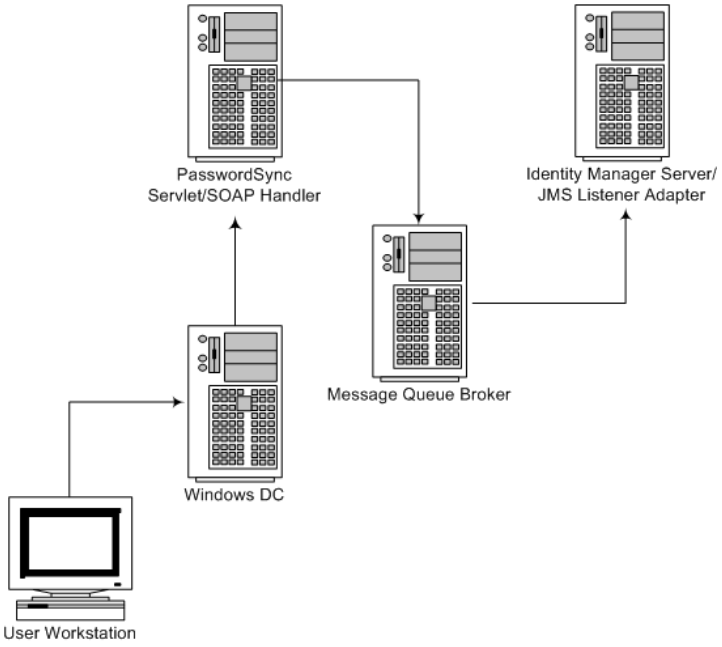
   ```
   password:zkpS8qcIJkVBWa/Frp+JqA==
   accounts:null
   resourceAccountGUID:8f245d1490de7a4192a8821c569c9ac4
   requestTimestamp: 1143639284325
   queueName:cn=pwsyncDestination
   jmsUser:guest
   resourcetype:Windows Active Directory
   resourcename:null
   JNDIProperties:
   java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory;
   java.naming.provider.url=ldap://gwenig.coopsrc.com:389/
   ou=sunmq,dc=coopsrc,dc=com
   connectionFactory:cn=pwsyncFactory
   clientEndpoint:W2003EE
   userEmailAddress:null
   sessionType:LOCAL
   jmsPassword:guest
   resourceAccountId:CN=John Smith,OU=people,DC=org,DC=local
   ```

4. Message Queue 代理程式使訊息形成佇列，JMS 偵聽程式配接卡擷取訊息。現在 Identity Manager 可以啓動工作流程。

   圖 9-7 說明了此方案範例中使用的配置：

備註 雖然此圖顯示的是不同伺服器上的 SOAP 處理程式和 Identity Manager，但是您可以在同一伺服器上同時執行它們。

圖 9-7 方案配置



JMS 簡介

Java Message Service (JMS) API 是一個訊息傳送標準，可讓應用程式元件 (基於 Java 2 Platform, Enterprise Edition (J2EE)) 建立、傳送、接收以及讀取訊息。此 API 可啓用鬆耦合、穩定且非同步的分散式通訊。

若要傳送或接收訊息，必須首先將 JMS 用戶端連線至 JMS 提供者 (通常將該 JMS 提供者做爲訊息代理程式實作)。此連線可開啓用戶端和代理程式間的通訊通道。然後，用戶端必須設定一個用於建立、產生以及消耗訊息的階段作業。

JMS 無法完全定義以下訊息傳送元素：

- **[Connection factories]** — 連線工廠管理的物件可產生用戶端與代理程式的連線。這些物件封裝有提供者特定的資訊，可管理特定方面的訊息傳送運作方式；例如連線處理、用戶端標識、訊息標頭置換、穩定性以及流量控制等等。源自指定連線工廠的每個連線都展示爲該工廠配置的運作方式。

- **[Destinations]** — 目標管理的物件參照代理程式上的實體目標。這些物件封裝有提供者特定的命名 (地址 - 語法) 慣例，並指定使用目標的訊息傳送網域 — 佇列或主題。

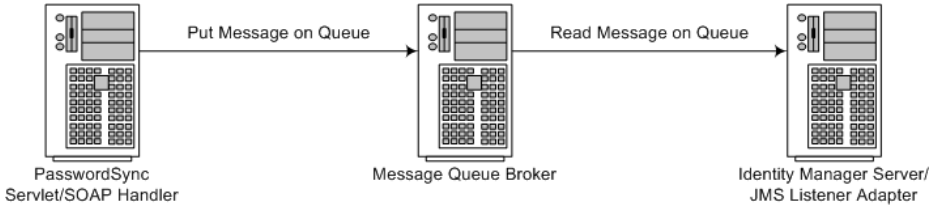
這兩個物件通常是使用管理工具建立和配置，而不是有計劃地建立。然後，它們將儲存在物件存放區，JMS 用戶端透過標準 JNDI 查詢對其進行存取。

備註 如需有關連線工廠和目標的更多資訊，請參閱「Sun Java™ System Message Queue Technical Overview」，位於：

http://docs.sun.com/source/819-2574/intro.html

圖 9-8 說明了方案範例的通訊流程：

圖 9-8 方案通訊流程



當 SOAP 處理程式接收到來自 Windows 密碼擷取 dll 的請求時，SOAP 處理程式會做爲代理伺服器將 SOAP 請求翻譯爲 JMS 訊息。然後 JMS 偵聽程式配接卡會接收訊息並觸發相關工作流程。

若要使用 JMS 代理程式，Identity Manager SOAP 處理程式和 Identity Manager JMS 偵聽程式配接卡必須都具有連線工廠和目標 (使用 JNDI 查詢)。

Identity Manager SOAP 處理程式會取得 SOAP 訊息中的必要詳細資訊 (如之前所示)：

代碼範例 9-3 SOAP 訊息

```
<jmsUser>guest</jmsUser>
<jmsPassword>guest</jmsPassword>
<queueName>cn=pwsyncDestination</queueName>
<connectionFactory>cn=pwsyncFactory</connectionFactory>
<sessionType>LOCAL</sessionType>
<JNDIProperties>java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory;java.naming.
  provider.url=ldap://gwenig.coopsrc.com:389/ou=sunmq,dc=coopsrc,dc=com</JNDIProperties>
```

在 Windows 上安裝並配置 PasswordSync 時，將提供以下所有參數 (圖 9-9 和圖 9-10 中所示)：

圖 9-9 [JMS Settings] 標籤

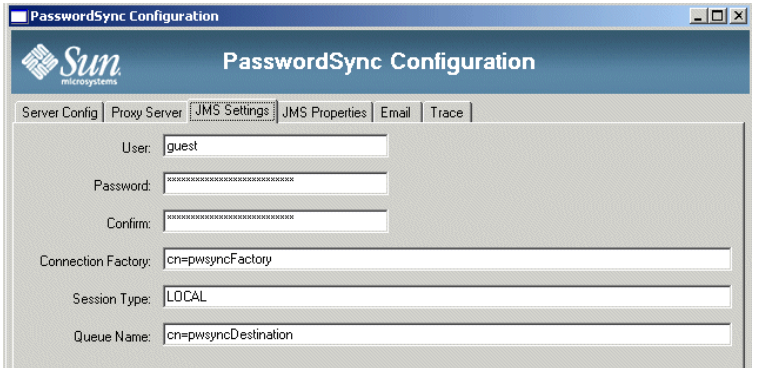
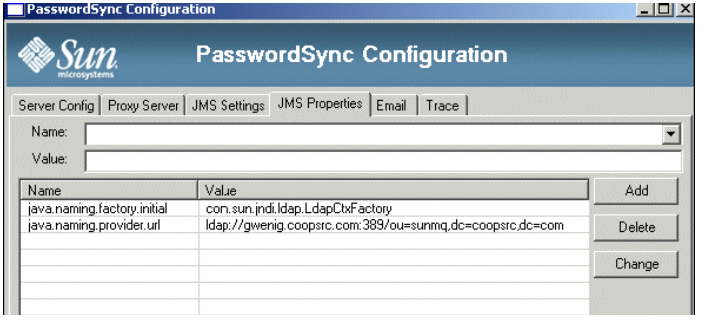


圖 9-10 [JMS Properties] 標籤



以下各節說明了這些參數：

- JMS 設定參數
- JMS 特性參數

JMS 設定參數

[JMS Settings] 標籤包含以下參數：

- **[User]** 和 **[Password]** 欄位：定義連線到 JMS 代理程式時要使用的憑證。
- **[Connection Factory]** 欄位：指定連線工廠物件的 JNDI 查詢名稱。
- **[Session Type]** 欄位：指定
- **[Queue Name]** 欄位：指定目標物件的 JNDI 查詢名稱。

在代碼範例 9-4 中，[Connection Factory] 和 [Queue Name] 都是 LDAP RDN，其 (當與 `java.naming.provider.url` 耦合時) 可形成完整 DN。一個簡單的 `ldapsearch` 即可顯示管理的物件項目：

代碼範例 9-4 連線工廠和佇列名稱範例

```
連線工廠：
#> ldapsearch -h gwenig.coopsrc.com -b 'dc=coopsrc,dc=com' 'cn=pwsyncfactory'
dn:cn=pwsyncFactory,ou=sunmq,dc=coopsrc,dc=com
objectClass:top
objectClass:javaContainer
objectClass:javaObject
objectClass:javaNamingReference
javaClassName:com.sun.messaging.QueueConnectionFactory
javaFactory:com.sun.messaging.naming.AdministeredObjectFactory
javaReferenceAddress:#0#version#3.0
javaReferenceAddress:#1#readOnly#false
javaReferenceAddress:#2#imqOverrideJMSPriority#false
javaReferenceAddress:#3#imqConsumerFlowLimit#1000
javaReferenceAddress:#4#imqAddressListIterations#1
javaReferenceAddress:#5#imqOverrideJMSExpiration#false
javaReferenceAddress:#6#imqConnectionType#TCP
javaReferenceAddress:#7#imqLoadMaxToServerSession#true
javaReferenceAddress:#8#imqPingInterval#30
javaReferenceAddress:#9#imqSetJMSXUserID#false
javaReferenceAddress:#10#imqConfiguredClientID#
javaReferenceAddress:#11#imqSSLProviderClassname#com.sun.net.ssl.internal.ssl.Provider
javaReferenceAddress:#12#imqJMSDeliveryMode#PERSISTENT
javaReferenceAddress:#13#imqConnectionFlowLimit#1000
javaReferenceAddress:#14#imqConnectionURL#http://localhost/imq/tunnel
javaReferenceAddress:#15#imqBrokerServiceName#
javaReferenceAddress:#16#imqJMSPriority#4
javaReferenceAddress:#17#imqBrokerHostName#localhost
javaReferenceAddress:#18#imqJMSExpiration#0
```

代碼範例 9-4 連線工廠和佇列名稱範例 (繼續)

```
javaReferenceAddress:#19#imqAckOnProduce#
javaReferenceAddress:#20#imqEnableSharedClientID#false
javaReferenceAddress:#21#imqAckTimeout#0
javaReferenceAddress:#22#imqAckOnAcknowledge#
javaReferenceAddress:#23#imqConsumerFlowThreshold#50
javaReferenceAddress:#24#imqDefaultPassword#guest
javaReferenceAddress:#25#imqQueueBrowserMaxMessagesPerRetrieve#1000
javaReferenceAddress:#26#imqDefaultUsername#guest
javaReferenceAddress:#27#imqReconnectEnabled#false
javaReferenceAddress:#28#imqConnectionFlowCount#100
javaReferenceAddress:#29#imqAddressListBehavior#PRIORITY
javaReferenceAddress:#30#imqReconnectAttempts#0
javaReferenceAddress:#31#imqSetJMSXAppID#false javaReferenceAddress:
#32#imqConnectionHandler#com.sun.messaging.jmq.jmsclient.protocol.
tcp.TCPStreamHandler
javaReferenceAddress:#33#imqSetJMSXRcvTimestamp#false
javaReferenceAddress:#34#imqBrokerServicePort#0
javaReferenceAddress:#35#imqDisableSetClientID#false
javaReferenceAddress:#36#imqSetJMSXConsumerTXID#false
javaReferenceAddress:#37#imqOverrideJMSDeliveryMode#false
javaReferenceAddress:#38#imqBrokerHostPort#7676
javaReferenceAddress:#39#imqQueueBrowserRetrieveTimeout#60000
javaReferenceAddress:#40#imqSSLIsHostTrusted#true
javaReferenceAddress:#41#imqSetJMSXProducerTXID#false
javaReferenceAddress:#42#imqConnectionFlowLimitEnabled#false
javaReferenceAddress:#43#imqReconnectInterval#3000
javaReferenceAddress:#44#imqAddressList#mq://gwenig:7676/jms
javaReferenceAddress:#45#imqOverrideJMSHeadersToTemporaryDestinations#false
cn:pwsyncFactory
```

目標如下：

代碼範例 9-5 目標範例

```
#> ldapsearch -h gwenig.coopsrc.com -b 'dc=coopsrc,dc=com' 'cn=pwsyncdestination'
dn:cn=pwsyncDestination,ou=sunmq,dc=coopsrc,dc=com
objectClass:top
objectClass:javaContainer
objectClass:javaObject
objectClass:javaNamingReference
javaClassName:com.sun.messaging.Queue
javaFactory:com.sun.messaging.naming.AdministeredObjectFactory
javaReferenceAddress:#0#version#3.0
javaReferenceAddress:#1#readOnly#false
javaReferenceAddress:#2#imqDestinationName#pwsyncQueue
javaReferenceAddress:#3#imqDestinationDescription#A Description for the Destination Object
cn:pwsyncDestination
```

JMS 特性參數

在方案範例中，連線工廠和目標物件位於 LDAP 目錄中。

`java.naming.factory.initial` 是用於建立初始 JNDI 環境的工廠類別值。

`java.naming.provider.url` 可保留環境特性的名稱，該環境特性用於爲使用中的服務提供者指定配置資訊。如果您不提供更多資訊，則 PasswordSync 將使用匿名 LDAP 階段作業擷取連線工廠和目標物件。

若要提供憑證和連結方法，請指定以下特性：

- `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

備註 您必須爲 JMS 偵聽程式配接卡定義同樣的設定。

圖 9-11 JMS 偵聽程式資源參數頁面

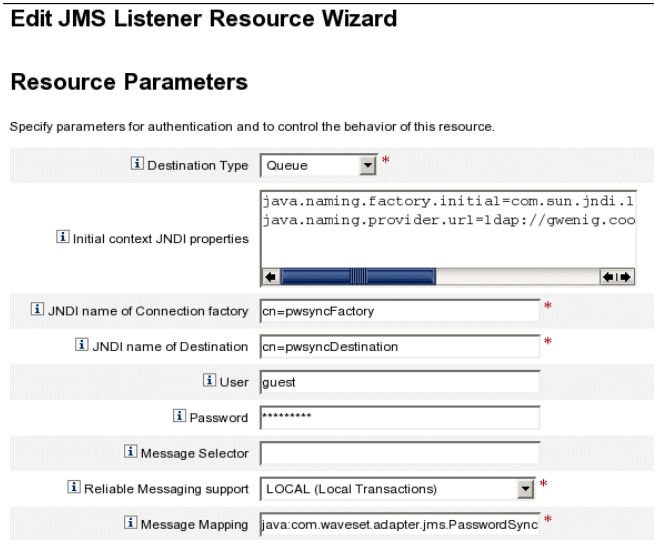
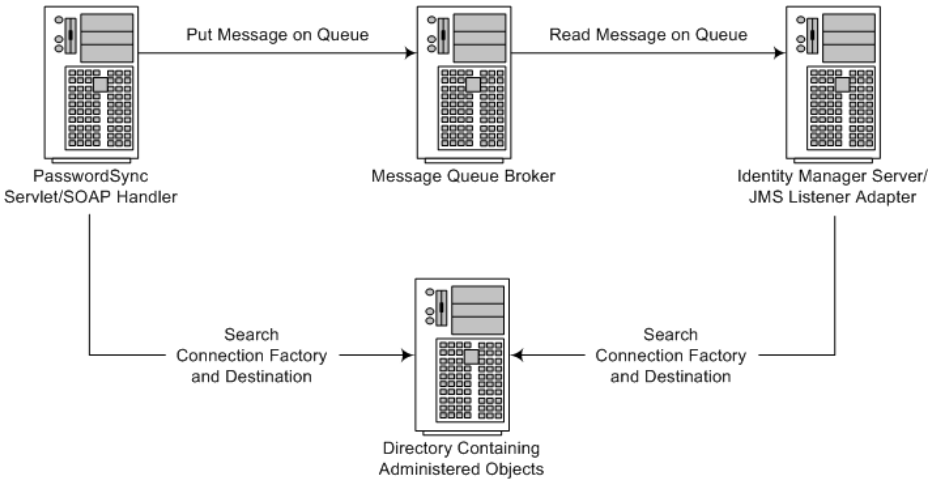


圖 9-12 詳細說明了程序：

圖 9-12 擷取連線工廠和目標物件



SOAP 處理程式和 JMS 偵聽程式配接卡都必須搜尋連線工廠和目標，以便傳送 / 接收訊息。

建立與儲存管理的物件

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

備註

- 本小節中的說明假設您已安裝 Sun Java™ System 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`) 建立這些受管理的物件。以下說明使用指令行工具。

將管理的物件儲存在 LDAP 目錄中

本小節提供了將連線工廠物件儲存在 LDAP 目錄中所需的指令。

儲存連線工廠物件

使用代碼範例 9-6 中的指令儲存連線工廠物件：

代碼範例 9-6 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.
```

其中 imqAddressList 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

使用代碼範例 9-7 中的指令儲存目標物件：

代碼範例 9-7 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。

將管理的物件儲存在檔案中

本小節說明了如何使用指令行工具將管理的物件儲存在檔案中。

儲存連線工廠物件

代碼範例 9-8 提供了儲存連線工廠物件和指定查詢名稱所需的指令：

代碼範例 9-8 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 Java System 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，則您必須使用代碼範例 9-9 (其中 *myTestQueue* 爲目標) 中顯示的指令在代理程式上建立目標物件：

代碼範例 9-9 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.
```

您可以將管理的物件儲存在目錄或檔案中：

- **在目錄中**：如果 Identity Manager SOAP 處理程式和 Identity Manager 伺服器未在您的 Identity Manager 部署中的同一伺服器上執行，則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，這些管理的物件做爲目錄項目儲存。

  備註 如果 Identity Manager SOAP 處理程式和 Identity Manager 伺服器未在同一台機器上，則二者必須都可以存取 `.bindings` 檔案。您可以重複建立兩次管理的物件 (在每台機器上)，或將 `.bindings` 檔案複製到每台機器上的適當位置。

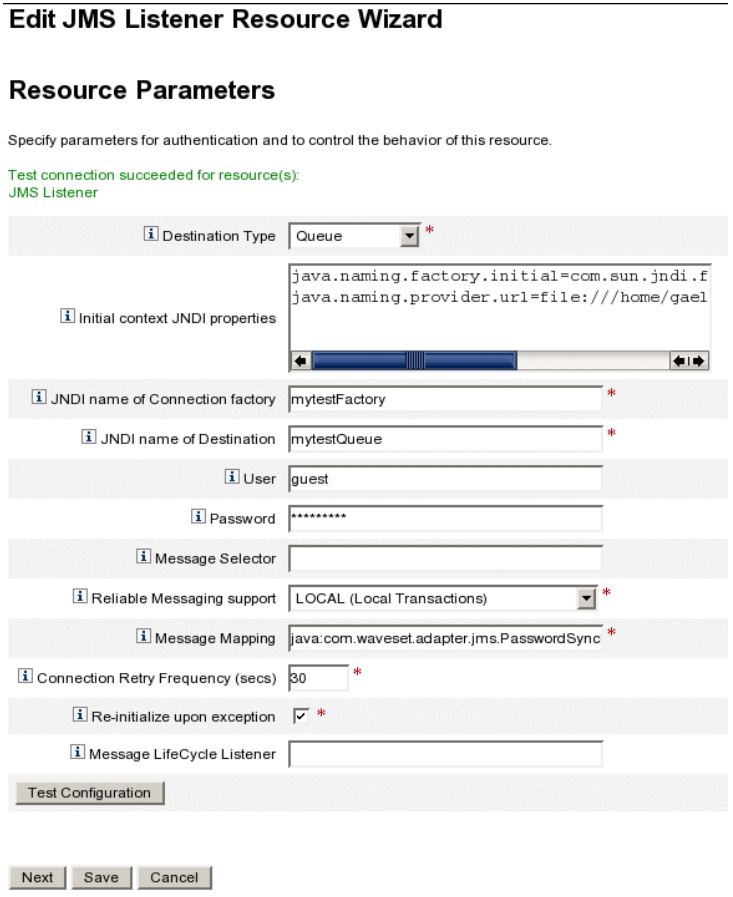
- **在檔案中**：如果 Identity Manager SOAP 處理程式和 Identity Manager 伺服器均在同一伺服器上執行 (或者如果沒有可用的目錄)，則可以將管理物件儲存在檔案中。

  使用檔案時，兩個管理的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 偵聽程式配接卡

JMS 偵聽程式配接卡配置的第一個頁面看起來應與圖 9-13 中的頁面相似：

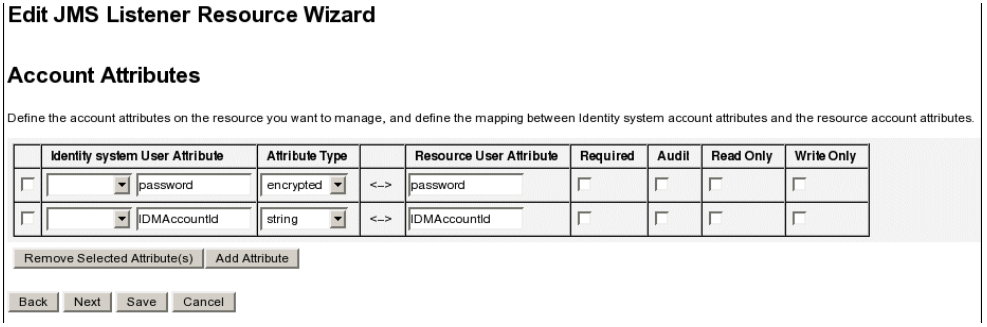
圖 9-13 JMS 偵聽程式 [Adapter Resource Parameters] 頁面



若要配置 JMS 偵聽程式配接卡，請：

1. 在 [Message Mapping] 欄位中指定 **`java:com.waveset.adapter.jms.PasswordSyncMessageMapper`**，以將內送 JMS 訊息轉換爲同步化使用者密碼工作流程可以使用的格式。
2. 爲此方案對映以下屬性 (JMS 偵聽程式配接卡可透過 `PasswordSyncMessageMapper` 使用)：
   - **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**：以 SOAP 請求接收加密密碼並以 JMS 訊息轉寄該密碼。

圖 9-14 對映 IDMAccountId 與 password 帳號屬性



在模式對映中配置這些屬性欄位時，Active Sync 精靈 (圖 9-15) 之 [Attribute Mappings] 區段中的資源可以使用這些屬性。

備註 此處未提供身份識別範本。

圖 9-15 Active Sync 屬性對映

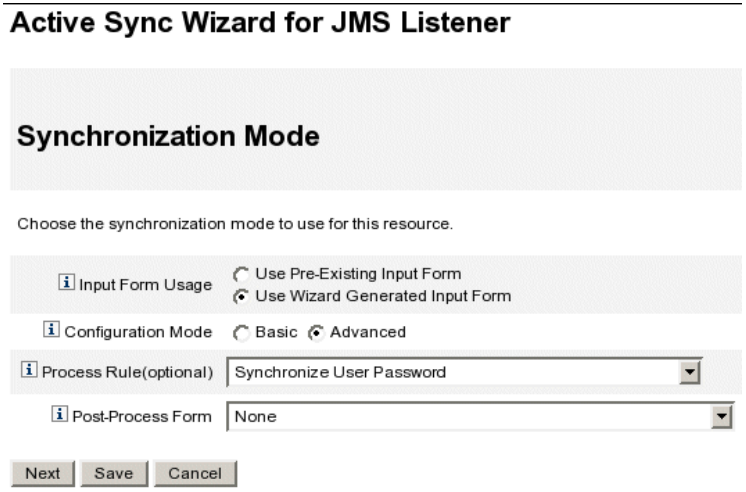
配置 Active Sync

使用 JMS 偵聽程式的 Active Sync 精靈在進階配置模式下為此方案配置 Active Sync。

1. 當 [Synchronization Mode] 螢幕顯示時 (圖 9-16)，您可以保持參數設定為預設值，然後按 [Next] 繼續。

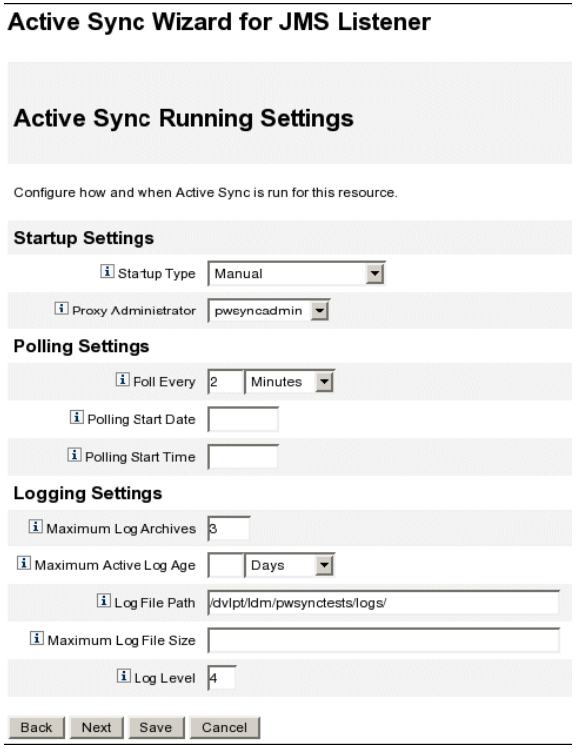
   預設的同步化使用者密碼工作流程接受來自 JMS 偵聽程式配接卡的每個請求，出庫使用 ChangeUserPassword 檢視器，然後再將 ChangeUserPassword 檢視器入庫納管。

圖 9-16 [Synchronization Mode] 螢幕



2. 顯示 [Active Sync Running Settings] 面板時，您必須定義與空白表單關聯的代理伺服器管理員 (pwsyncadmin)。

圖 9-17 [Active Sync Running Settings] 面板



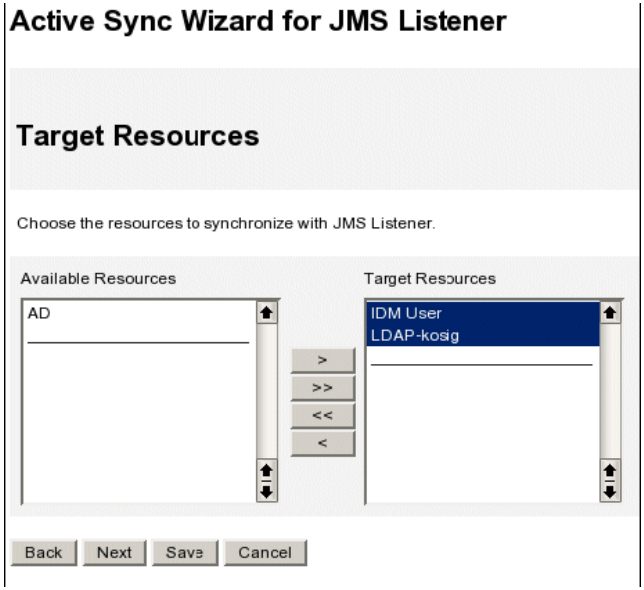
3. 爲除錯目的，將記錄層級設定爲 **4** 並指定記錄檔路徑，以在特定目錄中產生詳細的記錄檔。

   例如，圖 9-17 中顯示的記錄檔將儲存到 `/dvlpt/Idm/pwsynctests/logs/` 目錄中。

4. 完成後，按 [Next] 繼續。

5. 請勿變更接下來的兩個 Active Sync 精靈面板中的預設值。您只需按 [Next] 直到顯示 [Target Resources] 螢幕 (圖 9-18)。

圖 9-18 [Target Resources] 螢幕



6. 使用目標資源選取工具指定目標資源。從 [Available Resources] 清單中選取資源並按一下 [>] 按鈕，以將資源移至 [Target Resources] 清單。

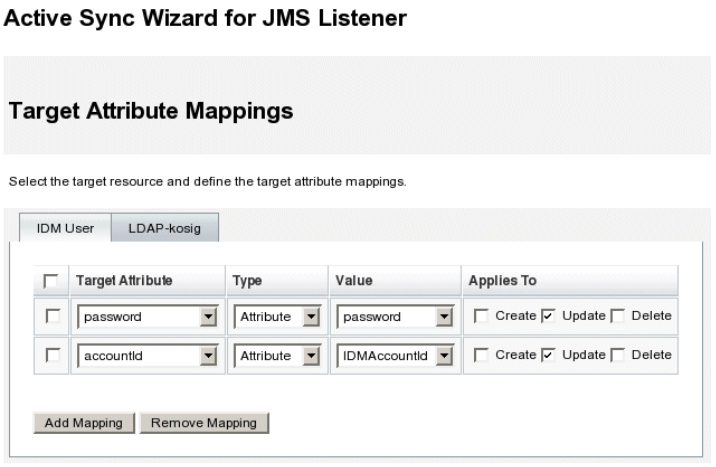
   例如，在此方案中你要同步化 Windows 密碼與 Sun Directory Server，並且要同步化 Identity Manager 密碼。

7. 按 [Next]，當顯示 [Target Attribute Mappings] 面板時，選取 [IDM User] 標籤 (如果尚未選取)。

8. 在 [IDM User] 標籤中，使用表格爲 Identity Manager 使用者指定目標屬性對映。

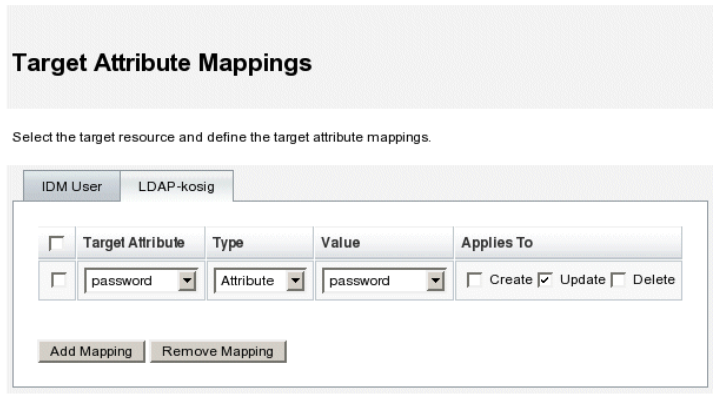
   例如，在圖 9-19 中定義了 `password` 和 `accountID`：

圖 9-19 定義 password 和 accountID



9. 完成後，按一下 [Add Mapping]。
10. 選取 [LDAP-kosig] 標籤以爲 Sun Directory 定義目標屬性對映 (圖 9-20)：

圖 9-20 爲 Sun Directory 定義目標屬性對映



11. 完成後，按一下 [Add Mapping]，然後儲存變更。

對您的配置執行除錯

您可以使用 Windows PasswordSync 配置應用程式來對 Windows 端的配置執行除錯。

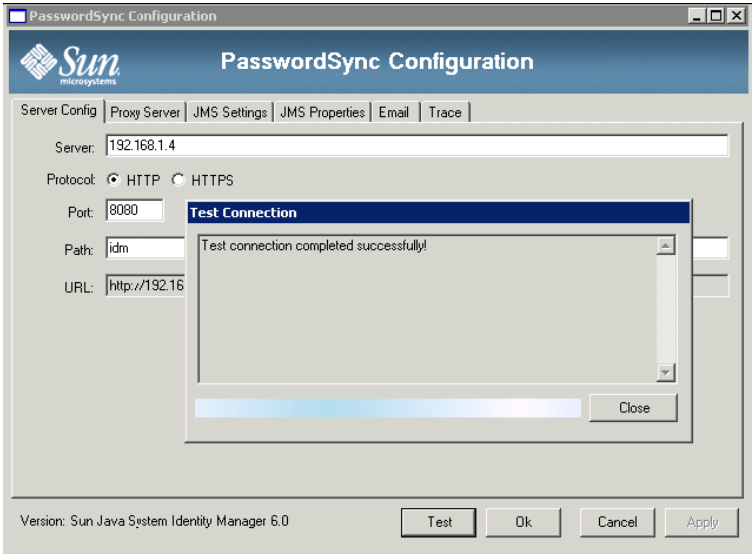
1. 如果尚未執行 PasswordSync 配置應用程式，請將其啓動。

   依預設，此配置應用程式安裝在 [Program Files] > [Sun Java System Identity Manager PasswordSync] > [Configuration] 中。

2. 當顯示 [PasswordSync Configuration] 對話方塊時，按一下 [Test] 按鈕。

3. 將顯示 [Test Connection] 對話方塊 (圖 9-21)，其中包含一條訊息表明測試連線是否成功完成。

圖 9-21 [Test Connection] 對話方塊

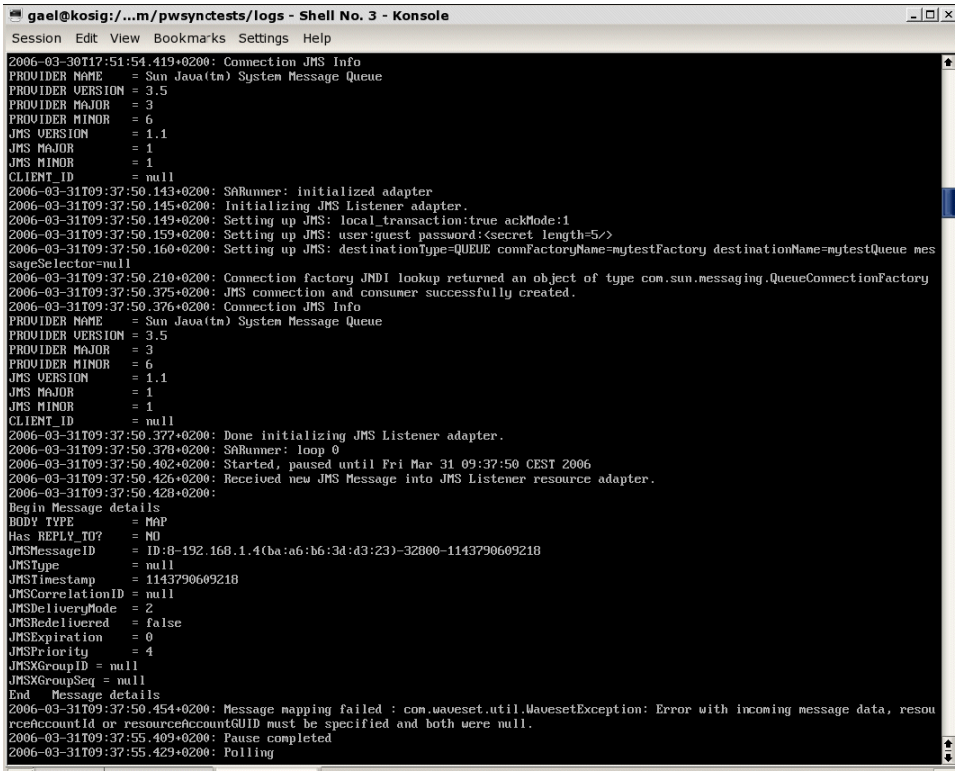


4. 按一下 [Close] 以關閉 [Test Connection] 對話方塊。

5. 按一下 [OK] 以關閉 [PasswordSync Configuration] 對話方塊。

   然後 JMS 偵聽程式配接卡將在除錯模式中執行，並在檔案中產生除錯資訊，與圖 9-22 所示相似：

圖 9-22 除錯資訊檔案

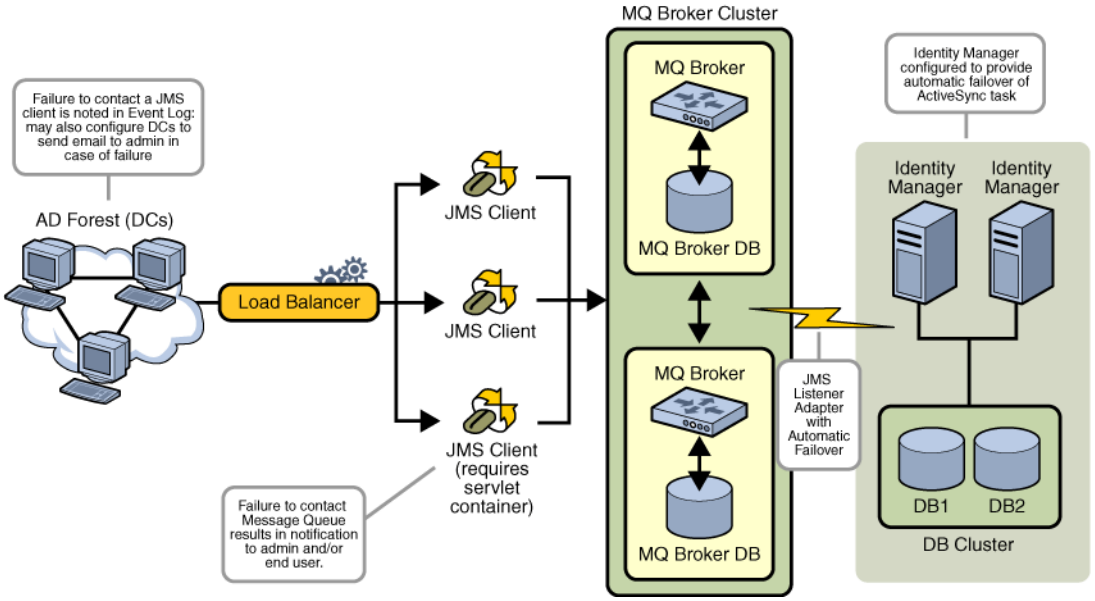


PasswordSync 的容錯移轉部署

PasswordSync 的架構有助於消除 Identity Manager 之 Windows 密碼同步化部署中的任何單一故障點。

如果您將每個 Active Directory 網域控制器 (ADC) 配置爲透過負載平衡器連線到一系列 JMS 用戶端之一 (請參閱圖 9-23)，則 JMS 用戶端可以向 Message Queue 代理程式叢集傳送訊息，以確保有 Message Queue 發生故障時不會遺失訊息。

圖 9-23 PasswordSync 的容錯移轉部署



備註 Message Queue 叢集可能需要一個用於保留訊息的資料庫。(在供應商的產品文件中應提供有配置 Message Queue 代理程式叢集的說明。)

執行配置爲自動容錯移轉之 JMS 偵聽程式配接卡的 Identity Manager 伺服器將連絡 Message Queue 代理程式叢集。儘管該配接卡每次僅在一個 Identity Manager 上執行，但是如果主 ActiveSync 伺服器發生故障，則該配接卡將開始在次要 Identity Manager 伺服器上輪詢密碼相關訊息，並將密碼變更向外傳播到下行流程的資源。

有關 PasswordSync 的常見問題

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 [Notification Package] 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 [Notification Package] 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。

密碼變更有時是否會導致 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。

章節 10

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。

檢視以下主題以瞭解有關使用 Identity Manager 管理系統安全性的更多資訊。

- 安全性功能
- 限制同步運作的登入階段作業
- 密碼管理
- 通過式認證
- 配置共用資源的認證
- 配置 X509 憑證認證
- 加密使用和管理
- 管理伺服器加密
- 安全性使用方案

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 可讓您透過單一動作停用組織或個人存取權限。
- **登入階段作業限制** — 你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 7 章 「報告」，以取得有關報告功能的更多資訊。)
- *Granular* **管理權限控制** — 您可以透過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，在 Identity Manager 中授予並管理管理控制。
- **伺服器金鑰加密** — Identity Manager 可以讓您透過 [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 *[Back]* 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。但是，您可以透過變更系統配置物件中 `security.authn.singleLoginSessionPerApp` 配置屬性的值，來將同步運作階段作業限制爲每個登入應用程式一個。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。將該屬性的值變更爲 `true` 會強制每個使用者具有單一登入階段作業。

如果已強制，則使用者可以登入多個階段作業；但是，僅最後登入的階段作業保持使用中狀態並且有效。如果使用者對無效的階段作業執行動作，則會自動強制其退出階段作業，並且階段作業會終止。

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 (**[Edit User]**、**[Find User]** 或 **[Change Password]** 頁面) 變更使用者密碼
  - 在任何一個可選擇 granular 資源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在登入應用程式中定義的登入模組群組。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套用的。

Identity Manager 會評估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，則它會依次評估每個登入模組群組，直到某個限制規則成功，或是評估沒有限制規則的登入模組群組 (隨即使用該模組)。

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

在下列基於位置的登入限制規則範例中，規則會從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。

代碼範例 10-1 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

從功能表列中選取 **[Configure]**，然後選取 **[Login]** 以存取 [Login] 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)
- 組成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 [Login] 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 [Modify Login Application] 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 **[Save]**。您建立的限制會顯示在登入應用程式清單中。

停用對應用程式的存取

在 [Create Login Application] 和 [Modify Login Application] 頁面中，您可以選取 [Disable] 選項以停用登入應用程式，從而阻止使用者登入。如果使用者嘗試登入已停用的應用程式，則該介面會將其重新導向至替代頁面，以指示該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，您不能停用管理員登入。

編輯登入模組群組

登入模組群組清單顯示：

- 每一個定義的 Identity Manager 登入模組群組
- 每一個登入模組群組包含的登入模組
- 登入模組群組是否包含限制規則

在 [Login Module Groups] 頁面中，您可以建立、編輯和刪除登入模組群組。從清單中選取其中一個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。)

- **[Login success requirement]** — 選取適用於此模組的需求。選項包括：
  - **[Required]** — 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。
  - **[Requisite]** — 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。
  - **[Sufficient]** — 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。
  - **[Optional]** — 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。
- **[Login search attributes]** — (僅限 LDAP) 指定在嘗試連結 (登入) 至關聯的 LDAP 伺服器時要使用的 LDAP 使用者屬性名稱的有序清單。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)。在將 Identity Manager 配置爲傳遞至 LDAP 時，這可允許使用者透過 LDAP cn 或電子郵件位址登入 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
  ```

- **[Login correlation rule]** — 選取在將登入資訊對映至 Identity Manager 使用者時使用的登入相互關聯規則。選取的規則必須具有 LoginCorrelationRule authType。

- **[New user name rule]** — 選取在自動建立新的 Identity Manager 使用者成爲登入的一部分時使用的新使用者名稱規則。

按一下 **[Save]** 以儲存登入模組。一旦儲存之後，您可以將模組放置在登入模組群組中其他所有模組所在的位置。

警示 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 [User Login] 表單中所輸入者不相符，登入將會失敗。這些系統中有一些可能有鎖定策略，當失敗的登入嘗試超過指定次數後，便會強制鎖定帳號；對這些系統而言，即使使用者仍可透過 Identity Manager 成功登入，使用者帳號最後還是會被鎖定。

配置共用資源的認證

如果您有多個在實體或邏輯上相同的資源 (例如針對相同實體主機定義的兩個資源，或代表 NT 或 AD 網域環境中信任的網域伺服器的數個資源)，則您可以在系統配置物件中將該組資源設爲**共用資源**。

將資源設爲共用之後，您可讓使用者認證進入其中一個共用資源，但使用另一個共用資源將使用者對映至其關聯的 Identity Manager 使用者。例如，使用者可以將其資源帳號連結至他的資源 AD-1 的 Identity Manager 使用者。登入模組可能會定義使用者必須認證進入資源 AD-2。如果 AD-1 及 AD-2 皆定義爲共用資源 (在此情況下，它們是在相同的受信任網域中)，則當使用者順利認證進入 AD-2 後，Identity Manager 可以對映到相關聯的 Identity Manager 使用者，方法是在資源 AD-1 上尋找具有相同 accountId 的使用者。

用來指定此系統配置物件屬性的格式如以下範例中所示：

代碼範例 10-2 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。

先決條件

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到瀏覽器中 (或可透過智慧卡讀取器使用)，而用於登入使用者憑證的可信任憑證應匯入到 Web 應用程式伺服器的可信任憑證金鑰存放區中。

此外，必須選取所使用的用戶端憑證來進行用戶端認證。若要確認這個動作：

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

爲 X509 憑證認證配置 Identity Manager：

1. 以 [Configurator] 的身份 (或具同等權限的身份) 登入 [Administrator Interface]。
2. 選取 **[Configure]**，然後選取 **[Login]**，以顯示 [Login] 頁面。
3. 按一下 **[Manage Login Module Groups]**，以顯示 [Login Module Groups] 頁面。
4. 在清單中選取登入模組群組。
5. 在 [Assign Login Module...] 清單中，選取 [Identity Manager X509 Certificate Login Module]。Identity Manager 會顯示 [Modify Login Module] 頁面。
6. 設定登入成功需求。可接受的值如下：
   - **[Required]** — 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。
   - **[Requisite]** — 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。
   - **[Sufficient]** — 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。
   - **[Optional]** — 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 **[Save]** 返回 [Modify Login Module Group] 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 **[Save]**。
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 [Login Module Groups] 頁面上，按一下 [Return to Login Applications]，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 **[Save]**。

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 [New User Name Rule]。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。

[New User Name Rule] 可用的輸入引數與 [Login Correlation Rule] 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 中有新使用者名稱規則的範例，名爲 NewUserNameRules.xml。

建立並匯入登入配置規則

Identity Manager X509 憑證登入模組會使用登入相互關聯規則來確定如何將憑證資料對映至適當的 Identity Manager 使用者。Identity Manager 包括一個內建相互關聯規則，名爲 Correlate via X509 Certificate subjectDN。

您也可以增加您自己的關聯規則。每一個相互關聯規則必須遵守這些指導原則：

- 其 `authType` 屬性必須設定爲 `LoginCorrelationRule`。(在 `<LoginCorrelationRule>` 元素中設定 `authType='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。

傳遞至登入配置規則的引數有：

- 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

登入配置規則 (使用傳入引數) 會傳回一或多個 AttributeConditions 的清單。[Identity Manager X509 Certificate Login Module] 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 [Administrator Interface] 中選取 **[Configure]**，然後選取 **[Import Exchange File]**，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 連線到配置應用程式介面的 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

如果用戶端憑證屬性在 http 請求中的名稱不是 javaxservlet.request.X509Certificate ，您會收到一個訊息表示在 http 請求中找不到此屬性。若要更正這個問題：

1. 啓用 SessionFactory 追蹤，以查看 http 屬性的完整清單，並確定 X509 憑證的名稱。
2. 使用 Identity Manager 除錯設備來編輯 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 10-1 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. 透過系統配置物件的 pbeEncrypt 屬性或 [Manage Server Encryption] 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：

- **[Default key]** — 此金鑰已編譯爲伺服器代碼。
- **[Randomly generated key]** — 此金鑰可以在初始伺服器啓動或目前金鑰的安全性出現問題時產生。

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 前。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。

備註 請勿從儲存庫中移除由某些物件的加密資料參照的任何伺服器加密金鑰，這一點非常重要，如果移除，則伺服器將無法對資料進行解密。如果從其他儲存庫匯入包含加密資料的物件，則必須首先匯入相關的伺服器加密金鑰，以確保可以成功匯入該物件。

爲避免這些多金鑰問題以及維護更高層級的資料完整性，請使用 [Manage Server Encryption] 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。

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 [Manage Server Encryption] 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) 做爲 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，方法是使用做爲初始伺服器至閘道握手的一部分的共用秘密主金鑰對階段作業金鑰進行加密。

在初始握手時，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

- **[Default mode]** — 伺服器至閘道的初始協定握手使用編譯爲伺服器代碼的預設 168 位元 triple-DES 金鑰加密。
- **[Secure mode]** — 產生針對共用儲存庫的隨機 168 位元金鑰 triple-DES 閘道金鑰，並做爲初始握手協定的一部分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。根據系統配置中 `pbeEncrypt` 屬性的值，將使用預設金鑰或 PBE 金鑰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。

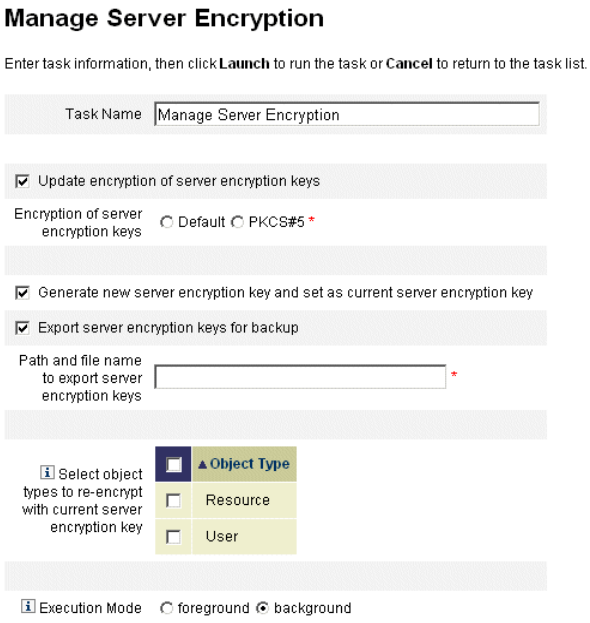
如何銷毀伺服器和閘道金鑰？

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 [Manage Server Encryption] 作業，可以從 **[Tasks]** 標籤存取該作業。

圖 10-1 [Manage Server Encryption] 作業



選取 **[Run Tasks]**，然後從清單中選取 [Manage Server Encryption]，以爲此作業配置以下資訊：

- **[Update encryption of server encryption keys]** — 選取此選項可指定是否使用預設 (3DES) 加密或 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。
- **[Generate new server encryption key and set as current server encryption key]** — 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。

- **[Select object types to re-encrypt with current server encryption key]** — 選取一或多個 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。
- **[Manage Gateway Keys]** — 選取此選項後，頁面會顯示這些閘道金鑰選項：
  - **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。
- **[Export server encryption keys for backup]** — 選取此選項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)。

- **[Execution Mode]** — 選取是在背景 (預設選項) 還是在前景中執行此作業。如果您選擇以新產生的金鑰重新加密一或多個物件類型，則此作業可能需要花費一點時間，並且最好在背景執行。

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其職務類別所需要的動作，並藉由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 應用程式中的活動。
- 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。

如果您的應用程式伺服器與 Servlet 2.2 相容，Identity Manager 安裝程序會將 http 階段作業逾時設定爲預設值 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：

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>
```

身份識別稽核

本章說明了 Identity Manager 中的功能，這些功能可讓您設定稽核控制以監視和管理企業資訊系統和應用程式中的稽核與規範遵循。

所述功能的重點在於如何執行稽核檢閱和實作實踐，以協助您維護安全性控制和管理對聯邦法規的規範遵循。

在本章中，您將瞭解以下概念與作業：

身份識別稽核的目標

身份識別稽核解決方案可透過以下方法提高稽核效能：

- **自動偵測遵循性違規，透過即時通知實現迅速補救**

  Identity Manager 稽核策略功能可讓您定義違規的**規則** (條件)。定義之後，系統便會掃描違反既定策略的動作，例如未經授權的存取變更或錯誤的存取權限。如果偵測到這類動作，系統會根據定義的層級上報鏈通知適當的人員或應用程式。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補救 (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。[Reports] 標籤還提供違規的圖形化報告。依據資源、組織或策略來檢視違規，並根據您定義的報告特性來自訂每個圖表。

- **自動化身份控制的認證檢查以降低操作風險**

  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活動並符合法規要求的完整報告**

  [Reports] 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 (PAR) 來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。然後 PAR 程序便會向指定驗證者通知要檢閱的擱置請求，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請求。

- **識別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 提供兩項不同的功能，用於稽核使用者帳號權限和存取權限以及維護和認證規範遵循，即基於策略的規範遵循和定期存取檢閱。

基於策略的規範遵循

Identity Manager 透過稽核策略系統使管理員能夠維護公司建立之所有使用者帳號需求的規範遵循。

稽核策略可用於透過以下兩種不同卻互補的方式來確保規範遵循：連續規範遵循和定期規範遵循。

在佈建作業可能在 Identity Manager 外部執行的環境中，這兩種技術更具互補性。無論何時，只要不執行現有稽核策略的程序可變更帳號，就需要定期規範遵循。

連續規範遵循

連續規範遵循表示策略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。

透過將稽核策略指定給組織和 / 或使用者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同時呼叫使用者指定的策略和組織指定的策略。

組織指定的策略是以階層方式取得的單一值策略。換言之，對於任何使用者都僅有一個有效的組織策略，該策略就是指定給最低層組織的策略。例如：

組織	直接指定的策略	有效的策略
Austin	策略 A	策略 A
銷售		策略 A
開發	策略 B	策略 B
支援		策略 B
測試	策略 C	策略 C
財務		策略 A
Houston		< 無 >

備註 在前面的範例中，直接指定的策略可以是一系列策略。

定期規範遵循

定期規範遵循表示 Identity Manager 依需要評估策略，並且將所有不相容的條件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。掃描程序會調合直接指定的策略 (使用者指定的策略和組織指定的策略) 與任意一組已選取的策略。

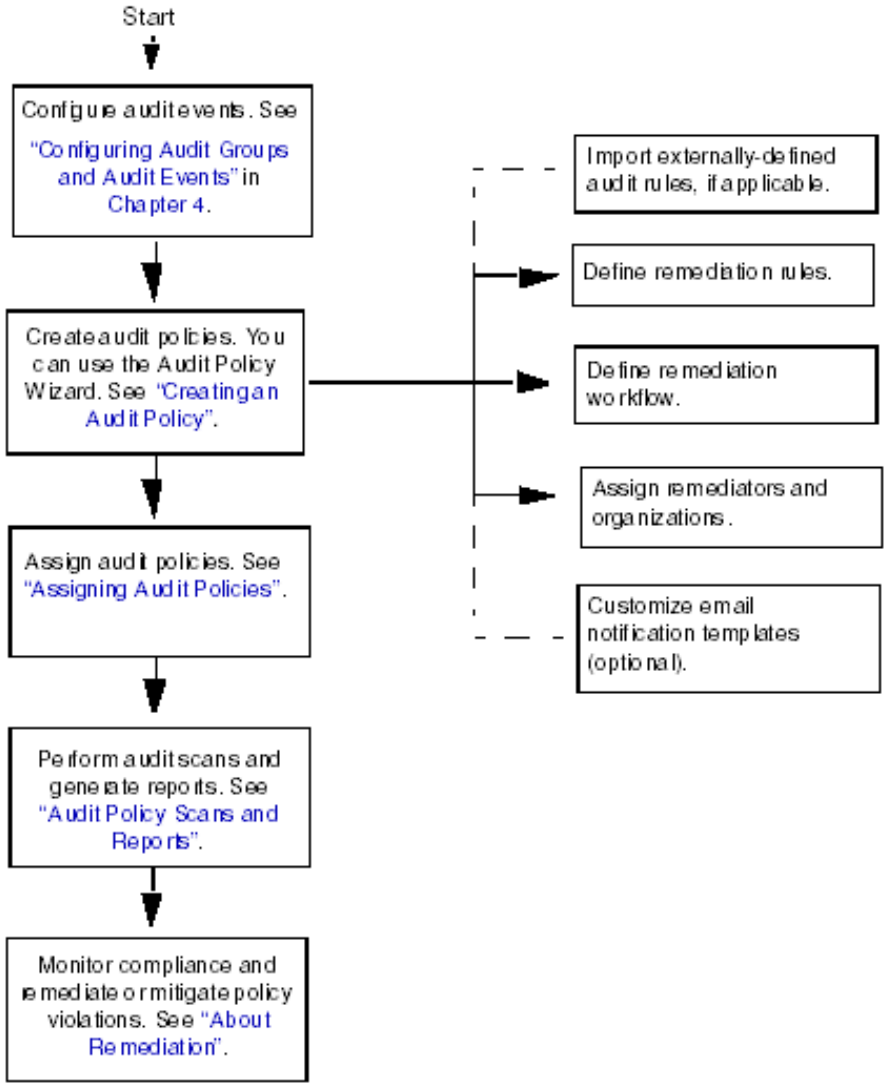
具有 Auditor 管理員權能的 Identity Manager 管理員可以建立稽核策略，並透過定期檢閱監視對這些策略的規範遵循與策略違規。可透過修正和緩解程序管理違規。如需有關 Auditor 管理員權能的更多資訊，請參閱第 152 頁的「瞭解與管理權能」。

Identity Manager 稽核允許常規的使用者掃描，並且會執行稽核策略以偵測是否與已建立的帳號限制有偏差。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，也可以是自訂的使用者定義規則。

備註 必須先爲規範遵循管理啓動並配置稽核，然後您才能執行稽核檢閱和管理規範遵循。如需相關資訊，請參閱第 328 頁的「啓用稽核」。

基於策略之規範遵循的邏輯作業流程

下圖顯示了用於完成本小節中所述稽核作業的邏輯作業流程。


Start
Configure audit events. See "Configuring Audit Groups and Audit Events" in Chapter 4.
Create audit policies. You can use the Audit Policy Wizard. See "Creating an Audit Policy".
Assign audit policies. See "Assigning Audit Policies".
Perform audit scans and generate reports. See "Audit Policy Scans and Reports".
Monitor compliance and remediate or mitigate policy violations. See "About Remediation".
Import externally-defined audit rules, if applicable.
Define remediation rules.
Define remediation workflow.
Assign remediators and organizations.
Customize email notification templates (optional).

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 356 頁的「定期存取檢閱與驗證」。

啟用稽核

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，您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 管理員可以配置稽核。

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儲存的事件，請選取功能表列中的 **[Configure]**，然後按一下 **[Audit]**。在 [Audit Configuration] 頁面中，選取 **[Compliance Management]** 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」一章中的第 134 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 12 章「稽核記錄」

介面的 [Compliance] 區域

您可以在 Identity Manager 管理員介面的 [Compliance] 區域中建立並管理稽核策略。選取功能表列中的 **[Compliance]** 以存取 [Manage Policies] 頁面，該頁面會列出您有權檢視和編輯的策略。您還可以在此區域中管理存取掃描。

管理策略

在 [Manage Policies] 頁面中，您可以使用稽核策略完成以下作業：

- 建立新的稽核策略
- 選取策略以進行檢視或編輯
- 刪除策略

「處理稽核策略」小節中將提供有關這些作業的更詳細資訊。

管理存取掃描

使用 [Compliance] 區域中的 [Manage Access Scans] 標籤可定義、修改和執行存取檢閱掃描。您可以使用此區域定義要執行或要排定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 356 頁的 「定期存取檢閱與驗證」。

存取檢閱

[Compliance] 區域中的 [Access Review] 標籤可讓您存取可協助您監視存取檢閱進度的資訊。其將顯示包含資訊連結 (在網路型介面中可用) 的掃描結果摘要報告，這些資訊連結可讓您存取有關檢閱狀態和擱置作業的更詳細資訊。

如需有關此功能的更多資訊，請參閱第 363 頁的 「管理存取檢閱」。

關於稽核策略

稽核策略是針對一個或多個資源之一組使用者的帳號限制的定義。其包括定義策略限制的**規則**，以及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來評估您的組織中是否發生違規狀況。

稽核策略包含以下元件：

- **[Policy rules]**，可包含以 XPRESS、XML Object 或 JavaScript 語言撰寫之定義特定違規的函數。
- **[Remediation workflow]**，當稽核掃描識別出策略規則違規時，便會選擇性地將其啓動。
- **補救者**，即授權要回應策略違規的指定管理員。修正者可以是個別使用者或使用者群組。
- **組織指定**，定義可使用此策略的組織
- **[User assignments]**，定義應套用此策略的使用者。

稽核策略規則

在稽核策略中，規則會根據屬性來定義可能的衝突。Auditor 規則中的變數受限於與使用者相關聯的特定資源的屬性。稽核策略可能包含參照廣泛資源的上百個規則。

引數可以傳遞至規則以控制其行爲，而規則可以參照和修改表單或補救工作流程所維護的變數。

規則必須包含 SUBTYPE_AUDIT_POLICY_RULE 類型定義。系統會自動爲透過稽核策略精靈產生或從中參照的規則指定此類型。

```
Rule subtype='SUBTYPE_AUDIT_POLICY_RULE'
```

請參閱「Identity Manager Deployment Tools」中的「**使用規則**」，以取得有關規則邏輯的討論。

修正工作流程

建立定義策略違規的規則後，您要選取當稽核掃描偵測到違規時，將啓動的工作流程。Identity Manager 提供預設的「標準補救」工作流程，爲「稽核策略」掃描提供預設的補救處理程序。除了其他動作之外，這個預設補救工作流程還會產生通知電子郵件給每個指定的第 1 級補救者 (必要時也會寄給其他層級的補救者)。

備註 修正工作流程與 Identity Manager 工作流程程序不同，必須爲修正工作流程指定 AuthType=AuditorAdminTask and the SUBTYPE_REMEDIATION_WORKFLOW 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 *332* 頁的「(可選擇) 將工作流程匯入 *Identity Manager*」以取得更多資訊。

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授權修正者。如需有關修正的附加資訊，請參閱本章中的「修正與緩解」。

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

您負責應付帳款及應收帳款，並且必須實作某些程序來預防責任集中在會計部門員工身上的潛在風險。這個策略會執行四個規則來檢查應付帳款的負責人員並未同時又負責應收帳款。

- 四個規則集，每個規則分別都指定一個構成策略違規的條件
- 啓動補救工作的相關聯的工作流程

- 指定的管理員或修正者群組，他們有權檢視和回應前述規則指定的策略違規

當規則辨別出策略違規 (也就是使用者擁有太多職權) 之後，相關聯的工作流程可以啓動特定的補救相關工作，包括自動通知選定補救者。

第 1 級補救者是當稽核掃描辨別出策略違規時，所要聯絡的第一批補救者。如果爲稽核策略指定了多個層級，則當超過此區域中識別的提升期間時，Identity Manager 會通知下一層級中識別的修正者。

組織和補救工作流程區域

顯示目前和可能擁有這個策略的存取權限的組織。

此區域也會列出與稽核策略相關聯的補救工作流程「標準補救」工作流程會分別爲每個第 1 級補救者產生工作項目和電子郵件通知。當第一位補救者對違規的工作項目採取行動時，此作業便得以繼續進行。如果在策略指定的逾時限制內沒有任何修正者採取動作，則 Identity Manager 會將違規提升至策略中的下一個修正層級 (取得新的修正者集與逾時)。

處理稽核策略

Identity Manager 提供稽核策略精靈，可協助您輕鬆設定稽核策略。定義稽核策略後，您可以對該策略執行各種動作，例如修改或刪除該策略。本小節中的主題說明了如何建立與管理稽核策略和稽核策略規則。

建立稽核策略

「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，請在介面的 **[Compliance]** 區域中按一下 **[Manage Policies]**，並建立新的稽核策略。

使用此精靈時，您將執行以下作業來建立稽核策略：

- 選取或建立您要用來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 **[Next]** 移至下一個步驟。

開始之前

建立稽核策略之前需要大量規劃，包括以下作業：

- 識別您在稽核策略精靈中建立策略時要使用的規則。這些規則由您正在建立的策略類型以及您要定義的特定限制決定。
- 匯入您要在新策略中包含的所有補救工作流程或規則。
- 請確保您具有建立稽核策略所需的管理員權能。請參閱第 152 頁的「瞭解與管理權能」中的必要權能。

辨別您需要的規則

您在策略中指定的限制將在您建立或匯入的規則集中實作。使用稽核策略精靈建立規則時，您將：

1. 識別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。

(可選擇 *)* 將責任分離規則匯入 *Identity Manager*

稽核策略精靈無法建立責任分離規則。必須在 Identity Manager 外部建構這些規則，並使用 [Configure] 標籤中的 [Import Exchange File] 選項將其匯入。

(可選擇 *)* 將工作流程匯入 *Identity Manager*

若要使用 Identity Manager 目前未提供的修正工作流程，請完成以下作業以匯入外部工作流程：

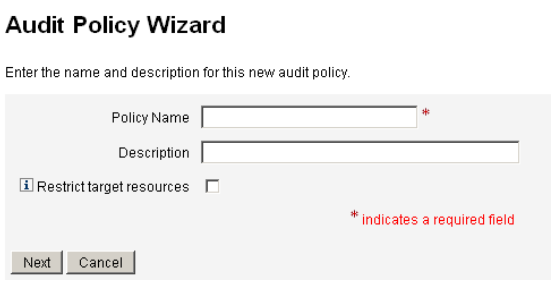
1. 設定 `authType='AuditorAdminTask' and add subtype='SUBTYPE_REMEDIATION_WORKFLOW'`。您可以選擇使用 Identity Manager IDE 或 XML 編輯器來設定這些配置物件。
2. 使用「匯入交換檔案」選項來匯入工作流程。(您可以從「配置」標籤存取這項功能)。

成功匯入工作流程後，其便會顯示在 [Audit Policy Wizard] 中的 [Remediation Workflow] 選項清單中。

命名和說明稽核策略

在 [Audit Policy Wizard] 螢幕 (如圖 11-1 所示) 中輸入新策略的名稱及其簡要描述。

圖 11-1 稽核策略精靈：輸入名稱與描述螢幕



如果選擇不命名規則，Identity Manager 會使用下列格式來指定預設名稱：`Policy_Name::Rule1`。

如果您希望在執行掃描時僅存取已選取的資源，請啓用 **[Restrict target resources]** 選項。

備註 如果稽核策略不限制資源，則掃描期間將存取使用者具有帳戶的所有資源。如果規則僅使用一些資源，則將策略限制爲僅這些資源會更加有效。

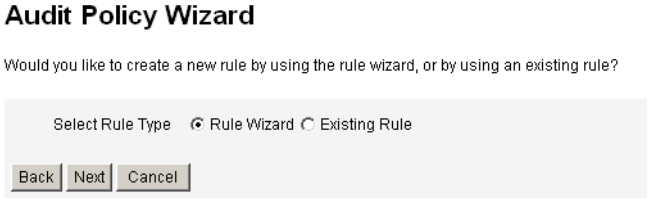
按 **[Next]** 繼續下一頁。

選取規則

使用這個螢幕來啓動在策略中定義或包含規則的程序。建立策略時，您的工作主要就是定義和建立規則。

如圖 11-2 所示，您可以選擇使用 Identity Manager 規則精靈建立自己的規則，或結合現有規則。依預設會選取 [Rule Wizard] 選項。按 **[Next]** 啓動規則精靈，然後移至第 336 頁的「使用規則精靈建立新規則」以取得有關建立規則的說明。

圖 11-2 稽核策略精靈：選取規則類型螢幕



選取現有規則

選取規則選項後，按一下 **[Existing Rule]** 以將現有規則包含在新策略中。然後，按 **[Next]** 以檢視並選取您可以存取的現有稽核策略規則。

從 [Rules] 選項清單中選取其他規則，然後按 **[Next]**。

備註 如果看不到之前匯入 Identity Manager 的規則名稱，請確認您已將 第 329 頁的「稽核策略規則」中所述的附加屬性增加至規則中。

增加規則

您可以建立其他規則，也可以匯入現有規則。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。

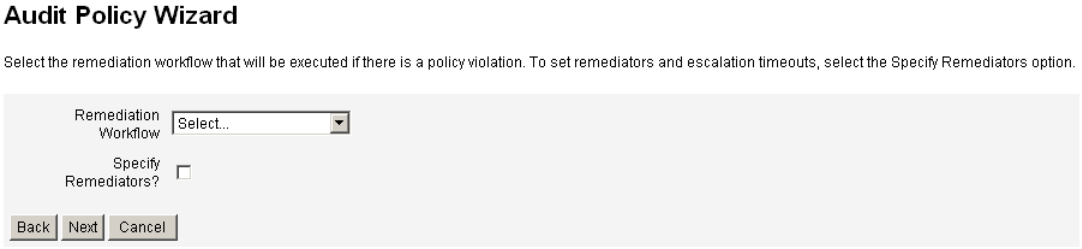
如有必要，請按一下 **[AND]** 或 **[OR]** 以繼續增加規則。若要移除某規則，請選取該規則，然後按一下 **[Remove]**。

僅當**所有**規則的布林表示式均評估爲 true 時，才會發生策略違規。使用 AND/OR 運算子對規則進行分組後，即使所有規則均未評估爲 true，策略也可能評估爲 true。Identity Manager 僅針對評估爲 true 的規則建立違規 (僅當策略表示式評估爲 true 時)。

選取補救工作流程

使用這個螢幕來選取要與此策略相關聯的「補救」工作流程。此處指定的工作流程可決定在偵測到稽核策略違規時，要在 Identity Manager 內採取的行動。

圖 11-3 稽核策略精靈：選取修正工作流程螢幕



備註 如需有關匯入您已在 XML 編輯器或 Identity Manager 整合開發環境 (IDE) 中建立之工作流程的資訊，請參閱第 332 頁的「(可選擇) 將工作流程匯入 Identity Manager」。

若要指定要與此修正工作流程相關聯的修正者，請按一下 **[Specify Remediators?]** 啓用此核取方塊後按 **[Next]**，將顯示 [Assign Remediators] 頁面。如果未啓用此核取方塊，則 [Audit Policy Wizard] 會接著顯示 [Assign Organizations] 螢幕。

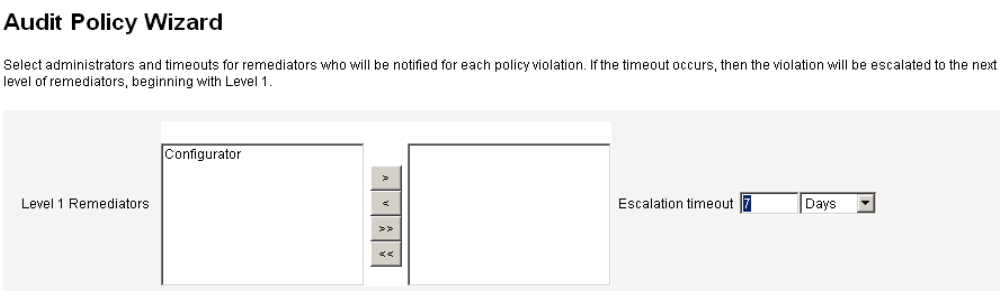
為補救選取管理員和逾時

如果您選取指定修正者，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。

您可以選擇指定至少一個第 1 級修正者，或指定的管理員。偵測到策略違規時，補救工作流程首先會使用電子郵件來聯絡第 1 級補救者。如果已達到指定的提升逾時期間而第 1 級修正者尚未回應，則 Identity Manager 接著會連絡您在此處指定的第 2 級修正者。僅當第 1 級或第 2 級修正者在提升時間段結束之前均無回應時，Identity Manager 才會連絡第 3 級修正者。

[Assigning Remediators] 是可選選項。如果您選取此選項，請按 **[Next]** 以在指定設定後繼續至下一個螢幕。

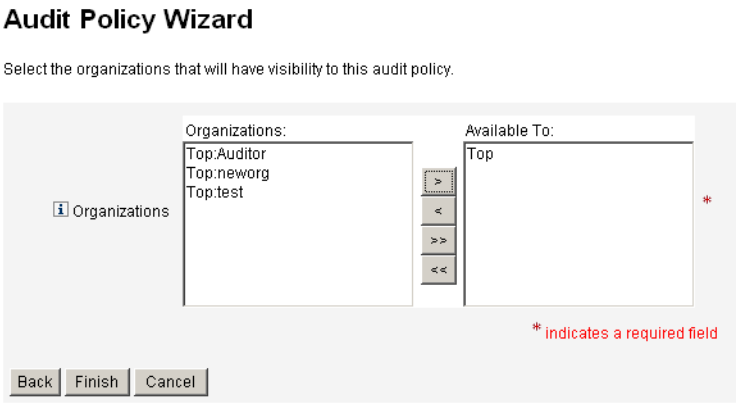
圖 11-4 稽核策略精靈：選取第 1 級修正者區域



選取可以存取此策略的組織

使用圖 11-5 所示螢幕，可選取可以檢視和編輯此策略的組織。

圖 11-5 稽核策略精靈：指定組織可視性螢幕



當您建立策略之後，策略便會列在可以從 [Compliance] 標籤存取的策略檢視中。

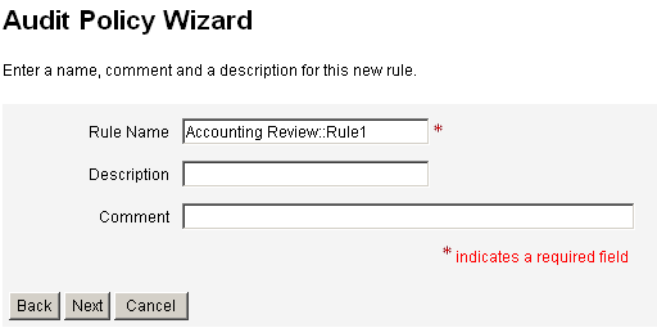
使用規則精靈建立新規則

如果您選擇使用 [Audit Policy Wizard] 中的 [Rule Wizard] 選項建立規則，請接著在下面各部分中所述的螢幕中輸入資訊。

命名和說明新規則

(可選擇) 使用此螢幕可輸入描述性文字，每次 Identity Manager 顯示規則時，描述性文字都會顯示在規則名稱旁邊。請輸入簡潔易懂且能夠描述規則的描述。這段說明會顯示在 Identity Manager 內的 [Review Policy Violations] 頁面中。

圖 11-6 稽核策略精靈：輸入規則描述螢幕



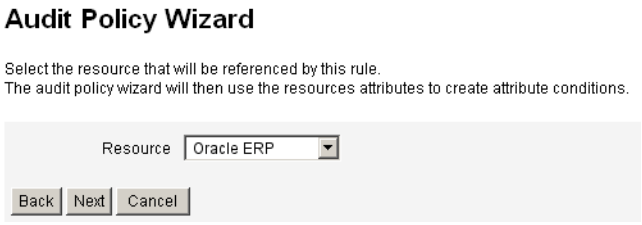
例如，如果您建立的規則可識別同時具有 Oracle ERP responsibilityKey 屬性值 `Payable User` 與 `Receivable User` 屬性值的使用者，則可以在 [Description] 欄位中輸入以下文字：**識別同時具有 `Payable User` 和 `Receivable User` 責任的使用者**。

使用 [Comments] 欄位可提供有關規則的附加資訊。

選取規則參照的資源

使用這個螢幕來選取規則將參照的資源。每個規則變數都必須對應到這個資源的屬性。您具有檢視存取權限的所有資源都會顯示在這個選項清單中。在此範例中，已選取 Oracle ERP。

圖 11-7 稽核策略精靈：選取資源螢幕



備註 支援每個可用資源適配器的大多數 (但不是全部) 的屬性。如需有關可用的特定屬性的資訊，請參閱「Identity Manager Resources Reference」。

按 **[Next]** 移至下一頁。

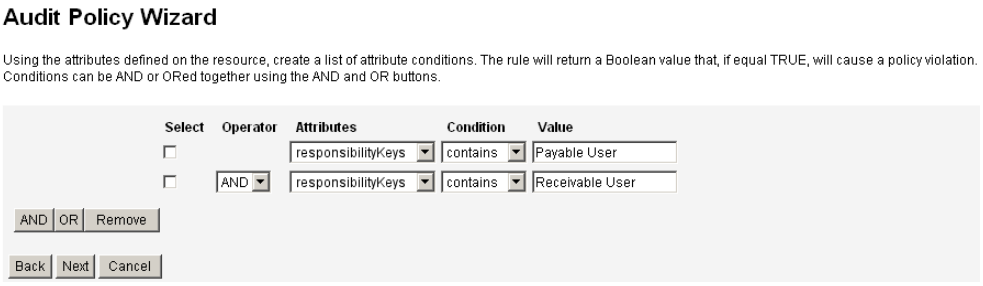
建立規則表示式

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。這個屬性會直接對應到規則變數。
2. 從清單中選取邏輯條件。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)、true、null、not null、以及 contains。針對此範例的目的，您可以從可能的屬性條件清單中選取 `Contains`。
3. 輸入表示式的值。例如，如果輸入 `Payable user`，則您在指定具有 responsibilityKeys 屬性值 `Payable user` 的 Oracle ERP 使用者。

4. （可選擇）按一下 **[AND]** 或 **[OR]** 運算子以增加另一行並建立其他表示式。

圖 11-8 稽核策略精靈：選取規則表示式螢幕



此規則會傳回布林值。如果兩個陳述式都爲 true，那麼規則會傳回 TRUE 值，進而引發策略違規。

備註 .Identity Manager 不支援規則套疊控制。如果指定了多個規則，則策略評估器永遠先執行 AND 作業，然後再執行 OR 作業。例如，R1 AND R2 AND R3 or R4 AND R5 (R1 + R2 + R3) | (R4 + R5)。

以下程式碼範例顯示了您已在此螢幕中建立之規則的 XML：

代碼範例 11-1 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 **[Remove]**。

按 **[Next]** 以繼續執行 [Audit Policy Wizard]。接著，藉由使用精靈來建立新規則或新增現有規則，您將有機會新增其他規則。

編輯稽核策略

稽核策略的常見編輯工作包括：

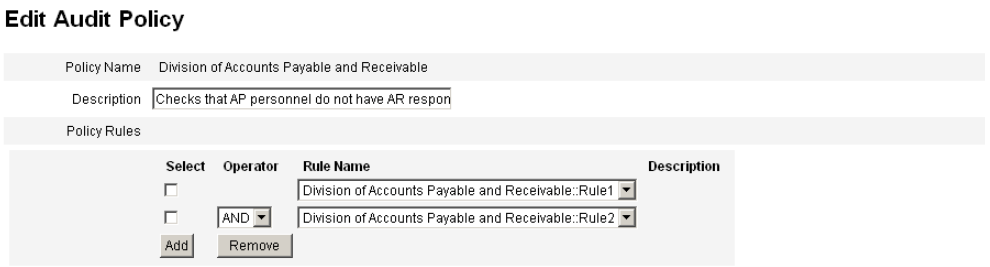
- 新增或刪除規則
- 調整具有此策略存取權限的組織清單
- 變更與各個補救層級相關聯的上報逾時
- 變更與此策略相關聯的補救工作流程

編輯策略頁面

在 [Audit Policy] 名稱欄中按一下策略名稱，即可開啓 [Edit Audit Policy] 頁面。[Edit Audit Policy] 頁面隨即開啓。此頁面將稽核策略資訊分類成以下區域：

- 識別與規則區域
- 補救者與上報逾時區域
- 工作流程與組織區域

圖 11-9 [Edit Audit Policy] 頁面：識別與規則區域



使用這個頁面區域可以：

- 編輯策略名稱和說明

- 新增或刪除規則

備註	您無法使用此產品來直接編輯現有的規則。請使用 Identity Manager IDE 或 XML 編輯器來編輯規則，然後將其匯入 Identity Manager。然後您可以移除舊版本，並加入新修改的版本。

編輯稽核策略名稱和說明

藉由選取欄位中的文字並輸入新文字，可以編輯 [Policy Description] 欄位和 [Rule Name] 欄位。

從策略中刪除規則

按一下規則名稱前面的 **[Select]** 按鈕，然後按一下 **[Remove]**。

新增規則到策略

按一下 **[Add]** 來附加您可以用來選取新增規則的新欄位。

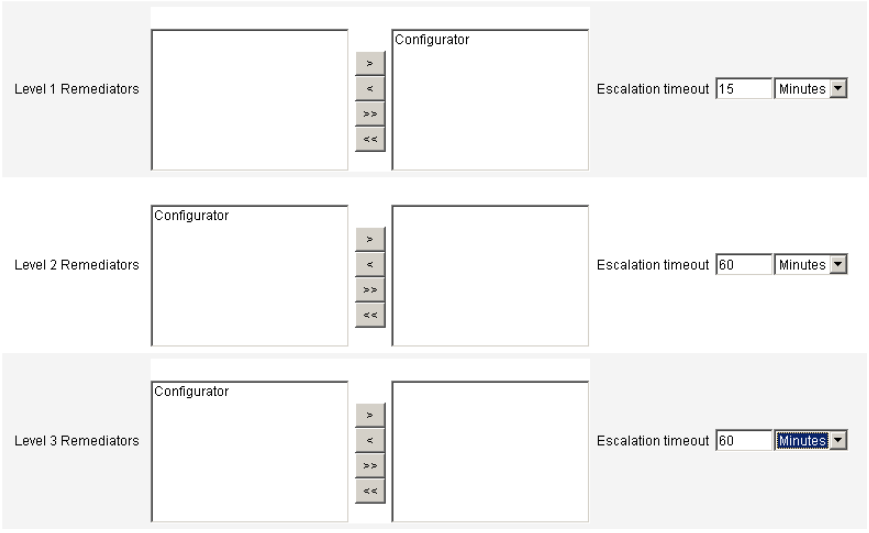
變更策略使用的規則

在 [Rule Name] 欄中，從選項清單中選取其他規則。

修正者區域

圖 11-10 顯示了用於爲策略指定修正者的修正者區域。

圖 11-10 [Edit Audit Policy] 頁面：指定修正者



使用這個頁面區域可以：

- 移除或指定策略的修正者。
- 調整提升逾時。

移除或指定補救者

透過選取名稱並使用 > 將每個修正層級之左側欄中的選項移至右側欄，來爲一個或多個修正層級選取修正者。您必須至少選取一個修正者。

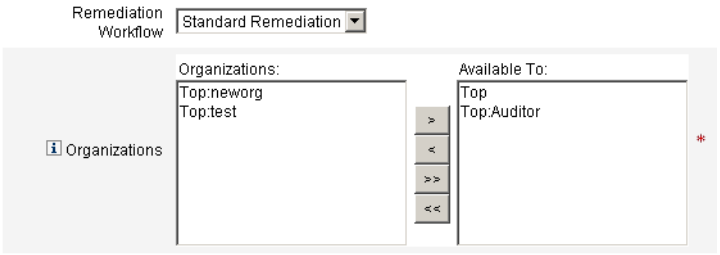
調整上報逾時

選取逾時值然後輸入新值。預設的逾時值爲 60 分鐘。

修正工作流程與組織區域

圖 11-11 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 11-11 [Edit Audit Policy] 頁面：修正工作流程與組織



使用這個頁面區域可以：

- 變更發生策略違規時啓動的修正工作流程。
- 調整可以存取此策略的組織。

變更補救工作流程

若要變更指定給策略的工作流程，您可以從選項清單中選取替代工作流程。依預設，不爲稽核策略指定任何工作流程。

備註 如果沒有為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。

從清單中選取補救工作流程，然後按一下 **[Save]**。

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**。

刪除稽核策略

從系統刪除稽核策略後，所有參照該策略的違規也將被刪除。

按一下 [Manage Policies] 以檢視策略後，可從介面的 [Compliance] 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 **[Delete]**。

對稽核策略進行疑難排解

使用策略規則除錯程式通常是解決稽核策略問題的最佳辦法。

對規則進行除錯

若要對規則除錯，請將下列追蹤元素新增到規則程式碼中。

```
<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。

請確認已將 `subtype='SUBTYPE_REMEDIATION_WORKFLOW'` 屬性增加到您的工作流程中。如果沒有這個子類型，便無法在 Identity Manager 介面中看到工作流程。

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這兩項權能。

若要指定組織層級策略，請在 [Accounts] 標籤中選取 [Organization]，然後從 [Assigned audit policies] 清單中選取策略。

如要指定使用者層級策略，請按一下 [Accounts] 標籤中的 [User]。然後，在使用者表單中選擇 [Compliance] 標籤，並從 [Assigned audit policies] 清單中選取策略。

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

掃描是對個別使用者或組織執行選定稽核策略的方法。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。您可以從介面的 **[Accounts]** 區域啓動掃描。

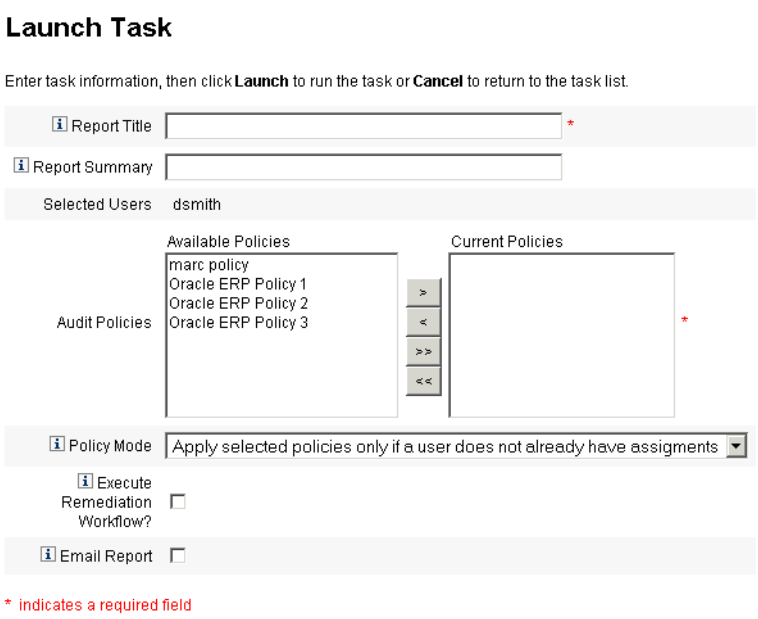
您也可以從 [Server Tasks] 標籤啓動稽核策略掃描。

若要從 [Accounts] 區域啓動對使用者帳號或組織的掃描，請：

1. 按一下 **[Accounts]** 標籤。
2. 在 [Accounts] 清單中，執行以下任一作業：
   a. 選取一個或多個使用者，然後從 [User Actions] 選項清單中選取 **[Scan]**。
   b. 選取一個或多個組織，然後從 [Organization Actions] 選項清單中選取 **[Scan]**。

   螢幕上將顯示 [Launch Task] 對話方塊。表 11-2 是稽核策略使用者掃描的 [Launch Task] 頁面範例。

圖 11-12 [Launch Task] 對話方塊



3. 在 [Report Title] 欄位中指定掃描的標題。這是必填欄位。您可以選擇是否要在 [Report Summary] 欄位中指定掃描的說明。
4. 選取一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 **[Policy Mode]**。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. 核取 **[Execute Remediation Workflow?]** 來執行稽核策略中指定的補救工作流程。如果稽核策略並未定義補救工作流程，此時便不會執行補救。
7. 核取 **[Email Report]** 來指定報告的收件人。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。
8. 如果您想要置換預設 PDF 選項，請啓用 **[Override default PDF options]** 核取方塊。
9. 按一下 **[Launch]** 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 11-1 Auditor 報告說明

Auditor 報告類型	說明
存取檢閱詳細資訊報告	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篩選此報告。
存取檢閱摘要報告	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。
稽核策略摘要報告	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。
已稽核的屬性報告	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 或標示為可稽核的資源屬性來指定它們。
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。您可依策略篩選此報告，並且可按天、週、月或季對其進行分組。
使用者存取報告	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。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。
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。
責任分離報告	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附加資訊。 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。
違規摘要報告	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 [Reports] 標籤中取得這些報告。

建立 Auditor 報告

若要產生報告，您必須首先建立報告。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。建立並儲存報告後，其將顯示在 [Run Reports] 頁面中。

圖 11-13 顯示了包含已定義之 Auditor 報告清單的 [Run Reports] 頁面範例。

圖 11-13 執行報告頁面選擇

若要建立 Auditor 報告，請執行以下程序：

1. 從功能表列中，選取 **[Reports]**。
2. 選取 **[Auditor Reports]** 報告類型，然後在 **[New]** 報告清單中選取以下任一報告選項：
   - 存取檢閱詳細資訊報告
   - 存取檢閱摘要報告
   - 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

將會顯示報告對話方塊。報告對話方塊的欄位與版面配置會因各種報告類型而異。請參閱線上說明，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 **[Run]** 以開始執行報告。Identity Manager 不會儲存報告 (如果您定義了新報告) 或變更的報告條件 (如果您編輯了現有報告)。
- 儲存報告 — 按一下 **[Save]** 以儲存報告。儲存報告後，您可以從 [Run Reports] 頁面 (報告清單) 執行此報告。

從 [Run Reports] 頁面執行報告後，您可以立即或稍後從 [View Reports] 標籤中檢視輸出。

- 如需有關排定報告的資訊，請參閱第 208 頁的「排定報告」。

修正與緩解

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
- 修正電子郵件範本
- 指定修正權能
- 使用 [Remediations] 頁面
- 檢視修正請求
- 緩解策略違規
- 補救策略違規
- 轉寄補救請求

關於修正

當 Identity Manager 偵測到未解決 (未緩解) 的稽核策略違規時，其會建立修正請求，此修正請求必須由**修正者** (可以評估和回應稽核策略違規的指定管理員) 加以解決。

Identity Manager 可讓您定義三個層級的補救者上報。補救請求最初會傳送給第 1 級補救者。如果第 1 級補救者在逾時期限到期前沒有對補救請求採取任何行動，Identity Manager 會將違規上報至第 2 級補救者，並開始新的逾時期限。如果第 2 級補救者在逾時期限到期前並未回應，則該請求會再次上報至第 3 級補救者。

若要執行補救，您必須在企業中至少指定一位補救者。您可以選擇是否要爲每個層級指定多位補救者，但是建議您最好這麼做。多位補救者將有助於確保工作流程不會延誤或停滯。

第 351 頁的「指定修正權能」提供指定補救者的指示。

修正工作流程程序

依預設，Identity Manager 實作標準修正工作流程，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第 1 級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。當稽核策略評估爲 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，且違規處於緩解狀態，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 329 頁的「關於稽核策略」。

補救回應

依照預設，會爲每位補救者提供三個回應選項：

- **已補救**：補救者指示已採取行動來修復資源的問題。

  修改過遵循性違規後，Identity Manager 會建立稽核事件來記錄補救。此外，Identity Manager 還會儲存補救者名稱和該人員提供的所有註釋。

備註 直到執行下一個稽核掃描才會刪除違規。

- **[Mitigate]**：補救者可允許違規，並於特定期間內授予使用者違規免責。

  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 會儲存緩解違規的補救者名稱，並儲存指定給免責的過期日期以及該人員提供的所有註釋。

備註	當 Identity Manager 偵測到過期的免責時，它會將緩解違規恢復成擱置違規。

- **[Forward]**：補救者重新指定解決違規的責任給另一位人員。

  請從以下轉寄選項中進行選取：

  - **[Peer]** — 具有修正者權能的使用者 (預設)
  - **[Controlled]** — 您控制之具有修正者權能的使用者
  - **[All]** — 所有具有修正者權能的使用者

例如，您的企業建立一條規則，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 管理員來補救衝突，然後在該資源的問題解決後，緩解違規。

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 **[Configuration]** 標籤，然後選取 **[Email Templates]** 子標籤)。您可以將此範本配置爲向補救者通知擱置違規。如需更多資訊，請參閱第 130 頁的「自訂電子郵件範本」。

指定修正權能

若要爲您企業中的管理員指定修正權能，請執行以下步驟：

1. 選取 **[Accounts]** 標籤，然後按一下 [Accounts] 清單中的管理帳號以開啓 [Edit User] 頁面。
2. 在 [Edit User] 頁面中，按一下 **[Security]** 子標籤。
3. 從 [Available Capabilities] 清單中選取 **[Auditor Remediator]**，並使用 > 按鈕將其移至 [Assigned Capabilities] 清單中。
4. 完成後按一下 **[Save]**。

備註 如需有關 Auditor 修正者權能的更多資訊，請參閱第 152 頁的 「瞭解與管理權能」。

使用 [Remediations] 頁面

選取工作項目，然後選取 Identity Manager 中的 **[Remediations]** 標籤，以存取 [Remediations] 頁面。

您可使用此頁面執行以下作業：

- 檢視所有擱置中與已完成的補救請求
- 緩解一或多項補救請求
- 補救一或多項補救請求
- 轉寄一或多項補救請求

檢視修正請求

採取行動之前，您可以先使用 [Remediations] 頁面來檢視有關補救請求的詳細資訊。

備註 視您的權能而定，您可能可以檢視其他補救者或管理員的補救請求並對其採取行動。

以下主題與檢視修正請求有關

- 第 352 頁的 「檢視擱置請求」

檢視擱置請求

依照預設，您的登入名稱和擱置請求會顯示在 [Remediations] 表格中。

您可以使用 **[List Remediations for]** 選項來檢視其他修正者的擱置修正請求：

- 選取另一修正者的登入名稱可檢視其擱置請求。
- 選取 **[All Remediators]** 可檢視所有擱置請求。

產生的表格會提供以下有關各個請求的資訊：

- **補救者**：指定的補救者名稱。

備註 當您檢視自己的補救請求時，並不會顯示 [Remediator] 欄。

- **請求**：補救者請求的動作。按一下請求內文可檢視更多有關策略違規的詳細資訊，並可以處理請求。
- **請求日期**：發出補救請求的日期與時間。
- **說明**：策略違規的簡短說明。

檢視已完成的請求

若要檢視已完成的修正請求，請按一下 **[My Work Items]** 標籤，然後按一下 **[History]** 標籤。螢幕上將顯示先前修正的工作項目清單。

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：

- **[Timestamp]**：補救請求的日期與時間
- **[Subject]**：處理請求的補救者名稱
- **[Action]**：補救者是否已緩解或補救 請求
- **[Type]**：永遠指示 `ComplianceViolation`
- **[Object Name]**：所違反的稽核策略名稱
- **[Resource]**：提供修正者的帳號 ID (或者可能指示 N/A)
- **[ID]**：永遠指示 `N/A`

- **[Result]**：永遠指示 Success

按一下表格中的時間戳記可開啓 [Audit Events Details] 頁面。

[Audit Events Details] 頁面提供已完成請求的相關資訊，包括關於補救或緩解、事件參數
(如果有的話) 以及可稽核屬性的資訊。

按一下 **[OK]** 可返回 [Previously remediated by Configurator] 頁面，在此頁面上按一下 **[OK]** 可返回 [Remediations] 頁面。

對 [Remediations] 表中的請求進行排序

您可以按一下表格標題來排序 [Remediations] 表格的內容。按一下可依向上順序排序，再按一下即可依向下順序排序。

若要對 [Remediations] 標籤中的擱置請求進行排序，請：

- 按一下 [Remediator] 依補救者名稱的字母順序來排序表格。
- 按一下 [Request] 依請求名稱的字母順序來排序表格。
- 按一下 [Date of Request] 依時間與日期的先後順序來排序表格。
- 按一下 [Description] 依請求說明的字母順序來排序表格。

若要對 [History] 標籤中的已完成請求進行排序，請：

- 按一下 [Timestamp] 依時間與日期的先後順序來排序表格。
- 按一下 [Subject] 依處理請求的補救者名稱的字母順序來排序表格。
- 按一下 [Action] 依動作的字母順序來排序表格。
- 按一下 [Object Name] 依違反的策略名稱的字母順序來排序表格。

備註 [Type]、[Resource]、[ID] 和 [Result] 欄永遠會顯示相同值，因此沒有排序這些欄的值。

更新表格

若要更新 [Remediations] 表中提供的資訊，請按一下 **[Refresh]**。[Remediation] 頁面會使用新的策略違規來更新該表。

緩解策略違規

您可以從 [Remediations] 頁面或 [Review Policy Violations] 頁面緩解策略違規。

從 [Remediations] 頁面

若要從 [Remediations] 頁面緩解擱置策略違規，請：

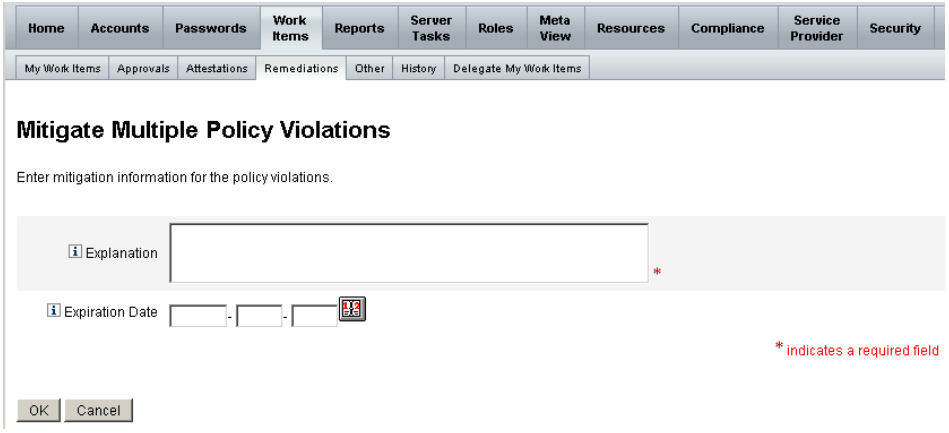
1. 在表格中選取列以指定要緩解的請求。
   - 啓用一個或多個個別核取方塊，以指定要緩解的請求。
   - 啓用表格標頭中的核取方塊，以緩解表格中列出的所有請求。

備註 請注意，Identity Manager 只允許您輸入一組註釋來說明緩解動作。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緩解。

2. 按一下 **[Mitigate]**。

   [Mitigate Policy Violation] 頁面 (或 [Mitigate Multiple Policy Violations] 頁面) 顯示如下：

圖 11-14 [Mitigate Policy Violation] 頁面



3. 在 [Explanation] 欄位中輸入您有關緩解的註釋。(這是**必填**欄位。)

   請記住，您的註釋可爲這個動作提供稽核線索，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. 直接在 [Expiration Date] 欄位中輸入日期 (**YYYY-MM-DD**)，或按一下日期 按鈕並從行事曆中選取日期，這兩種方法都可以指定免責的過期日期。

備註	若未提供日期，免責就會無限期有效。

5. 完成時按一下 **[OK]** 來儲存您的變更，並返回 [Remediations] 頁面。

補救策略違規

若要補救一或多項策略違規，請：

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補救。

2. 按一下 **[Remediated]**。
3. 螢幕上將顯示 [Remediate Policy Violation] 頁面 (或 [Remediate Multiple Policy Violations] 頁面)。
4. 在 [Comments] 欄位中輸入您有關補救的註釋。

   請記住，您的註釋可爲這個動作提供稽核線索，因此請務必輸入完整、有用的資訊。例如，說明您要補救策略違規的原因或者日期。

5. 完成時按一下 **[OK]** 來儲存您的變更，並返回 [Remediations] 頁面。

轉寄補救請求

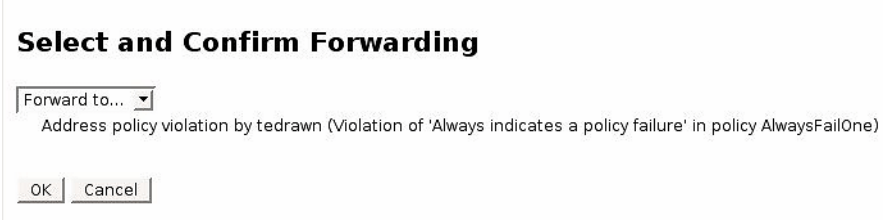
必要時，您可以轉寄一或多個補救請求給另一位補救者，如下所示：

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 **[Forward]**。
3. 螢幕上將顯示 [Select and Confirm Forwarding] 頁面。

圖 11-15 [Select and Confirm Forwarding] 頁面



4. 從 [Forward to] 選項清單中選取另一位修正者的名稱，然後按一下 **[OK]**。

再次顯示 [Remediations] 頁面時，新修正者的名稱將顯示在表格的 [Remediator] 欄中。

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。此程序有助於持續識別與管理使用者權限積累，還有助於維護對 Sarbanes-Oxley、HIPAA 與其他聯邦命令的規範遵循。

可臨時執行存取檢閱或將其排定爲定期進行 (例如每個行事曆季度一次)，從而使您可以執行定期存取檢閱來維護使用者權限的正確層級。存取檢閱可包括稽核掃描。

關於定期存取檢閱

定期存取檢閱是用於驗證一組員工在特定時間對相應資源是否具有相應權限的定期程序。

定期存取檢閱涉及以下作業：

- 存取檢閱掃描 — 您定義與執行 (或排定執行) 的掃描，該掃描可評估指定使用者集的**使用者軟體權利文件**，並執行基於規則的評估以確定是否需要驗證。
- 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指示使用者帳號或特定資源集之詳細資訊的記錄。

存取檢閱掃描

若要啓動定期存取檢閱，您必須首先至少定義一個**存取掃描**。

存取掃描可定義要掃描的對象、掃描要包括的資源、掃描期間要評估的所有稽核策略，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

通常，Identity Manager 存取檢閱程序按如下步驟工作：

- 建構使用者清單、取得每個使用者的帳號資訊並評估稽核策略
- 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首次拒絕
- 如果在指定逾時期間內未收到任何對請求的回應，則提升至下一個驗證者
- 使用解決方案更新使用者軟體權利文件記錄

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，使用者必須具有 Auditor 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。如需有關這些和其他 Auditor 權能的更多資訊，請參閱第 152 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。該工作流程根據存取掃描中定義的規則做出此決定。

存取掃描評估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，每個驗證者負責一項工作項目。可使用 ScanNotification 工作流程傳送給這些工作項目之驗證者的通知，該工作流程針對每個掃描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

已授權以下 Identity Manager 使用者存取驗證工作項目：

- 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

這些授權選項適用於 `authType` AttestationWorkItem 的工作項目。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」；
- `firstLevel` — 要包括在結果中的第一個從屬層級；0 表示直接報告
- `lastLevel` — 要包括在結果中的最後一個從屬層級；-1 表示所有層級

`firstLevel` 和 `lastLevel` 的整數值預設爲 0 和 -1，表示直接和間接從屬。

可透過以下方法增加或修改這些選項：

```
UserForm:AccessApprovalList approval/editAttestation.jsp
```

委託驗證

依預設，存取掃描工作流程讓使用者建立的驗證工作項目和通知委託優先。存取掃描管理員可取消選取 [Follow Delegation] 選項來忽略委託設定。如果驗證者已將所有工作項目委託給其他使用者，但是沒有爲存取檢閱掃描設定 [Follow Delegation] 選項，則該委託所指定給的驗證者 (而非使用者) 將接收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化該程序的許多部分，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要考慮以下注意事項：

- 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。

  一個大規模組織執行單一定期存取檢閱時，掃描可能要花費一天或幾天的時間，而完成手動驗證可能也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

  如果資源很分散，則處理時間可能會增加。

- 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更好地進行控制，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。

- 使用驗證者提升規則可協助縮短對驗證請求的回應時間。

  設定預設提升驗證者規則，或使用自訂的規則可設定驗證者提升鏈。還可指定提升逾時值。

- 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。

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 **[Compliance]** > **[Manage Access Scans]**。
2. 在 [Create New Access Scan] 頁面上，指定存取掃描的名稱。
3. (可選擇) 增加有助於識別掃描的描述。
4. 從以下選項中選取 **[User Scope Type]** ：(這是必填欄位。)
   - **[Members of Organization(s)]** — 選擇此選項可掃描一個或多個已選取組織的所有成員。
   - **[Reports to manager(s)]** — 選擇此選項可掃描向已選取管理員報告的所有使用者。管理員階層由使用者 Lighthouse 帳號的 Identity Manager 屬性決定。
   - **[According to attribute condition rule]** — 選擇此選項可選取用於指定要掃描之使用者類型的規則。Identity Manager 提供以下規則：
     - 所有管理員
     - 所有非管理員
     - 無管理員的使用者

備註 您可以使用 Identity Manager 整合開發環境 (IDE) 增加使用者範圍設定規則。詳細資訊請參閱 *Identity Manager Deployment Tools*。

如果使用者範圍爲**組織**或**管理員**，則 [Recursive Scope] 選項可用。此選項允許透過受控制成員鏈遞迴選取使用者。

5. 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，請將您的選項從 [Available Audit Policies] 移至 [Current Audit Policies]，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都將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做爲其邏輯的一部分。

6. 如果您還選擇掃描前面步驟中的稽核策略，則可以使用 **[Policy mode]** 選項指定存取掃描如何確定要針對指定使用者執行的稽核策略。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

7. (可選擇) 指定 **[Review Process Owner]**。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。

8. **[Follow delegation]** — 選取此選項可爲存取掃描啓用委託。如果已核取此選項，則存取掃描將僅遵循委託設定。依預設，啓用 [Follow Delegation]。

9. **[Restrict target resources]** — 選取此選項可限制掃描目標資源。

   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。

10. **[Execute Violation Remediations]** — 選取此選項可在偵測到違規時啓用稽核策略的修正工作流程。

    如果選取此選項，則偵測到之對任何指定稽核策略的違規都將導致執行相應的稽核策略修正工作流程。

11. **[Access Approval Workflow]** — 選取預設的標準驗證工作流程或選取自訂的工作流程 (如果有)。

    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。如果存取掃描指定提升，則此工作流程將負責提升休止過久的工作項目。如果爲指定任何工作流程，則使用者驗證將無限期地處於擱置狀態。

12. **[Attestor Rule]** — 選取預設驗證者規則，或選取自訂驗證者規則 (如果有)。

    將使用者軟體權利文件記錄做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 [Follow Delegation]，則存取掃描會遵循原始名稱清單中每個使用者配置的委託資訊，將名稱清單轉送給適當的使用者。如果 Identity Manager 使用者的委託導致路由循環，則將捨棄委託資訊，並將工作項目傳送至原始驗證者。預設驗證者規則指示驗證者應爲軟體權利文件記錄表示之使用者的管理員 (idmManager)，或配置程式帳號 (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。如需有關自訂規則的資訊，請參閱 *Identity Manager Deployment Tools* 指南。

13. **[Attestor Escalation Rule]** — 使用此選項指定預設提升驗證者規則，或選取自訂規則 (如果有)。您還可以指定規則的提升逾時值。

    此規則可指定已超過提升逾時期間之工作項目的提升鏈。預設提升驗證者規則提升至指定驗證者的管理員 (idmManager) 或配置程式 (如果驗證者的 idmManager 值爲空)。

    您可以分鍾、小時或天指定提升逾時。

14. **[Review Determination Rule]** — 選取以下任一規則來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。)

    - **[Reject Changed Users]** — 如果某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。
    - **[Review Changed Users]** — 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。
    - **[Review Everyone]** — 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，以便將比較限制在帳號資料的已選取部分。請參閱 *Identity Manager Deployment Tools* 以取得有關自訂規則的資訊。

15. **[Notification Workflow]** — 選取以下任一選項以指定每個工作項目的通知運作方式。

    - **[None]** — 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]** — 該選項可將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 7。

      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。

16. **[Violation limit]** — 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。空值欄位表示無限制。

    儘管與使用者數目相比，稽核掃描或存取掃描期間的策略違規數目通常很小，但設定此值可防止能大大增加違規數目之不完善策略帶來的不良影響。例如，考慮以下情況：

    如果存取掃描涉及 50K 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。

17. **[Organizations]** — 選取可使用該存取掃描物件的組織。這是必填欄位。

按一下 **[Save]** 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 [Compliance] 標籤中選取 [Manage Access Scans]，再選取掃描的名稱，然後按一下 **[Delete]**。

管理存取檢閱

定義存取掃描後，您便可以使用它或將其排定爲存取檢閱的一部分。啓動存取檢閱後，可使用多項作業來管理檢閱程序。

使用以下作業啓動與管理存取檢閱。

- 啓動存取檢閱
- 排定存取檢閱作業
- 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

若要啓動存取檢閱，請從管理員介面的 **[Server Tasks] > [Run Tasks]** 區域中選取 [Access Review] 作業。在 [Launch Task] 頁面中，指定存取檢閱的名稱。從 [Available Access Scans] 清單中選取掃描，然後將其移至 [Selected] 清單。如果您選取多個掃描，則可以選擇以下任一啓動選項：

- **[immediately]** — 按一下 [Launch] 按鈕後，此選項會立即開始執行掃描。如果您在 [Launch Task] 中爲多個掃描選取該選項，則掃描將並列執行。
- **[after waiting]** — 此選項可讓您指定啓動掃描前要等待的時間段，該時間段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數天才能完成。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 **[Launch]** 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。某些報告可能會比較具有相同名稱之定期執行的存取檢閱。

當您啓動存取檢閱時，螢幕上將顯示工作流程程序圖，其中顯示該程序的步驟。

排定存取檢閱作業

您可從 [Server Tasks] 區域排定存取檢閱作業。例如，若要定期設定存取檢閱，請使用 **[Manage Schedule]** 標籤定義排程。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 [Schedule Tasks] 頁面中選取作業，然後填寫 [Create task schedule] 頁面中的資訊。

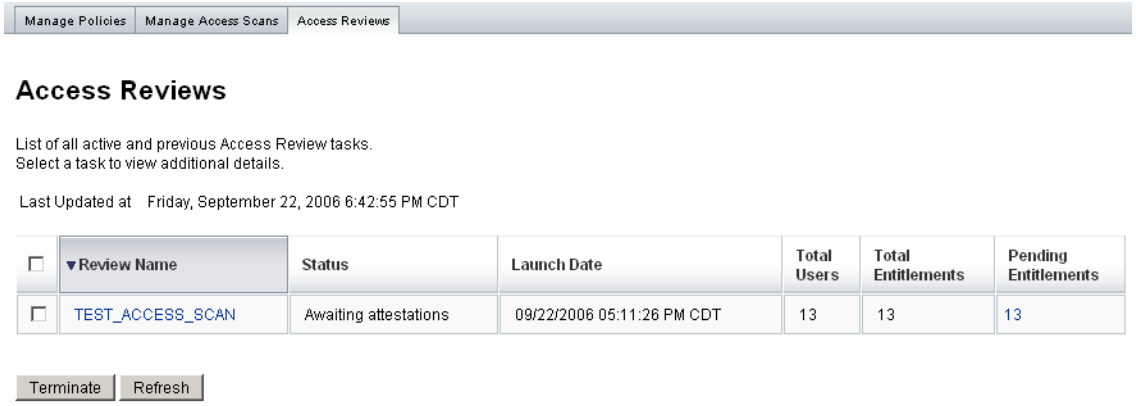
按一下 **[Save]** 儲存已排定的作業。

備註 依預設，Identity Manager 可將存取檢閱作業的結果保留一週。如果您選擇不到一週便排定一次檢閱，請將 [Results Options] 設定爲 [delete]。如果未將 [Results Options] 設定爲 [delete]，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 [Access Reviews] 標籤可監視存取檢閱的進度。透過 **[Compliance]** 標籤存取該功能。

圖 11-16 [Access Reviews] 頁面



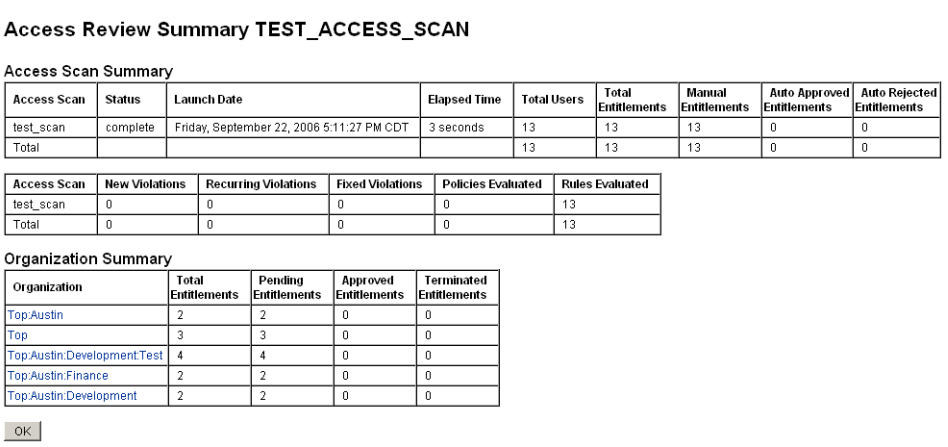
如前面的圖中所示，透過 [Access Reviews] 標籤，您可以檢閱所有使用中和先前已處理之存取檢閱的摘要。提供了所列之每個存取檢閱的以下資訊：

- **[Status]** — 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。
- **[Launch Date]** — 啓動存取檢閱作業的日期 (時間戳記)。
- **[Total Users]** — 要掃描的使用者總數。
- **[Total Entitlements]** — 針對檢閱產生的軟體權利文件記錄總數。
- **[Pending Entitlements]** — 尚未驗證的軟體權利文件記錄數目。

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 11-17 顯示了存取檢閱摘要報告範列。

圖 11-17 存取檢閱摘要報告頁面



Access Review Summary TEST_ACCESS_SCAN

Access Scan Summary

Access Scan	Status	Launch Date	Elapsed Time	Total Users	Total Entitlements	Manual Entitlements	Auto Approved Entitlements	Auto Rejected Entitlements
test_scan	complete	Friday, September 22, 2006 5:11:27 PM CDT	3 seconds	13	13	13	0	0
Total				13	13	13	0	0

Access Scan	New Violations	Recurring Violations	Fixed Violations	Policies Evaluated	Rules Evaluated
test_scan	0	0	0	0	13
Total	0	0	0	0	13

Organization Summary

Organization	Total Entitlements	Pending Entitlements	Approved Entitlements	Terminated Entitlements
Top:Austin	2	2	0	0
Top	3	3	0	0
Top:Austin:Development:Test	4	4	0	0
Top:Austin:Finance	2	2	0	0
Top:Austin:Development	2	2	0	0

OK

在網路型介面中，您可以按一下某連結以存取有關每個存取掃描、組織和驗證者的狀態資訊。

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 [Access Scans] 清單中選取該定義，然後在 [Edit Access Review Scan] 頁面中修改屬性。

您必須按一下 **[Save]** 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新取得之使用者軟體權利文件記錄中的資訊，因爲如果檢閱確定規則正在將使用者軟體權利文件與舊的使用者軟體權利文件記錄相比較，則其可能會對此規則產生影響。

取消存取檢閱

在 [Access Reviews] 標籤中，您可以按一下 **[Terminate]** 以停止進行中的已選取檢閱。終止檢閱將導致發生以下動作：

- 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
- 將所有擱置的使用者軟體權利文件都標記爲已取消
- 將使用者完成的所有驗證保留不變

刪除存取檢閱作業

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。

如要刪除存取檢閱作業，請選取功能表列中的 [Server Tasks]，然後選取 **[Run Tasks] > [Delete Access Review]**。

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，則將驗證請求傳送給受委託人。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 **[Attestation]** 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 [Work Items] 區域檢視驗證工作項目。選取 [Work Items] 區域中的 **[Attestation]** 標籤，可列出所有需要核准的軟體權利文件記錄。在 [Attestations] 頁面中，您還可以列出所有直接報告和您可直接或間接控制之特定使用者的軟體權利文件記錄。

[My Work Items] 標籤顯示每類指定，以及各類指定的擱置工作項目數。

檢閱與核准軟體權利文件記錄

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：

- **[Approve]** — 針對軟體權利文件記錄中記錄的日期，驗證軟體權利文件是否正確。
- **[Reject]** — 軟體權利文件記錄指示目前無法驗證之可能的不一致。
- **[Forward]** — 可讓您爲檢閱指定其他收件者。
- **[Abstain]** — 對此記錄的驗證不正確，但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。

如果在指定的提升逾時期間之前，驗證者未採取以上任一動作來回應請求，則會將通知傳送至提升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 **[Compliance] > [Access Reviews]** 標籤監視驗證狀態。

存取檢閱報告

Identity Manager 提供以下報告，可讓您評估存取檢閱的結果：

- **[Access Review Detail Report]** — 該報告以表格的格式提供以下資訊：
  - **[Name]** — 使用者軟體權利文件記錄的名稱
  - **[Status]** — 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
  - **[Attestor]** — 指定爲記錄驗證者的 Identity Manager 使用者
  - **[Scan Date]** — 記錄之掃描發生的時間戳記
  - **[Disposition Date]** — 驗證軟體權利文件記錄的日期 (時間戳記)
  - **[Organization]** — 軟體權利文件記錄中使用者的組織
  - **[Manager]** — 已掃描使用者的管理員
  - **[Resources]** — 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

- **[Violations]** — 檢閱期間偵測到的違規數目

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 11-18 顯示了使用者軟體權利文件記錄檢視中提供的資訊範例。

圖 11-18 使用者軟體權利文件記錄

- **[Access Review Summary Report]** — 此報告 (也已在第 365 頁的「管理存取檢閱進度」中討論，並在圖 11-17 中說明) 顯示以下有關您爲報告選取之存取掃描的摘要資訊：
  - **[Review Name]** — 存取掃描的名稱
  - **[Status]** — 啓動檢閱的時間戳記
  - **[User Count]** — 針對檢閱掃描的使用者數目
  - **[Entitlement Count]** — 產生的軟體權利文件記錄數目
  - **[Approved]** — 已核准的軟體權利文件記錄數目
  - **[Rejected]** — 已拒絕的軟體權利文件記錄數目
  - **[Pending]** — 仍處於擱置狀態的軟體權利文件記錄數目
  - **[Canceled]** — 已取消的軟體權利文件記錄數目

這些報告均可從 [Run Reports] 頁面，以可移植文件格式 (PDF) 或逗號分隔值 (CSV) 格式下載。

身份識別稽核作業參照

表 11-2 提供了經常執行之身份識別稽核作業的快速參照。此表格顯示了您開始每項作業的主要 Identity Manager 介面位置，以及可用於執行作業的替代位置或方法 (如果有)。

表 11-2 身份識別稽核作業參照

若要執行以下作業：	**請至：**
建立、編輯或刪除稽核策略	**[Compliance]** 標籤，**[Manage Policies]** 子標籤
定義修正者並指定修正工作流程	**[Compliance]** 標籤，**[Manage Policies]** 子標籤
對一或多個使用者或組織執行稽核掃描	**[Accounts]** 標籤，從 [User Actions] 或 [Organization Actions] 清單中選取 **[Scan]**
回應策略違規修正請求	**[Work Items]** 標籤，**[Remediations]** 子標籤
緩解策略違規	**[Work Items]** 標籤，**[Remediations]** 子標籤
檢閱補救的策略違規	**[Work Items]** 標籤，**[Remediations]** 子標籤
產生稽核策略報告	**[Reports]** 標籤，**[Run Report]** 子標籤
停用或啟用稽核	**[Configure]** 標籤，**[Audit]** 子標籤
設定要擷取的稽核事件	**[Configure]** 標籤，**[Audit]** 子標籤
編輯管理員稽核權能	**[Security]** 標籤，**[Capabilities]** 子標籤
設定稽核通知的電子郵件範本	**[Configure]** 標籤，**[Email Templates]** 子標籤
匯入資料檔 / 規則 (例如 XML 格式表單)	**[Configure]** 標籤，**[Import Exchange File]** 子標籤
定義存取檢閱掃描	**[Compliance]** 標籤，**[Manage Scans]** 子標籤
執行存取檢閱	**[Server Tasks]** 標籤，**[Run Task]** 子標籤
終止存取檢閱	**[Compliance]** 標籤，**[Access Reviews]** 子標籤
排定存取檢閱	**[Server Tasks]** 標籤，**[Manage Schedule]** 子標籤
設定定期存取檢閱	**[Compliance]** 標籤，**[Manage Access Scans]** 子標籤
監視存取檢閱狀態	**[Compliance]** 標籤，**[Access Reviews]** 子標籤
指定驗證者	**[Compliance]** 標籤，**[Manage Access Scans]** 子標籤
執行驗證者責任 (檢閱與認證使用者軟體權利文件)	**[Work Items]** 標籤，**[My Work Items]** 標籤，**[Attestation]** 子標籤
檢閱責任分離報告	**[Reports]** 標籤，**[Run Report]** 子標籤

章節 12

稽核記錄

本章說明 Sun Java™ System Identity Manager 稽核系統如何記錄事件。資訊組織如下：

概況

Identity Manager 稽核的目的是記錄誰在什麼時間對哪些 Identity Manager 物件執行了什麼作業。

稽核事件由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 「稽核檢閱與規範遵循管理」。

Identity Manager 稽核什麼內容？

大多數預設稽核都由內部 Identity Manager 元件執行。但是，有些介面允許從工作流程或從 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：

- **[Provisioner]** — 稱爲佈建程式的內部元件可產生稽核事件。
- **[View Handlers]** — 在視圖架構中，視圖處理程式需要產生稽核記錄。視圖處理程式應永遠在建立或修改物件時進行稽核。
- **[Session]** — 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視圖處理程式中。
- **[Workflow]** — 依預設，僅將核准工作流程配置爲產生稽核記錄。當核准或拒絕請求時，它們會產生稽核事件。稽核記錄程式透過 com.waveset.session.WorkflowServices 應用程式連接工作流程功能。

建立事件

雖然 Identity Manager 可處理內部稽核，但是在某些情況下，您可能希望從自訂工作流程記錄稽核事件。

從工作流程稽核

使用 com.waveset.session.WorkflowServices 應用程式可從任何工作流程程序中產生稽核事件。表 12-1 說明了適用於此應用程式的引數。

表 12-1 適用於 com.waveset.session.WorkflowServices 的引數

引數	類型	說明
op	字串	WorkflowServices 的作業。必須設定為稽核。
type	字串	要稽核的物件類型名稱。
action	字串	已執行的動作名稱。
status	字串	指定動作的狀態名稱。
name	字串	受指定動作影響的物件名稱。
resource	字串	(**可選擇**) 要變更之物件所在的資源名稱。
accountId	字串	(**可選擇**) 要修改的帳號 ID。 其應為本機資源帳號名稱。
error	字串	(**可選擇**) 與任何故障同時顯示的已本土化錯誤字串。
reason	字串	(**可選擇**) ReasonDenied 物件的名稱，該物件對映至說明一般故障原因的國際化訊息。
attributes	對映	(**可選擇**) 已增加或修改之屬性名稱和值的對映。
parameters	對映	(**可選擇**) 最多對映五個與某事件相關的附加名稱或值。
organizations	清單	將放置此事件的組織名稱或 ID 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	(**可選擇**) 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。

請參閱表 12-18，以取得預設物件、動作和狀態名稱的清單。

範例

代碼範例 12-1 說明了一個簡單工作流程作業。它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：

代碼範例 12-1 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>
```

代碼範例 12-2 顯示了如何將特定屬性增加至某個工作流程，該工作流程可追蹤核准程序中每個使用者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。

根據實際執行核准的人員，在表單和工作流程 (如果從核准表核准) 中設定 ACTUAL_APPROVER。APPROVER 可識別將其指定給的人員。

代碼範例 12-2 用於在核准程序中追蹤變更的已增加屬性

```
<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)'/>
```

代碼範例 12-2 用於在核准程序中追蹤變更的已增加屬性

```
<Action name='Audit the Approval'
   application='com.waveset.session.WorkflowServices'>
     <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>
    <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>
```

代碼範例 12-2 用於在核准程序中追蹤變更的已增加屬性

```
<Action name='Audit the Approval'
   application='com.waveset.session.WorkflowServices'>
    </Argument>
    <Argument name='approver' value='$(APPROVER)'/>
</Action>
```

稽核配置

稽核配置由一個或多個發佈程式以及數個預先定義的群組組成。

稽核群組可根據物件類型、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。可以爲稽核發佈程式指定文字格式化程式：文字格式化程式可提供稽核事件的文字說明。

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
- 發佈程式

filterConfiguration

`filterConfiguration` 屬性可列出事件群組，這些事件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 12-2 中列出的屬性。

表 12-2 filterConfiguration 屬性

屬性	類型	說明
groupName	字串	事件群組名稱
displayName	字串	表示群組名稱的訊息目錄關鍵字
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	清單	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。

代碼範例 12-3 說明了預設資源管理群組。

代碼範例 12-3 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 提供了以下預設事件群組：

- 帳號管理
- 規範遵循管理
- 配置管理
- Identity Manager 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 管理介面的 [Audit Events] 頁面配置每個群組 (`configure/auditeventconfig.jsp`)。此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 enabledEvent，但是您可以使用 Identity Manager 除錯頁面執行這些作業。

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 12-3 預設帳號管理事件群組

類型	動作
資源帳號	建立、更新、刪除、啟用、停用、拒絕、核准、重新命名
Identity Manager 帳號	建立、更新、刪除、啟用、停用、重新命名

規範遵循管理

依預設啓用此群組。

表 12-4 預設規範遵循管理群組事件

類型	動作
AuditPolicy	所有動作
ComplianceViolation	所有動作
補救工作流程	所有動作

配置管理

依預設啓用此群組。

表 12-5 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
規則	所有動作
EmailTemplate	所有動作
LoginConfig	所有動作
策略	所有動作
XMLData	匯入
記錄	所有動作

Identity Manager 登入 / 登出

依預設啓用此群組。

表 12-6 預設 Identity Manager 登入 / 登出事件群組

類型	動作
使用者	登入、登出、憑證過期
管理員	登入、登出、憑證過期

密碼管理

依預設啓用此群組。

表 12-7 預設密碼管理事件群組和事件

類型	動作
資源帳號	變更 / 重設密碼

資源管理

依預設啓用此群組。

表 12-8 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

角色管理

依預設停用此群組。

表 12-9 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 12-10 預設安全性管理事件群組和事件

類型	動作
ObjectGroup	所有動作
AdminGroup	所有動作
管理員	所有動作
加密金鑰	所有動作

作業管理

依預設停用此群組。

表 12-11 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

Identity Manager 之外的變更

依預設停用此群組。

表 12-12 Identity Manager 之外的變更事件群組和事件

類型	動作
NativeChange	ResourceAccount

Service Provider Edition

依預設啓用此群組。

表 12-13 Service Provider Edition 事件群組和事件

類型	動作
IDMXUser	建立、修改、刪除、使用者名稱回復、詢問回應、更新認證答案、作業前和作業後圖說文字、

extendedTypes

您增加至 com.waveset.object.Type 類別的每種新類型均可稽核。必須爲新類型指定唯一的雙字元資料庫關鍵字，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，您可能希望稽核沒有相關 com.waveset.objectType 的物件，或者希望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 12-14 延伸式物件屬性

引數	類型	說明
name	字串	類型名稱，在建構 AuditEvents 時和篩選事件期間使用。
displayName	字串	表示類型名稱的訊息目錄關鍵字。
logDbKey	字串	在記錄表中儲存此物件時要使用的雙字元資料庫關鍵字。請參閱「記錄資料庫關鍵字」以取得保留值。
supportedActions	清單	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	(可選擇) 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。

表 12-14 延伸式物件屬性

引數	類型	說明
organizationalMembership	清單	(可選擇) 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。

所有用戶特定關鍵字均應以 # 符號開頭，以防止增加新的內部關鍵字後出現重複的關鍵字。

代碼範例 12-4 說明了延伸式類型 Identity Manager 帳號。

代碼範例 12-4 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到 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 12-15 中列出的屬性。

表 12-15 extendedAction 屬性

屬性	類型	說明
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關鍵字。
logDbKey	字串	在記錄表中儲存此動作時要使用的雙字元資料庫關鍵字。 請參閱「記錄資料庫關鍵字」以取得保留值。

所有用戶特定關鍵字均應以 # 符號開頭，以防止增加新的內部關鍵字後出現重複的關鍵字。

代碼範例 12-5 說明了如何增加登出動作。

代碼範例 12-5 增加登出動作

```
<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到 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 12-16 中說明的屬性。

表 12-16 extendedResults 屬性

屬性	類型	說明
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關鍵字。
logDbKey	字串	在記錄表中儲存此結果時要使用的單字元資料庫關鍵字。請參閱標題為資料庫關鍵字的小節，以取得保留值。

所有用戶特定關鍵字均應使用 0 到 9 之間的數字，以防止增加新的內部關鍵字後出現重複的關鍵字。

發佈程式

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 12-17 發佈程式屬性

屬性	類型	說明
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關鍵字。
description	字串	對發佈程式的說明。
filters	清單	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	清單	發佈程式選項清單。這些選項是發佈程式特定的；清單中的每個項目均是 PublisherOption 的對映表示。請參閱 sample/auditconfig.xml 以取得範例。

資料庫模式

Identity Manager 資料庫中有兩個用於儲存稽核資料的表格：

- **waveset.log** — 儲存大部分事件詳細資訊。
- **waveset.logattr** — 儲存每個事件所屬組織的 ID。

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 C 「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關鍵字。如需關鍵字定義，請參閱標題爲「記錄資料庫關鍵字」的小節

- **objectType CHAR(2)** — 表示要稽核之物件類型的雙字元關鍵字。
- **action CHAR(2)** — 表示已執行之動作的雙字元關鍵字。

- **actionStatus CHAR(1)** — 表示已執行動作之結果的單字元關鍵字。
- **reason CHAR(2)** — 用於在發生故障時說明 ReasonDenied 物件的雙字元資料庫關鍵字。ReasonDenied 是包含訊息目錄項目的類別，用於一般故障 (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 (如果有)。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)** — 要對其執行動作的帳號 ID (如果有)。
- **server VARCHAR(128)** — 執行動作的伺服器 (由事件記錄程式自動指定)。
- **message VARCHAR(255)** — 任何與動作相關的已本土化訊息，包括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。
- **interface VARCHAR(50)** — 從中執行作業的 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做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 敘述來查詢此欄位。

  代碼範例 12-6 說明了 acctAttrChanges 欄中的值：

代碼範例 12-6 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)** — 這五個附加 NAME 槽是五個欄，它們最多可升級五個要儲存在各自欄中，而非大的二進位大型物件中的屬性。您可以使用 "audit?" 設定，從 [Resource Schema Configuration] 頁面升級屬性，這樣該屬性將適用於資料堪查。
- **acctAttr01value-acctAttr05value VARCHAR(128)** — 五個附加 VALUE 槽，它們最多可升級五個要儲存在獨立欄中，而非二進位大型物件欄中的屬性。
- **parm01label-parm05label VARCHAR(50)** — 五個用於儲存與事件相關之參數的槽。其範例爲用戶端 IP 和階段作業 ID。
- **parm01value-parm05value VARCHAR(128)** — 五個用於儲存與事件相關之參數的槽。其範例爲用戶端 IP 和階段作業 ID。
- **id VARCHAR(50)** — 透過 waveset.logattr 表中參照的儲存庫指定給每個記錄的唯一 ID。
- **name VARCHAR(128)** — 指定給每個記錄之已產生的名稱。

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)** — 目前永遠是 MEMBEROBJECTGROUPS。
- **attrval VARCHAR(255)** — 事件所屬 MemberObject 群組的 ID。

記錄資料庫關鍵字

actionStatus、動作、objectType 和原因欄在資料庫中儲存爲關鍵字，以節省空間。

物件類型、動作和結果

表 12-18 說明了在資料庫中儲存爲關鍵字的物件類型、動作和結果：

表 12-18 儲存爲關鍵字的物件類型、動作和結果

物件類型名稱	資料庫關聯字	動作名稱	資料庫關聯字	結果名稱	資料庫關聯字
帳號	AN	核准	AP	成功	S
管理員	AD	略過驗證	BV	失敗	F
AdminGroup	AG	取消調解	CR		
屬性定義	AF	詢問回應	CD		
應用程式	AP	變更密碼	CP		
權能	US	建立	CT		
配置	CN	連線	CO		
探索	DS	刪除	DL		
電子郵件範本	ET	取消佈建	DP		
取	ER	停用	DS		
ExtractTask	EX	結束連線	DC		
Identity Manager 帳號	LA	啟用	EN		
IDMX 使用者	UX	執行	LN		
載入配置	LD	匯出	EP		
LoadTask	LT	匯入	IM		
登入配置	LC	清單	LI		
策略	PO	載入	LD		
佈建作業	PT	登入	LG		
資源	RS	更新	MO		
資源帳號	RA	登出	LO		
資源表單	RF	本機變更	NC		
資源物件	RE	作業後	PT		
風險報告作業	RR	作業前	PE		
角色	RL	佈建	PV		
規則	RU	重設密碼	RP		
使用者	US	重新佈建	RV		
作業定義	TD	拒絕	RJ		
作業實例	TI	終止	TR		
作業排程	TS	使用者名稱回復	UR		
TaskTemplate	TT				
作業結果	TR				
使用者表單	UF				
WorkItem	WI				

表 12-18 儲存爲關鍵字的物件類型、動作和結果

物件類型名稱	資料庫關聯字	動作名稱	資料庫關聯字	結果名稱	資料庫關聯字
XML 資料	XD				

原因

表 12-19 說明了在資料庫中儲存爲關鍵字的原因：

表 12-19 儲存爲關鍵字的原因

原因名稱	英文	資料庫關聯字
策略違規	Violation of policy {0}: {1}	PV
憑證無效	Invalid credentials	CR
權限不足	Insufficient privileges	IP
資料庫存取失敗	Database access failed	DA
帳號已停用	Account disabled	DI

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中的記錄
- 修改現有稽核記錄中的記錄
- 刪除稽核記錄中的記錄或整個稽核記錄
- 截斷稽核記錄

所有 Identity Manager 稽核記錄中的記錄均具有唯一的、視伺服器而定的序列號以及記錄和序列號的加密雜湊。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：

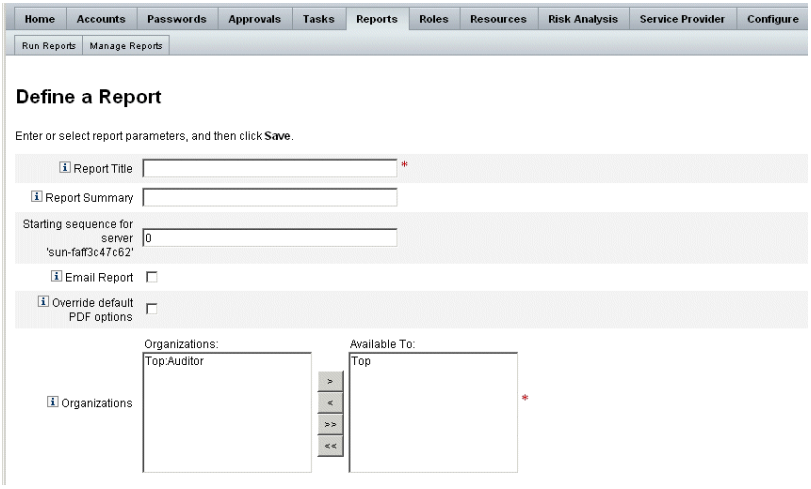
- 序列號中的間隔 (表示已刪除某記錄)
- 雜湊不相符 (表示已修改某記錄)
- 重複的序列號 (表示已複製某記錄)
- 小於預期序列號的最後一個序列號 (表示已截斷某記錄)

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 **[Reports] > [New] > [Audit Log Tampering Report]**，以建立竄改報告。
2. 當顯示 [Define a Tampering Report] 頁面 (請參閱圖 12-1) 時，爲報告輸入標題，然後 **[Save]** 該報告。

圖 12-1 配置稽核記錄竄改報告

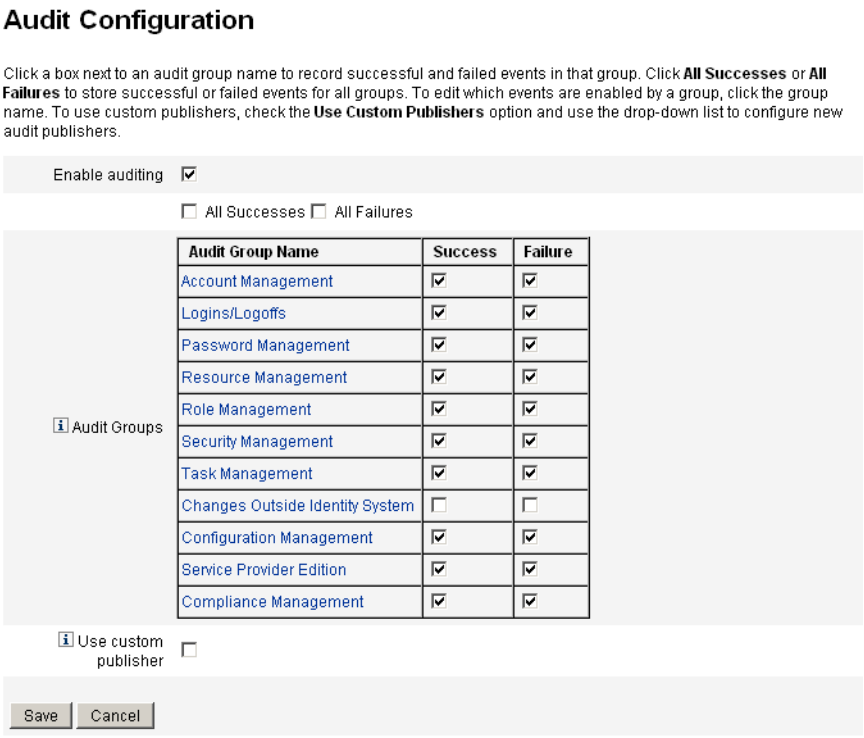


您也可以指定以下可選參數：

- **Report Summary** — 輸入報告的說明性摘要。
- **Starting sequence for server '<*server_name*>'** — 輸入伺服器的起始序列號。
- 此選項可讓您刪除舊的記錄項目而無需將其標記爲竄改，以及出於效能原因限制報告範圍。
- **Email Report** — 可將報告結果以電子郵件的形式傳送至指定的電子郵件地址。
- 選取此選項時，頁面會更新並提示您輸入電子郵件地址。但是，請記住，使用電子郵件傳送文字內容是不安全的 — 機密資訊 (例如帳號 ID 或帳號歷程記錄) 可能會洩漏。
- **Override default PDF options** — 選取改選項可以置換此報告的預設 PDF 選項。
- **Organizations** — 選取應具有此報告之存取權的組織。

3. 接下來選取 **[Configure] > [Audit]**，以開啓 [Audit Configuration] 頁面 (如圖 12-2 所示)。

圖 12-2 防竄改稽核記錄配置



4. 選取 **[Use Custom Publisher]**，然後按一下 [Repository publisher] 連結。
5. 選取 **[Enable tamper-resistant audit logs]**，然後按一下 **[OK]**。
6. 按一下 **[Save]** 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。

使用自訂發佈程式

Identity Manager 可以將稽核事件提交給自訂稽核發佈程式。提供了以下自訂發佈程式：

- 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

您可在參照工具組中找到這些發佈程式的原始碼。參照工具組中還提供了 Javadoc 格式的介面文件。

開發發佈程式

所有發佈程式均可實作 AuditLogPublisher 介面。(請參閱 Javadoc，以取得有關介面的詳細資訊)。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。(請參閱參照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置發佈程式的配置介面時會呼叫此方法。

Identity Manager 可在伺服器啓動時和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

參照工具組包含以下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) 格式化稽核事件。Sun Java System Application Server 就使用此格式。

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。請參閱參照工具組中的 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。

服務提供者管理

本章提供了您要管理 Sun Java™ System Identity Manager 中服務提供者 (SPE) 功能需要瞭解的資訊。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 SPE 部署」。

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 Service Provider Edition 功能可讓公司管理員將身份識別帳號分爲兩種不同的類型：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 [Service Provider User] 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 **SPE 系統帳號策略** (已增加至主 [Policies] 表) 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 [Resources] 頁面上的 [Resource Actions] 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 429 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 425 頁的「一般使用者介面」。

Access Manager 整合

您可以將 Sun Java System Access Manager 7 2005Q4 用於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。依預設匯入名爲 SPE 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。

Edit Main Configuration

若要編輯服務提供者實作的配置物件，請執行以下程序：

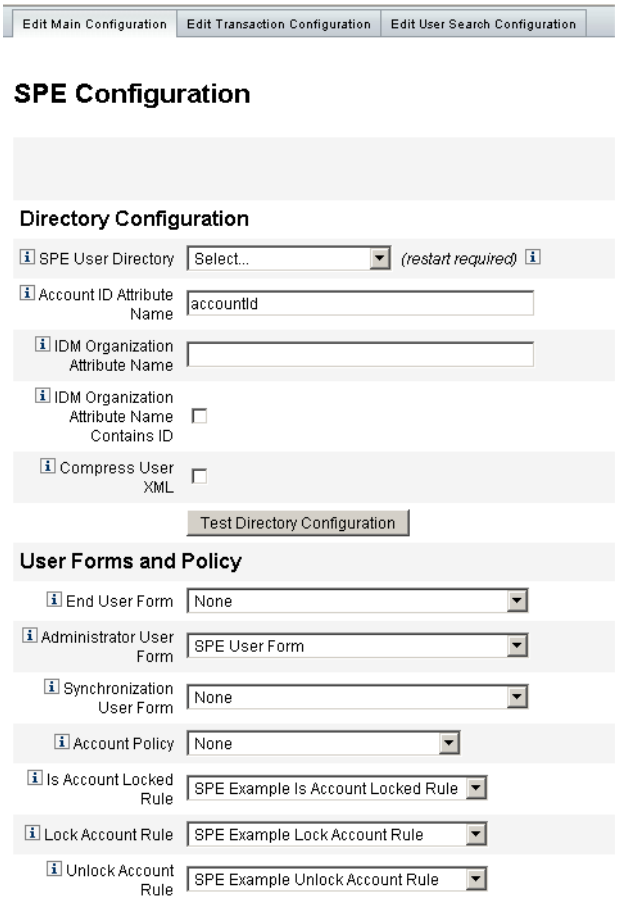
1. 使用配置程式權限登入 Identity Manager。
2. 按一下功能表列中的 **[Service Provider]**。
3. 按一下 **[Edit Main Configuration]**。螢幕上將顯示 **[SPE Configuration]** 頁面。在 [SPE Configuration] 頁面的以下每個區段中，依需要輸入資訊或選擇選項：
   - Directory Configuration
   - User Forms and Policy
   - 作業事件資料庫
   - 追蹤的事件配置
   - 同步化帳號索引
   - 圖說文字配置

Directory Configuration

在 [Directory Configuration] 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 13-1 顯示了 [SPE Configuration] 頁面的該區域，以及下小節中說明的 [User Forms and Policy] 區域。

圖 13-1 服務提供者 (SPE) 配置 (目錄、使用者表單與策略)



1. 從清單中選取 **[SPE End-User Directory]**。

   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 **[Account ID Attribute Name]**。

   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 Organization Attribute Name]**。

   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 如果您要透過組織授權啓用委託管理，則應指定 Identity Manager 組織屬性名稱 (以及包含 ID 的 IDM 組織屬性名稱 [如果需要])。

4. 如果您選擇選取 **[IDM Organization Attribute Name Contains 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 **[Compress User 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 **[Test Directory Configuration]** 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。

User Forms and Policy

在 [User Forms and Policy] 區域 (如上面的圖 13-1 所示) 中，指定要用於服務提供者使用者管理的表單與策略。

1. 從清單中選取 **[End User Form]**。

   此表單用於任何地方，[Delegated Administrator] 頁面和同步化期間除外。如果選取 **[None]**，則不使用任何預設使用者表單。

2. 從清單中選取 **[Administrator User Form]**。

   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 **[None]**，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 **[Synchronization User Form]**。

   使用服務提供者同步化作業時，請使用預設服務提供者使用者表單。如果選取 **[None]**，則不使用任何預設使用者表單。

4. 從清單中選取 **[Account Policy]**。

   選項包括透過 [Configure] > [Policies] 定義的任何身份識別帳號策略。

5. 從清單中選取 **[Is Account Locked Rule]**。

   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 **[Lock Account Rule]**。

   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。

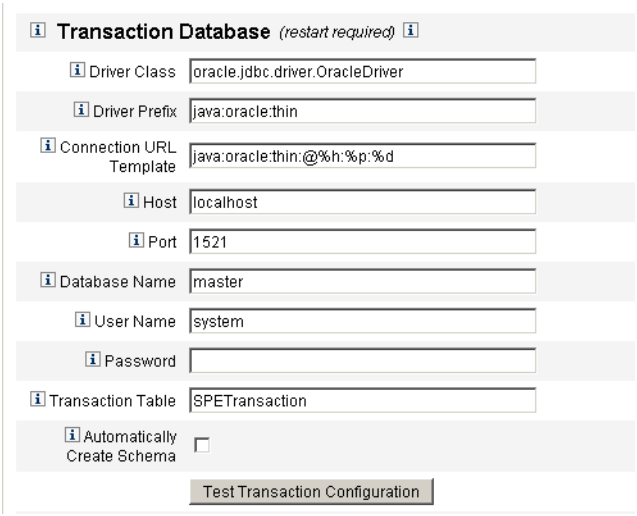
7. 選取 **[Unlock Account Rule]**。

   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 [SPE Configuration] 頁面的此區段 (如圖 13-2 所示)，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。

圖 13-2 服務提供者配置 (作業事件資料庫)



1. 輸入以下資料庫資訊：
   - **[Driver Class]** — 指定 JDBC 驅動程式類別名稱。
   - **[Driver Prefix]** — 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。
   - **[Connection URL Template]** — 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。
   - **[Host]** — 輸入正在執行資料庫的主機名稱。
   - **[Port]** — 輸入資料庫伺服器正在偵聽的連接埠號。
   - **[Database Name]** — 輸入要使用的資料庫名稱。
   - **[User Name]** — 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。
   - **[Password]** — 輸入資料庫使用者密碼。
   - **[Transaction Table]** — 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. 啓用 **[Automatically Create Schema]** 選項，以使 Identity Manager 自動建立表格的模式。

   對於生產系統，請停用此選項。對於生產系統，自訂 `Web/samples` 中的範例資料庫初始化程序檔。

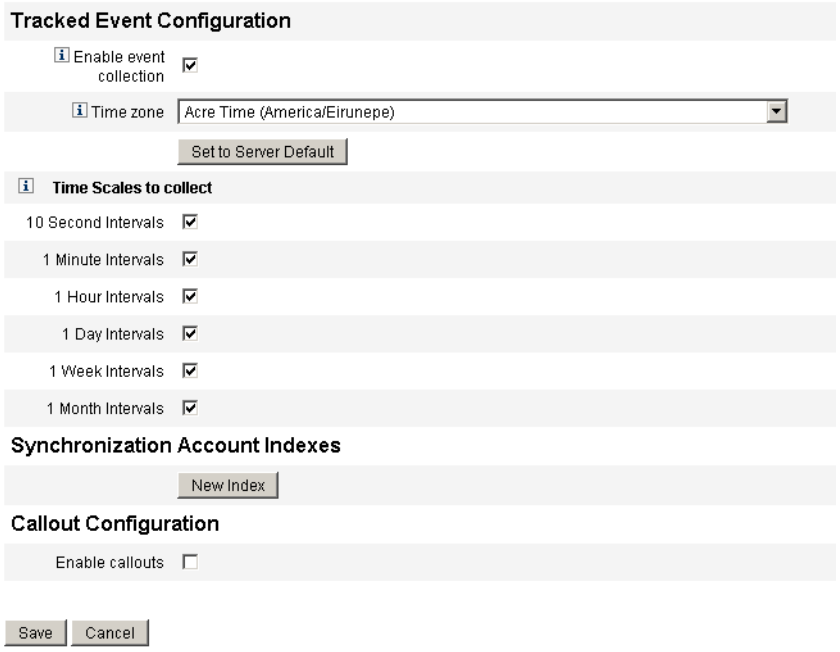
3. 按一下 **[Test Directory Configuration]** 以驗證項目 (如果適用)。

繼續至 [Service Provider Configuration] 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 13-3 所示。清除 **[Enable event collection]** 核取方塊可停用收集。

圖 13-3 服務提供者配置 (追蹤的事件、帳號索引和圖說文字配置)



執行以下程序來設定時區並指定服務提供者追蹤事件的收集間隔。

1. 從清單中選取 **[Time zone]**。

   選取記錄追蹤事件時要使用的時區，或選取 **[Set to Server Default]** 以使用伺服器上設定的時區。

2. 選取 **[Time Scales to collect]** 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使用 ActiveSync 資源時，可能需要定義 **[Account Indexes]** 以正確地將此資源傳送的事件與服務提供者目錄中的使用者相關聯。

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，不會一貫地傳送 accountId；例如，ActiveDirectory 的刪除事件僅包含 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 ActiveSync 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所有索引屬性之後：

1. 在配置頁面的 [Synchronization Account Indexes] 區域中，按一下 **[New Index]** 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 **[Resource]**。

   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 Attribute]** 或 **[Full Indentity Attribute]** 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 **[New Index]**，以定義其他資源的索引屬性。

5. 若要刪除索引，請按一下 **[Resource]** 選取欄位右側的 **[Delete]** 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 [Callout Configuration] 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 [None]。

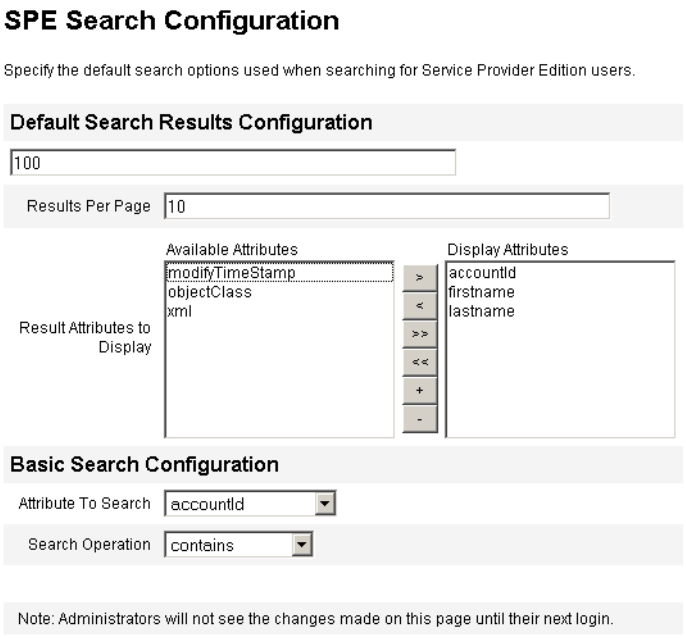
如果您指定作業後圖說文字，請使用 **[Wait for post-operation callout]** 選項指定作業事件必須等待作業後圖說文字處理完成後才能完成。這可確保僅在作業後圖說文字成功完成後才執行任何附屬作業事件。

備註 在 [SPE Configuration] 頁面上所有區段中完成選取後，按一下 **[Save]** 以完成配置。

編輯使用者搜尋配置

使用此頁面 (如圖 13-4 所示) 爲 [Manage Service Provider Users] 頁面上委託之管理員進行的搜尋配置預設搜尋設定。這些預設適用於 [Manage Service Provider Users] 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 13-4 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 **[Service Provider]**。
2. 按一下 **[Edit User Configuration]**。
3. 爲 **[Maximum Results Returned]** 輸入數字 (預設爲 100)。
4. 爲 **[Results Per Page]** 輸入數字 (預設爲 10)。
5. 使用箭頭鍵選取 **[Result Attributes to Display]** 旁邊的 **[Available Attributes]**。
6. 從清單中選取 **[Attribute to search]**。
7. 從清單中選取 **[Search Operation]**。
8. 按一下 **[Save]**。

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。

如果尚未配置 SPE 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

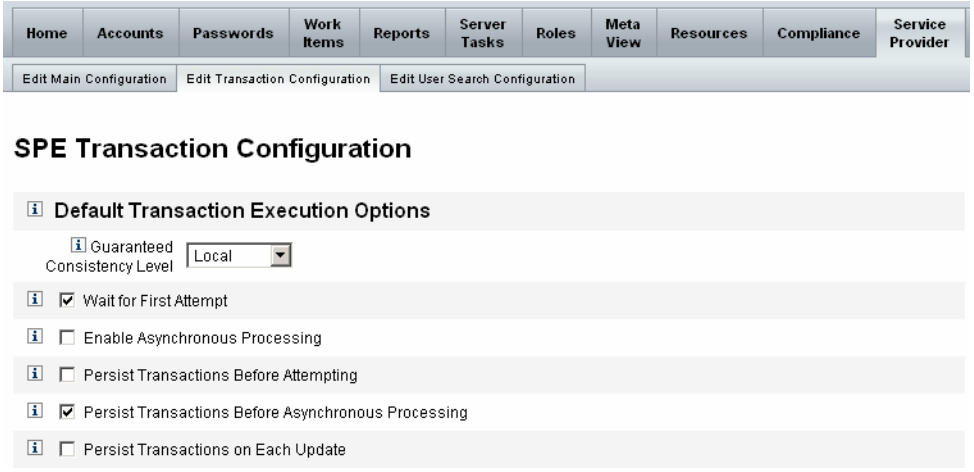
這些選項控制執行作業事件的方式，包含同步 / 非同步處理以及將其保留至「作業事件永久性存放區」中的時間。可以在 IDMXUser 檢視中置換它們或透過用於處理作業事件的表單來置換。如需更多資訊，請參閱 Identity Manager SPE 部署。

若要配置服務提供者作業事件，請執行以下步驟：

1. 按一下 **[Service Provider] > [Edit Transaction Configuration]**。螢幕上將顯示 **[SPE Transaction Configuration]** 頁面。

   圖 13-5 顯示了 [Default Transaction Execution options] 區域。

圖 13-5 作業事件配置



2. 從以下選項中選取 **[Guaranteed Consistency Level]**，以爲使用者更新指定作業事件一致性層級：

   - **[None]** — 使用者的資源更新沒有保證的順序
   - **[Local] —** 保證由相同伺服器處理的使用者資源更新按順序進行。
   - **[Complete]** — 保證使用者在所有伺服器上的所有資源更新都按順序進行。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：

   - **[Wait for First Attempt] —** 指定登入 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，則會阻斷登入作業，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。
   - **[Enable Asynchronous Processing]** — 此選項可控制在傳回登入呼叫後是否繼續處理佈建作業事件。由於僅同步進行一次嘗試，因此如果需要重試作業事件，請啓用此選項。

     選取 **[Enable Asynchronous Processing]** 後，請輸入 **[Retry Timeout]** 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。
   - **[Persist Transactions Before Attempting]** — 如果啓用，則會在嘗試佈建作業事件之前將其寫入作業事件永久存放區。啓用此選項可能會帶來不必要的經常性耗用時間，因爲大多數佈建作業事件在第一次嘗試時成功。除非已停用 **[Wait for First Attempt]** 選項，否則請考慮停用此選項。如果選取 [Complete] 一致性層級，則無法使用此選項。
   - **[Persist Transactions Before Asynchronous Processing]** (預設選項) — 如果啓用，則會在非同步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 [Wait for First Attempt] 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 [Wait for First Attempt] 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 [Complete] 一致性層級，則無法使用此選項。
   - **[Persist Transactions on Each Update]** — 如果啓用，則會在每次重試嘗試之後保留佈建作業事件。由於作業事件永久存放區 (可從 **[Search Transaction]** 頁面搜尋) 永遠保持最新狀態，因此其可協助隔離問題。

設定作業事件永久存放區

[SPE Transaction Configuration] 頁面上的這些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 13-6 配置 SPE 作業事件永久存放區

請執行以下程序來設定這些選項：

1. 從清單中選取所需的 **[Transaction Persistent Store Type]**。

   如果選取 **[Database]** 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。這可保證在重新啓動伺服器時，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 **[Simulated memory-based]** 選項，則需要重試的作業事件僅會儲存在記憶體中，並且在重新啓動伺服器時會遺失。對於生產環境，請啓用 **[Database]** 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 **[Transaction Persistent Store Type]** 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. 如有需要，請輸入 **[Customized queryable user attributes]**。

   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：

   - **[User path expression]** — 將路徑表示式輸入 IDMXUser 物件中。

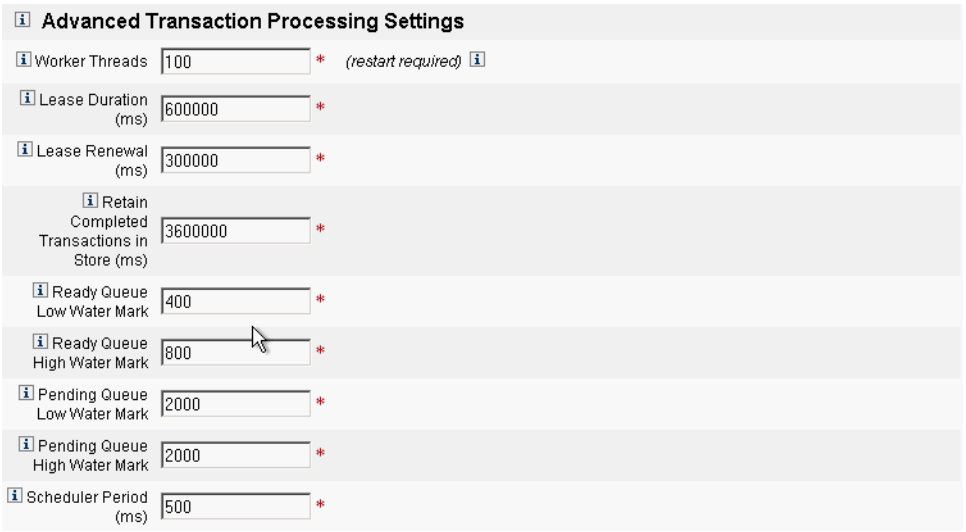
- **[Display name]** — 選擇與路徑表示式對應的顯示名稱。此顯示名稱會顯示在作業事件搜尋頁面上。

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 13-5 說明了 [Edit Transaction Configuration] 頁面上的 [Advanced Transaction Processing Settings] 區域。

圖 13-7 進階作業事件處理設定



1. 輸入所需的 **[Worker Threads] 數目 (預設為 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 **[Worker Threads]** 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 **[Lease Duration (ms)] (預設為 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「作業事件永久性存放區」的負載。

3. 輸入所需的 **[Lease Renewal (ms)]** 時間 **(預設為 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 **[Retain Completed Transactions in Store (ms)] (預設為 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「作業事件永久性存放區」不會包含所有完成的作業事件。

5. 輸入所需的 **[Ready Queue Low Water Mark] (預設為 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 **[Ready Queue High Water Mark] (預設為 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 **[Pending Queue Low Water Mark] (預設為 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 **[Pending Queue High Water Mark] (預設為 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 **[Scheduler Period (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 **[Save]** 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 [Edit Transaction Configuration] 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。

[Transaction Search] 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：

1. 登入 Identity Manager。
2. 按一下功能表列中的 **[Server Tasks]**。
3. 按一下 **[Service Provider Transactions]**。

   螢幕上將顯示 **[SPE Transaction Search]** 頁面，您可以在其中指定搜尋條件。

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 **[Accounts] > [Find Users]** 頁面相似。

4. 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 Transaction Configuration] 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)。

5. 如有需要，選取按 **[Type]** 搜尋。

   此選項可讓您搜尋所選類型的作業事件。

6. 如有需要，選取按 **[State]** 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 **[Unattempted]** 作業事件。
   - 已嘗試一次或多次 **[Pending retry]** 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。
   - **[Success]** 作業事件已成功完成。
   - **[Failure]** 作業事件已完成，但發生一次或多次故障。

7. 如有需要，選取按 **[Attempts]** 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。

8. 如有需要，選取按 **[Submitted]** 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。

9. 如有需要，選取按 **[Completed]** 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。

10. 如有需要，選取按 **[Cancelled Status]** 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。

11. 如有需要，選取按 **[Transaction 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。

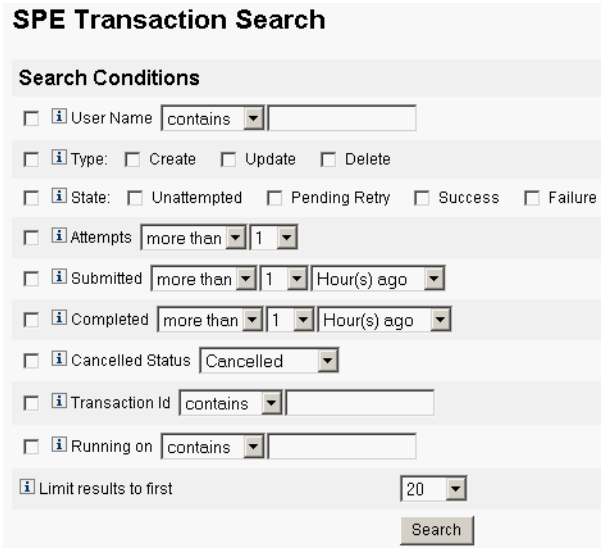
12. 如有需要，選取按 **[Running On]** (伺服器名稱) 搜尋。

    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。

13. 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。即使有更多的結果可用，也不會做任何指示。

圖 13-8 Search Transactions



14. 按一下 **[Search]**。

    螢幕上將顯示搜尋結果。

15. 如有需要，按一下結果頁面底部的 **[Download All Matched Transactions]**。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 **[Cancel Selected]**。無法取消已完成或已取消的作業事件。

委託管理

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委託管理。

透過組織授權進行委託

依預設，Identity Manager 透過基於組織的授權模式來提供管理責任委託。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受控制組織的 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 Main Configuration] 螢幕中 **[Identity Manager Organization Attribute Name Contains 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**管理員的受控制組織清單來比較屬性。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 Service Provider Edition 管理員在 `Top` 中具有服務提供者使用者權能，以管理這些使用者。
- 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。有特定於 Service Provider Edition 作業的權能，可以將其指定給使用者 (在 **[Edit User]** 頁面的 **[Security]** 標籤中)。受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 委託管理的更多資訊，請參閱第 5 章「管理」中的「委託管理」

透過管理員角色指定進行委託

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)。

若要對服務提供者使用者使用管理員角色委託，您必須在 Identity Manager 系統配置中將其啓用。

如果啓用透過管理員角色指定進行委託，則 [SPE Configuration] 中的 [IDM Organization Attribute Name] 不是必填欄位。

啟用服務提供者管理員角色委託

若要啓用服務提供者管理員角色委託 (SPE 委託管理)，請使用 Identity Manager 除錯頁面，將系統配置物件中的以下特性設定爲 `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 SPE 委託管理，請將系統配置配置物件中的以下屬性設定爲 「true」：

```
security.authz.external.Administrator Interface.Service Provider Users
```

如果爲指定的 Identity Manager 或服務提供者應用程式停用了 SPE 委託管理，則會使用基於組織的授權模式。

啓用 SPE 委託管理後，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。這些統計資料可在面板中找到。

配置服務提供者使用者管理員角色

若要配置服務提供者使用者管理員角色，請執行以下程序來建立管理員角色並指定控制範圍、權能以及應將其指定給的使用者：

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。您必須爲規則指定 `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 SPE 部署」。

1. 在 [Security] 標籤上，選取 [Admin Roles]，然後按一下 **[New]** 以開啓 [Create Admin Role] 頁面。
2. 指定管理員角色名稱，並選取 **[Service Provider Users]** 類型。
3. 按照以下各小節中的說明指定 [Scope of Control]、[Capabilities] 和 [Assign To Service Users] 選項。

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：

- **[User search context]** — 指定是使用規則還是文字字串來開始搜尋。

  如果指定 [None]，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。

- **[User search filter]** — 指定是將規則還是文字字串套用於搜尋篩選。

  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。

- **[After user search filter rule]** — 選取將在套用使用者搜尋篩選之後套用的規則。

  此規則在對服務提供者使用者目錄執行初始 LDAP 搜尋後執行，並可評估結果以確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 [Capabilities] 標籤上，選取 [Capabilities Per User Rule] 以套用於此管理員角色。

將管理員角色指定給服務提供者使用者

透過指定將在登入時進行評估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 [Assign To Service Provider Users] 標籤，並選取要套用於指定的規則。

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，方法是將以下系統配置物件設定爲 `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
- 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 Main configuration] (請參閱初始配置) 中的 [Identity Manager **Organization Attribute Name**] 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。

如果定義了 [Identity Manager **Organization Attribute Name**]，則在 [Create User] 或 [Edit User] 頁面上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 SPE 使用者表單以顯示完整組織路徑。

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。

您可從主 [Policies] 表中取得 **[SPE System Account Policy]**。

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：

1. 按一下功能表列中的 **[Accounts]**。
2. 按一下 **[Manage Service Provider Users]** 標籤。
3. 按一下 **[Create Account]**。

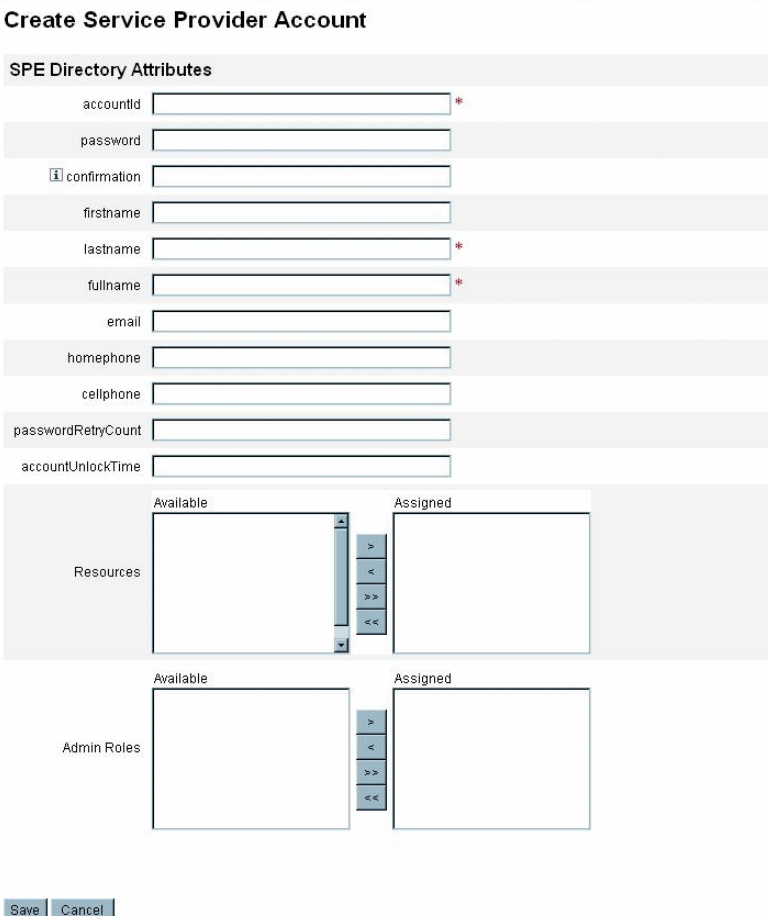
備註 使用預設服務提供者使用者表單時，實際顯示的欄位取決於在服務提供者目錄資源之 [Account Attributes] 表 (模式對映) 中配置的屬性。而且，當您將資源指定給使用者 (例如委託管理員) 時，可以看到顯示中增加了新的區段，您可以在其中指定這些資源的屬性值。您還可以自訂欄位。

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 [Available] 清單中指定所需的 [Resources]。
6. **[Account Status]** 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 13-9 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。如有需要，請自訂提供的服務提供者使用者表單範例。

7. 按一下 **[Save]** 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 **[Accounts]** 區域)，請按一下 **[Manage Service Provider Users]**，然後輸入搜尋值並按一下 **[Search]**。

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

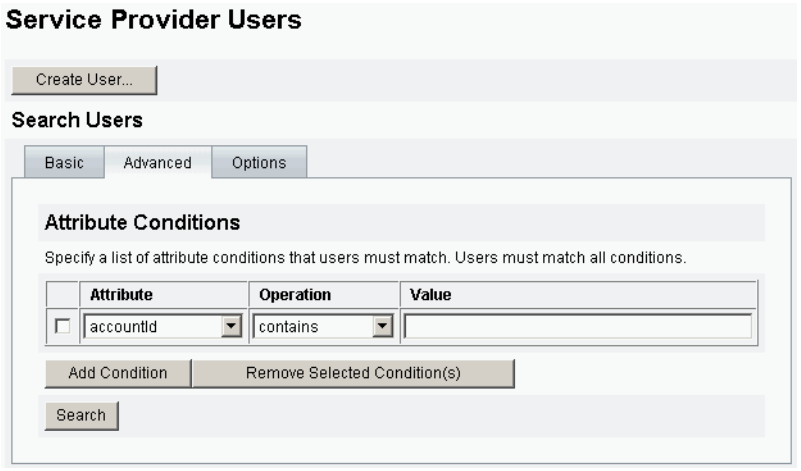
進階搜尋

若要執行服務提供者使用者進階搜尋 (從 [Service Provider Users Search] 頁面)，請按一下 **[Advanced]**，然後完成以下動作：

1. 從清單中選擇所需的 **[Attribute]**。
2. 從清單中選擇所需的 **[Operation]**。

   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 **[Search]**。

圖 13-10 搜尋使用者



您可以使用以下選項增加或移除 [Attribute Conditions]：

- 按一下 **[Add Condition]** 並指定新屬性。
- 選取項目並按一下 **[Remove Selected Condition(s)]**。

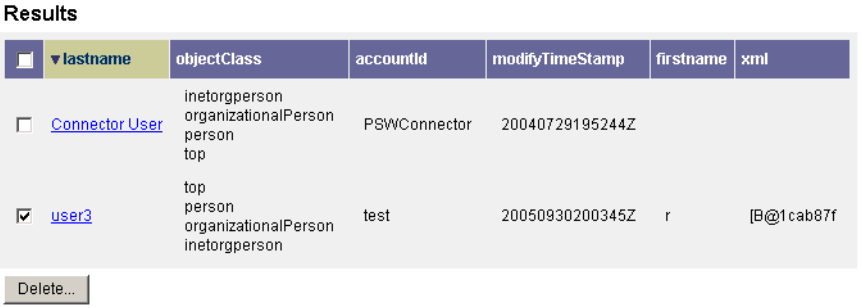
搜尋結果

服務提供者搜尋結果顯示在表格中，如圖 13-11 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 13-11 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 **[Delete]** 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」)。

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，請執行以下程序：

1. 登入 Identity Manager。
2. 按一下功能表列中的 **[Accounts]**。
3. 按一下 **[Manage Service Provider Users]**。
4. 執行基本搜尋或進階搜尋。
5. 選取所需的使用者。
6. 按一下 **[Delete]** 按鈕。
7. 如有需要，請選取其中一個全域選項：
   - **Delete All resource accounts**

備註	刪除資源可刪除帳號，但資源指定仍然存在。使用者的後續更新會重建帳號。刪除永遠意味著取消連結資源帳號。

   - **Unassign All resource accounts**

備註	取消指定資源會移除該資源指定。取消指定意味著取消連結資源帳號。取消指定資源時，不會刪除資源帳號。

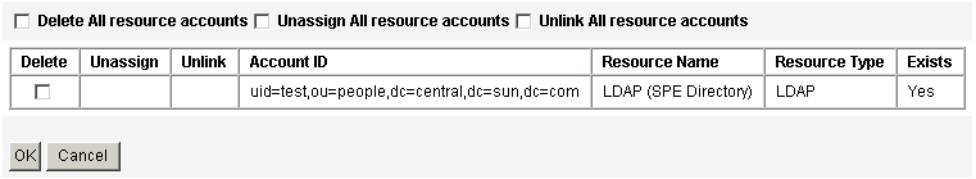
   - **Unlink All resource accounts**

備註	取消連結會移除使用者與資源帳號之間的連結，但不會刪除帳號，也不會移除資源指定，因此使用者的後續更新會重新連結帳號或在資源上建立新帳號。

8. 或者，在 **[Delete]**、**[Unassign]** 或 **[Unlink]** 欄中爲一個或多個資源帳號選取動作。

9. 選取所需的使用者帳號之後，按一下 **[OK]**。

圖 13-12 刪除、取消指定或取消連結帳號



設定搜尋選項

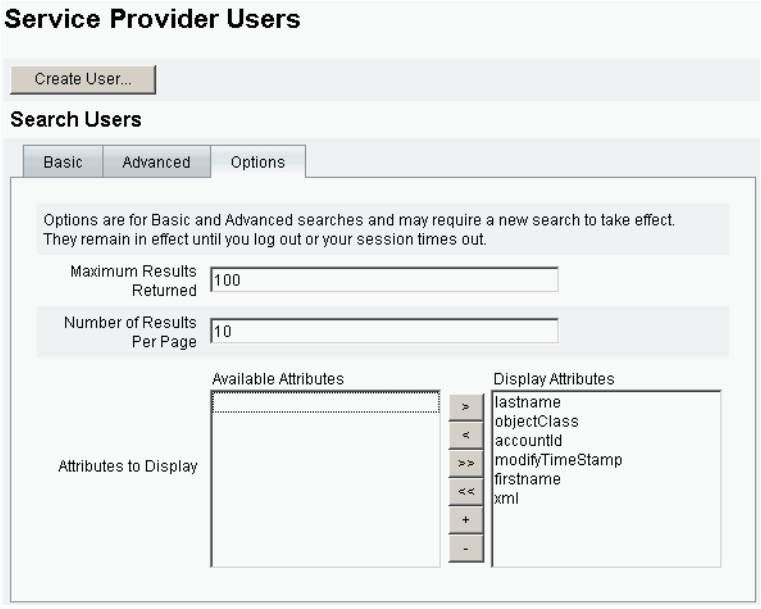
請執行以下程序來設定服務提供者使用者的搜尋選項：

1. 按一下功能表列中的 **[Accounts]**。
2. 按一下 **[Service Provider]**。
3. 按一下 **[Options]**。

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 **[Maximum Results Returned]**。
5. 輸入 **[Number of Results Per Page]**。
6. 使用箭頭鍵從 **[Available Attributes]** 中選擇所需的 **[Display Attribute]**。

圖 13-13 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 SPE 部署」。

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，可以延伸或替代做爲 Servlet 篩選器實作的模組認證服務。這將允許與存取管理系統 (如 Sun Java System 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：

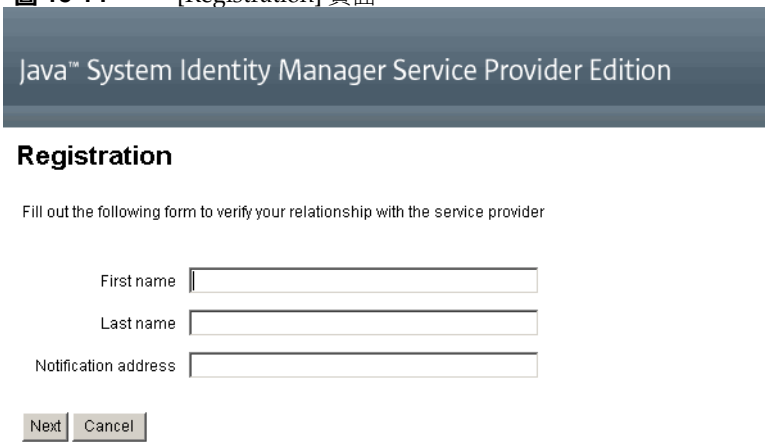
- 商標
- 配置選項 (例如失敗的登入嘗試次數)
- 增加 / 移除頁面

如需有關自訂頁面的更多資訊，請參閱 「Identity Manager SPE 部署」。

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。

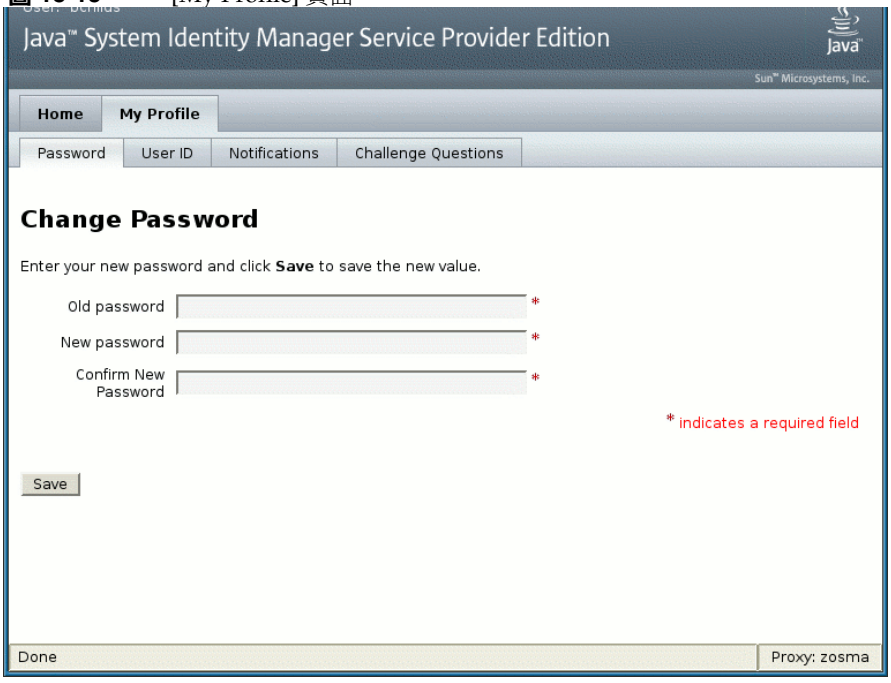
圖 13-14 [Registration] 頁面



[Home] 螢幕和 [Profile] 螢幕

圖 13-15 顯示了一般使用者 [Home] 標籤和 [Profile] 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 13-15 [My Profile] 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 **[Resources]** 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 200 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 **[Service Provider Edition User]** 做爲目標物件類型。
- 在 [Scheduling Settings] 區段中，選取 **[Enable Synchronization]**。

按照第 200 頁的「配置同步化」中的說明，指定適合您環境的其他選項。

備註 配置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 SPE 部署」，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 **[Save]** 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 [Synchronization Resource Action] 下的 **[Start for Service Provider]** 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 [Resource] 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，依預設啓用服務提供者同步化。若要停用服務提供者 Active Sync，請執行以下程序：

1. 在 **[Resources]** 區域中，選取資源並按一下 **[Edit Synchronization Policy]** 以編輯策略。
2. 清除 **[Enable Synchronization]** 核取方塊。

3. 按一下 **[Save]**。

   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 [Synchronization Resource Action] 中選取 **[Stop for Service Provider]**。

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。

若要遷移現有的 Identity Manager 使用者，請：

1. 按一下功能表列中的 **[Tasks]**。
2. 按一下 **[Run Tasks]**
3. 按一下 **[SPE Migration]**。
4. 輸入唯一的 **[Task Name]**。
5. 從清單中選取 **[Resource]**。

   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 **[Identity Attribute]**。

   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 **[Identity Rule]**。

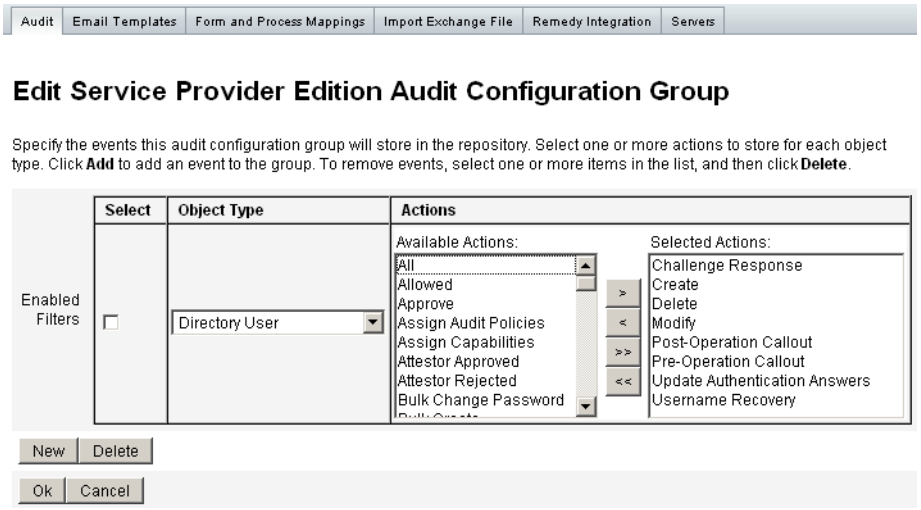
   這是可以由 Identity Manager 使用者屬性計算目錄使用者名稱的可選規則。身份識別規則可以計算簡單名稱 (通常爲 uid)，該簡單名稱然後會透過資源的身份識別範本得以處理，以形成目錄伺服器的辨別名稱 (DN)。此規則還可傳回不使用 ID 範本的完整指定 DN。
8. 按一下 **[Launch]** 以啓動背景遷移作業。

配置服務提供者稽核事件

在服務提供者實作中，Identity Manager 的稽核記錄系統會稽核與企業外部網路使用者作業相關的事件。Identity Manager 提供了 Service Provide Edition 稽核配置群組 (依預設已啓用)，其可指定爲服務提供者使用者記錄的稽核事件。請參閱圖 13-16。

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 12 章 「稽核記錄」

圖 13-16 [Edit Service Provider Edition Audit Configuration Group] 頁面



lh 參照

用法

使用以下語法呼叫 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。

  如果您安裝的是 Sun 提供的標準 JRE (不含 JDK)，典型的目錄位置將會是 `C:\Program Files\Java\j2re1.4.1_01`。此目錄包含內有 Java 程式檔的 `bin` 目錄。在此情況下，請將 `JAVA_HOME` 設定爲 `C:\Program Files\Java\j2re1.4.1_01`。

  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。如需典型安裝，請將 `JAVA_HOME` 設定爲 `D:\java\jdk1.3.1_02.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：

  ```
  set WSHOME=C:\tomcat\webapps\idm
  ```

備註 在 Unix 系統上，您還必須匯出路徑變數，如下所示：

```
export WSHOME
export JAVA_HOME
```

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：

- `config` — 啓動業務程序編輯器。
- `console` — 啓動 Identity Manager 主控台。
- `js` — 呼叫 JavaScript 程式。
- `javascript` — 與 js 相同
- `import` — 匯入 Identity Manager 物件
- `license [options] {status | set {parameters }}` — 設定 Identity Manager 授權碼。
- `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案。
- `syslog [options]` — 從系統記錄檔中擷取記錄。
- `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`

license 指令

使用情況

`license [options] { status | set {parameters} }`

選項

- `-U` *`username`* (如果重新命名了配置程式帳號)
- `-P` *`PathtoPassword`*`.txt` (如果變更了配置程式密碼)

`set` 選項的參數必須爲 `-f` *`File`* 形式。

範例

- `lh license status`
- `lh license set -f` *`File`*

syslog 指令

使用情況

```
syslog [options]
```

選項

- `-d` *Number* — 顯示以前 *Number* 天的記錄 (預設 = 1)
- `-F` — 僅顯示嚴重嚴重性層級的記錄
- `-E` — 僅顯示錯誤嚴重性層級或更高層級的記錄
- `-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)

線上文件進階搜尋

在搜尋 Identity Manager 線上文件時，您可以使用進階語法建立複雜的查詢。這些情況說明如下：

- 萬用字元符號 — 可讓您指定拼字式樣，而非完整的詞。
- 查詢運算子 — 指定將組合或修改查詢元素的方式。

備註 您可以在同一搜尋中使用萬用字元符號和查詢運算子。

萬用字元符號

萬用字元是在搜尋中代表其他字元或多組字元的特殊字元。

Identity Manager 線上文件搜尋功能支援這些萬用字元符號

表 B-1 支援的萬用字元符號

萬用字元符號	用途
問號 (?)	比對任何單一字元。 例如，搜尋 t?p 將比對詞 tap、tip 和 top。搜尋 ball???? 將比對詞 ballpark、ballroom 和 ballyhoo，但不會尋找 ballet 或 balloon，因為它們在「ball」之後不是正好包含四個字母。
星號 (*)	比對任何一組字元。 例如，搜尋 comp* 會尋找以字母 comp 開頭的詞的任何相符項，如 computer、company 或 comptroller。

查詢運算子

查詢運算子可讓您組合、修改或排除搜尋元素。您可以以大寫、小寫或大小寫混合的方式鍵入查詢運算子。通常，查詢運算子以角括號開頭和結尾，例如 <CONTAINS>。

備註 基本布林運算子 (AND、OR 和 NOT) 和特殊字元運算子 (例如 <、= 和 !=) 不需要括號。

優先順序規則

如果在查詢中使用多個運算子，則優先順序規則和括號將決定運算子的範圍。AND 運算子的優先順序高於 OR 運算子。例如，以下查詢：

```
resource AND adapter OR attribute
```

等同於：

```
(resource AND adapter) OR attribute
```

如果希望搜尋功能解譯爲「adapter」和「attribute」其中任意一個要與「resource」一起尋找，則必須使用括號，如下所示：

```
resource AND (adapter OR attribute)
```

預設運算子

如果鍵入一連串查詢字詞或元素而不指定運算子，則會使用標準的預設運算子 <AND> 來組合查詢元素。

如果查詢由單個詞組成，但沒有明確的一元字詞運算子 (例如 <EXACT>、<MORPH> 或 <EXPAND>)，則假設這些詞由預設字詞運算子 <MORPH> 管理。

下表列出了線上文件搜尋最常用的查詢運算子。

表 B-2 線上文件搜尋常用的查詢運算子

運算子	說明	範例
<AND> 或 AND	為搜尋增加必要條件。	搜尋「apples AND oranges」將以任意順序傳回包含「apples」和「oranges」的相符項。將忽略僅包含一個詞的文件。
<CASE>	與以下字詞的大小寫相符。 備註：Identity Manager 會自動處理為大寫查詢字詞在比對時大小寫需相符，因此無需 <CASE>。小寫字詞被視為大小寫不需相符，因此您必須使用 <CASE> 來僅比對小寫字詞。	搜尋「<CASE> bill」將尋找「bill」而非「Bill」的相符項。
<EXACT>	尋找包含指定的精確詞的文件。	搜尋「<EXACT> soft」將尋找包含詞「soft」的文件，但不會尋找包含「softest」或「softer」的文件。
<MORPH>	尋找結構上與指定詞不同的文件，包括複數、過去式和包含前綴、後綴和複合詞的複雜形式。還將使用詞典中的知識正確處理不規則形式。	搜尋「<MORPH> surf」將尋找包含詞「surf」的可推理變體 (如「surfs」、「surfed」和「surfing」) 的文件，以及包含前綴 (「resurf」) 和複合詞 (「surfboard」) 的文件。
<NEAR>	尋找指定詞之間間隔不超過 1000 個詞的文件。詞的距離越近，該文件在搜尋結果中的位置越靠前。	搜尋「resource <NEAR> configuration」將尋找包含兩個詞且兩詞間不多於 1000 個詞的文件。
<NEAR/n>	尋找指定詞之間間隔不超過 n 個詞的文件。 備註：*n* 的值必須在 1 和 1024 之間。	搜尋「buy <NEAR/3> sell」將尋找包含「buy low and sell high」的文件，因為在「buy」和「sell」之間不多於三個詞。
<NOT> 或 NOT	尋找不包含特定詞或片語的文件。	搜尋「surf <AND> <NOT> channel」將尋找包含「surf」但不包含「channel」的文件。

稽核記錄資料庫模式

此附錄提供了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 C-1 列出了 Oracle 資料庫類型的資料模式值：

表 C-1 Oracle 資料庫類型的資料模式值

資料庫欄	值
id	VARCHAR(50) NOT NULL
name	VARCHAR(128) NOT NULL
resourceName	VARCHAR(128)
accountName	VARCHAR(50)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDate	CHAR(8)

表 C-1 Oracle 資料庫類型的資料模式值

資料庫欄	值
actionTime	CHAR(12)
acctAttrChanges	VARCHAR(4000)
acctAttr01label	VARCHAR(50)
acctAttr01value	VARCHAR(128)
acctAttr02label	VARCHAR(50)
acctAttr02value	VARCHAR(128)
acctAttr03label	VARCHAR(50)
acctAttr03value	VARCHAR(128)
acctAttr04label	VARCHAR(50)
acctAttr04value	VARCHAR(128)
acctAttr05label	VARCHAR(50)
acctAttr05value	VARCHAR(128)
parm01label	VARCHAR(50)
parm01value	VARCHAR(128)
parm02label	VARCHAR(50)
parm02value	VARCHAR(128)
parm03label	VARCHAR(50)
parm03value	VARCHAR(128)
parm04label	VARCHAR(50)
parm04value	VARCHAR(128)
parm05label	VARCHAR(50)
parm05value	VARCHAR(128)

DB2

表 C-2 列出了 DB2 資料庫類型的資料模式值：

表 C-2 DB2 資料庫類型的資料模式值

資料庫欄	值
id	VARCHAR(50) NOT NULL
name	VARCHAR(128) NOT NULL
resourceName	VARCHAR(128)
accountName	VARCHAR(50)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDate	CHAR(8)
actionTime	CHAR(12)
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)
message	VARCHAR(255)
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)
acctAttr05label	VARCHAR(50)
acctAttr05value	VARCHAR(128)

表 C-2 DB2 資料庫類型的資料模式值

資料庫欄	值
parm01label	VARCHAR(50)
parm01value	VARCHAR(128)
parm02label	VARCHAR(50)
parm02value	VARCHAR(128)
parm03label	VARCHAR(50)
parm03value	VARCHAR(128)
parm04label	VARCHAR(50)
parm04value	VARCHAR(128)
parm05label	VARCHAR(50)
parm05value	VARCHAR(128)

MySQL

表 C-3 列出了 MySQL 資料庫類型的資料模式值：

表 C-3 MySQL 資料庫類型的資料模式值

資料庫欄	值
id	VARCHAR(50) BINARY NOT NULL
name	VARCHAR(128) BINARY NOT NULL
resourceName	VARCHAR(128)
accountName	VARCHAR(50)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDate	CHAR(8)
actionTime	CHAR(12)
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)

表 C-3 MySQL 資料庫類型的資料模式值

資料庫欄	值
reason	CHAR(2)
message	VARCHAR(255)
acctAttrChanges	BLOB
acctAttr01label	VARCHAR(50)
acctAttr01value	VARCHAR(128)
acctAttr02label	VARCHAR(50)
acctAttr02value	VARCHAR(128)
acctAttr03label	VARCHAR(50)
acctAttr03value	VARCHAR(128)
acctAttr04label	VARCHAR(50)
acctAttr04value	VARCHAR(128)
acctAttr05label	VARCHAR(50)
acctAttr05value	VARCHAR(128)
parm01label	VARCHAR(50)
parm01value	VARCHAR(128)
parm02label	VARCHAR(50)
parm02value	VARCHAR(128)
parm03label	VARCHAR(50)
parm03value	VARCHAR(128)
parm04label	VARCHAR(50)
parm04value	VARCHAR(128)
parm05label	VARCHAR(50)
parm05value	VARCHAR(128)

Sybase

表 C-4 列出了 Sybase 資料庫類型的資料模式值：

表 C-4 Sybase 資料庫類型的資料模式值

資料庫欄	值
id	VARCHAR(50) NOT NULL
name	VARCHAR(128) NOT NULL
resourceName	VARCHAR(128)
accountName	VARCHAR(50)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDate	CHAR(8)
actionTime	CHAR(12)
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)
message	VARCHAR(255)
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)
acctAttr05label	VARCHAR(50)
acctAttr05value	VARCHAR(128)

表 C-4 Sybase 資料庫類型的資料模式值

資料庫欄	值
parm01label	VARCHAR(50)
parm01value	VARCHAR(128)
parm02label	VARCHAR(50)
parm02value	VARCHAR(128)
parm03label	VARCHAR(50)
parm03value	VARCHAR(128)
parm04label	VARCHAR(50)
parm04value	VARCHAR(128)
parm05label	VARCHAR(50)
parm05value	VARCHAR(128)

稽核記錄資料庫對映

表 C-5 包含已儲存稽核記錄資料庫關鍵字和其在稽核報告輸出中與之對映的顯示字串之間的對映。Identity Manager 可將用做常數的項目儲存爲短的資料庫關鍵字，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 C-5 物件關鍵字類型、動作和動作狀態資料庫關鍵字

稽核物件類型	資料庫關鍵字	動作	資料庫關鍵字	動作狀態	資料庫關鍵字
管理員	AD	核准	AP	失敗	F
管理員群組	AG	變更密碼	CP	成功	S
應用程式	AP	變更資源密碼	CR		
稽核配置	AC	配置	CG		
稽核記錄	AL	連線	CN		
電子郵件範本	ET	建立	CT		
Lighthouse 帳號	LA	憑證已過期	CE		
登入配置	LC	刪除	DL		
通知	NT	刪除帳號	DA		
物件群組	OG	取消佈建	DP		

表 C-5 物件關鍵字類型、動作和動作狀態資料庫關鍵字

稽核物件類型	資料庫關鍵字	動作	資料庫關鍵字	動作狀態	資料庫關鍵字
策略	PO	停用	DS		
Remedy 配置	RC	結束連線	DC		
資源帳號	RA	啓用	EN		
資源	RS	啓動	LN		
資源物件	RE	載入	LD		
角色	RL	登入	LG		
角色屬性	RT	登出	LO		
作業定義	TD	本機變更	NC		
作業實例	TI	保護資源密碼	PT		
作業排程	TS	佈建	PV		
使用者	US	拒絕	RJ		
工作流程情況	WC	重新佈建	RV		
工作流程程序	WP	重設密碼	RP		
工作流程作業	WT	終止	TR		
		更新	MO		
		檢視	VW		

Active Sync 精靈

概況

在 7.0 之前版本的 Identity Manager 中，Active Sync 精靈用於建立和管理使用中的同步化。此附錄所包含的資訊，說明如何使用 Active Sync 精靈在受支援的 Identity Manager 版本中，設定和管理使用中的同步化作業。對於 7.0 及更高版本，同步化策略用於配置同步化。

設定同步化

在 Identity Manager 資源區域中，使用 Active Sync 精靈設定使用中的同步化。此精靈會透過各種步驟集 (視您所做的選擇而定) 引導您爲資源設定使用中的同步化。

若要啓動 Active Sync 精靈，請從 [resources] 清單中選取資源，然後從 [Resource Actions] 選項清單中選取 **[Active Sync Wizard]**。

同步化模式

[Synchronization Mode] 頁面可讓您決定在設定使用中的同步化期間，可以選擇的配置選項的範圍。

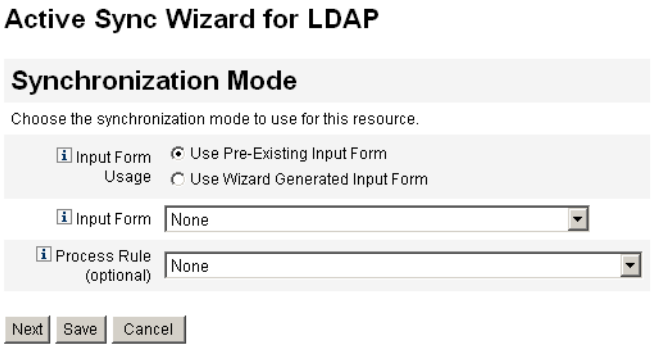
從這些選項中選取：

[Input Form Usage] — 選取當設定使用中的同步化時要使用的模式。您可以選擇使用預先存在的表單，該表單會限制此資源的配置選擇。或者，您可以使用由「Active Sync 精靈」產生的表單，該表單會提供完整的配置選擇集。

- 如果您選取 [Pre-Existing Input Form] (預設值)，請爲下列選項做出選擇：
    - **[Input Form]** — 選取要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。

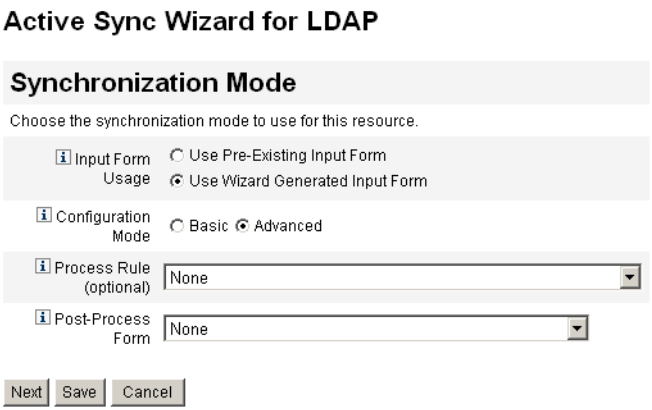
- **[Process Rule]** — 選擇性地選取要針對每個內送帳號執行的處理規則。此選擇將置換所有其他選項。如果您指定一個處理規則，則不論資源上的其他設定爲何，皆會針對每一列執行此處理程序。可以是程序名稱，也可以是評估程序名稱的規則。

圖 13-17 Active Sync 精靈：同步化模式，預先存在的表單選擇



- 如果選取 **[Use Wizard Generated Input Form]**，請對以下選項進行選取：
  - **[Configuration Mode]** — 選取在 Active Sync 精靈內使用基本模式，還是使用進階模式。預設選項是基本模式。如果選取進階模式，則可以定義事件類型及設定處理規則。
  - **[Process Rule]** — (只隨進階配置模式顯示。) 選擇性地選取要針對每個內送帳號執行的處理規則。此選擇將置換所有其他選項。如果您指定一個處理規則，則不論資源上的其他設定爲何，皆會針對每一列執行此處理程序。可以是程序名稱，也可以是評估程序名稱的規則。
  - **[Post-Process Form]** — (只隨進階配置模式顯示。) 選擇性地選取除執行由 Active Sync 精靈產生的表單外，也要執行的表單。此表單會置換來自 Active Sync 精靈的任何設定。

圖 13-18 Active Sync 精靈：同步化模式，精靈產生的表單選擇



按 **[Next]** 繼續執行精靈。[Active Sync Running Settings] 頁面隨即出現。

執行設定

此頁面可讓您爲使用中的同步化建立以下設定：

- 啓動
- 輪詢
- 記錄

啟動設定

從以下選項中選取用於 Active Sync 啓動的選項：

- **[Startup Type]** — 選取以下任一選項：
  - **[Automatic] 或 [Automatic with failover]** — 當 Identity 系統啓動時，啓動授權來源。
  - **[Manual]** — 需要管理員啓動授權來源。
  - **[Disabled]** — 停用資源。
- **[Proxy Administrator]** — 選取負責處理更新的管理員。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。

輪詢設定

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：

- 在 2005 年 7 月 18 日 (週二) 配置資源的「使用中的同步化」
- 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 日開始輪詢 (下個週一)。

如果未指定開始日期或時間，則資源會立即輪詢。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。

選擇如何設定輪詢：

- **[Poll Every]** — 指定輪詢的頻率。輸入數字，然後選取時間單位 (日、小時、分鐘、月、秒或週)。預設單位是分鐘。
- **[Polling Start Date]** — 輸入第一個排定間隔的開始日期 (格式爲 yyyyMMdd)。
- **[Polling Start Time]** — 輸入第一個排定間隔開始的當天時間 (格式爲 `HH:mm:ss`)。

記錄設定

從以下選項中進行選取以設定記錄資訊及層級：

- **[Maximum Log Archives]** — 如果此值大於零，將會保留最近的 N 個記錄檔案。如果此值爲零，將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。
- **[Maximum Active Log Age]** — 超過此段期間之後，將歸檔現用的記錄。如果時間爲零，則不會執行定期封存。如果 [Maximum Log Archives] 爲零，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。此有效期間標準的評估與 [Maximum Log File Size] 中所指定的標準無關。

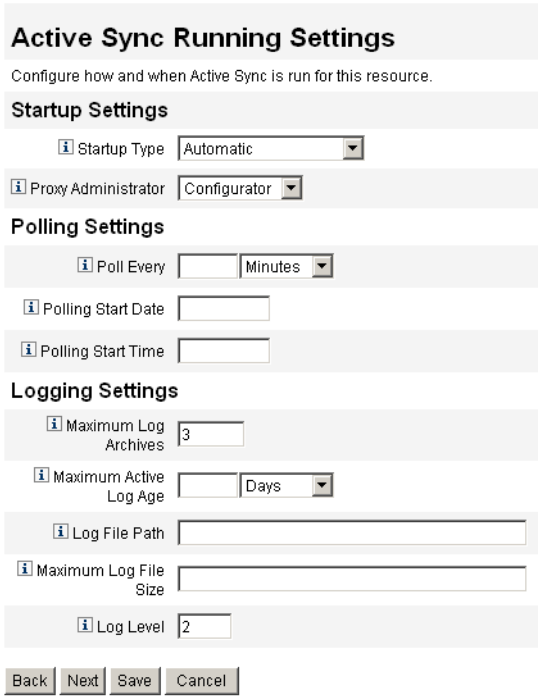
輸入數字，然後選取時間單位 (日、小時、分鐘、月、秒或週)。預設單位是日。

- **[Log File Path]** — 輸入要在其中建立使用中記錄檔案與歸檔記錄檔案的目錄路徑。記錄檔案名稱的開頭將會是資源名稱。
- **[Maximum Log file Size]** — 以位元組爲單位輸入現用記錄檔案的最大值。當現用記錄檔案達到最大限制時，就會被封存起來。如果 [Maximum Log Archives] 爲零，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。此大小標準的評估與 [Maximum Active Log Age] 中所指定的有效期間標準無關。

- **[Log Level]** — 輸入記錄的層級：
  - 0 — 不記錄
  - 1 — 錯誤
  - 2 — 資訊
  - 3 — 詳細的
  - 4 — 除錯

圖 13-19 是 [Running Settings] 頁面的視圖範例。

圖 13-19 Active Sync 精靈：執行設定



按 **[Next]** 繼續執行精靈。[General Active Sync Settings] 頁面隨即出現。

一般 Active Sync 設定

使用此頁面指定一般使用中的同步化配置參數。

資源特定設定

可用的資源特定設定因資源類型而異。例如，對於 LDAP 資源，以下設定可能適用。.

- **[Object Classes to Synchronize]** — 輸入要同步的物件類別。變更記錄是針對所有物件，而此項功能會篩選只列出物件類別的更新。
- **[LDAP Filter for Accounts to Synchronize]** — 輸入要同步之物件的選擇性 LDAP 篩選器。變更記錄是針對所有物件，所以此篩選器只會更新符合所指定篩選器的物件。指定了篩選器，則只有在符合篩選器且包括已同步的物件類別時，才會同步物件。
- **[Attributes to synchronize]** — 輸入要同步的屬性名稱。如果變更記錄中的更新並沒有更新任何已命名的屬性，則會忽略這些更新。比如，如果只有列出部門，則只會處理影響部門的變更。其他變更則略過。若爲空白 (預設值)，將會處理所有變更。
- **[Change Log Blocksize]** — 輸入每次查詢時擷取的變更記錄項目的數目。預設數目是 100。
- **[Change Number Attribute Name]** — 在變更記錄項目中輸入變更數字屬性的名稱。
- **[Filter Changes By]** — 輸入要從變更中篩選出來的目錄管理員名稱 (RDN)。將篩選出符合此清單中項目的 `modifiersname` 屬性變更。

標準值是此配接器爲避免迴圈而使用的管理員名稱。項目的格式應該爲 `cn=Directory Manager`。

常用設定

- **[Correlation Rule]** — 選擇性地指定相互關聯規則，以置換資源調解策略中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。
- **[Confirmation Rule]** — 選擇性地指定確認規則，以置換資源調解策略中指定的確認規則。
- **[Resolve Process Rule]** — 選擇性地指定當輸入之記錄有多個相符項目時所要執行的作業定義名稱。此處理過程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。
- **[Delete Rule]** — 選擇性地指定規則，而該規則會在評估每個內送使用者更新之後傳回 true 或 false，以確定是否要執行刪除作業。
- **[Create Unmatched Accounts]** — 爲 true 時，配接器將嘗試建立 Identity 系統中找不到的帳號。爲 false 時，配接器會根據 [Resolve Process Rule] 傳回的處理程序來對帳號執行動作。

- **[Assign Active Sync resource on create events]** — 選取此選項後，Active Sync 來源資源將指定給偵測到建立事件時建立的使用者。
- **[Populate Global]** — ActiveSync 名稱空間下的表單，一律可使用內送帳號中的所有屬性。若選取此選項，則全域名稱空間上也可使用所有屬性 (accountId 除外)。
- **[When reset, ignore past changes]** — 當首次啓動配接器或對其進行重設時，選取忽略過去的變更。若要重設配接器，請編輯 XmlData 物件 SYNC_resourceName 以移除同步化程序所需的 MapEntry，例如 ActiveSync。並非所有配接器都可以使用此選項。
- **[Pre-Poll Workflow]** — 選取要在每個輪詢前立即執行的選擇性工作流程。
- **[Post-Poll Workflow]** — 選取要在每個輪詢後立即執行的選擇性工作流程。

按 **[Save]** 或 **[Next]**，以儲存資源的一般設定變更：

- 如果您正在使用預先存在的輸入表單，請按一下 **[Save]**，以完成精靈選取並回到 [Resources] 清單。
- 如果您正在使用由精靈產生的輸入表單，請按 **[Next]** 繼續。
    - 如果您正在使用 *[basic]* 配置模式，則會顯示 [Target Resources] 頁面。(在本章節中直接跳至第 457 頁的「目標資源」。)
    - 如果您正在使用 *[advanced]* 配置模式，則會顯示 [Event Types] 頁面。

事件類型

使用此頁面配置一個機制，以確定在 Active Sync 資源上是否發生了某個類型的變更事件。

關於事件

使用中的同步化事件定義爲在 Active Sync 資源上發生的變更。針對每個資源列出的事件類型視變更事件所影響之資源及物件的類型而定。有些事件類型是建立、刪除、更新、停用、啓用及重新命名。

忽略事件

您可以選取一個機制，確定是否要忽略 Active Sync 事件。選項如下：

- **[None]** — 不忽略任何 Active Sync 事件。
- **[Rule]** — 使用規則來確定是否要忽略 Active Sync 事件。如果選取此選項，您必須同時從選項清單選取規則。
- **[Condition]** — 使用條件來確定是否要忽略 Active Sync 事件。在選取此選項之後，請按一下 [Edit Condition] 以使用 [Condition Panel] 定義條件。

用於確定事件類型的選項如下：

- **[None]** — 沒有用於確定事件類型的方法。
- **[Rule]** — 使用規則來確定事件類型。如果選取此選項，您必須同時從選項清單選取規則。
- **[Condition]** — 使用條件來確定事件類型。在選取此選項之後，請按一下 [Edit Condition] 以使用 [Condition Panel] 定義條件。

按 **[Next]** 繼續執行精靈。[Process Selection] 頁面隨即出現。

程序選擇

使用此頁面，設定當爲特定 Active Sync 事件實例或 Active Sync 事件類型移入使用者檢視時要執行的工作流程或程序。

程序模式

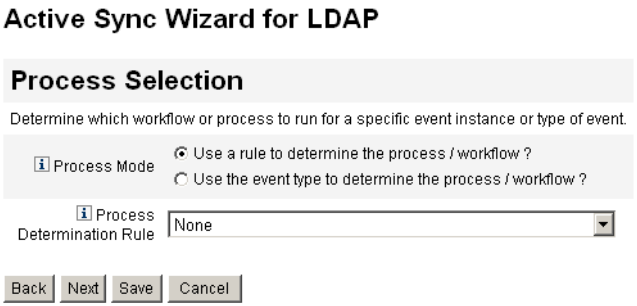
您可以從兩個模式中選取，以確定發生 Active Sync 事件時要執行的工作流程或程序：

- **[Rule]** — 您可以使用特定規則決定將對每個 Active Sync 事件實例執行何種工作流程或程序。這表示每次發生事件時都將執行規則。

  在選取此選項之後，從清單中選取規則 (程序確定規則)。

  圖 13-20 圖解您指定規則時所用的 [Process Selection] 頁面。

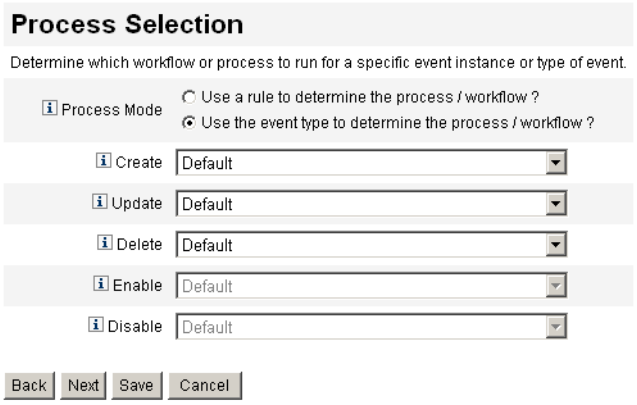
  圖 13-20 Active Sync 精靈：程序選擇 (規則)

- **[Event Type]** — 您可以根據每個事件實例的事件類型來執行工作流程或程序。這是預設選擇。

  選取此選項之後，選取要對所列每種事件類型執行的工作流程或程序，如圖 13-21 所示。

圖 13-21 Active Sync 精靈：程序選擇 (事件類型)

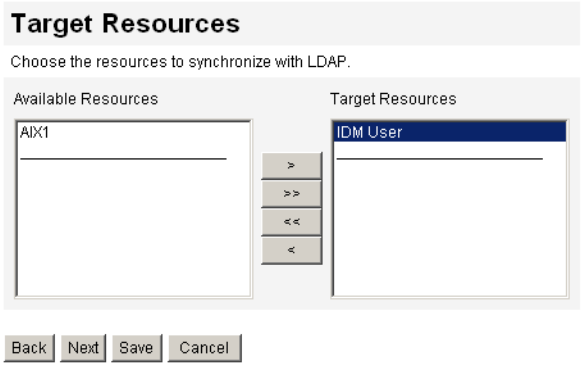


按 **[Next]** 繼續執行精靈。[Target Resources] 頁面隨即出現。

目標資源

使用此頁面指定要與此資源同步的目標資源。

圖 13-22 Active Sync 精靈：目標資源

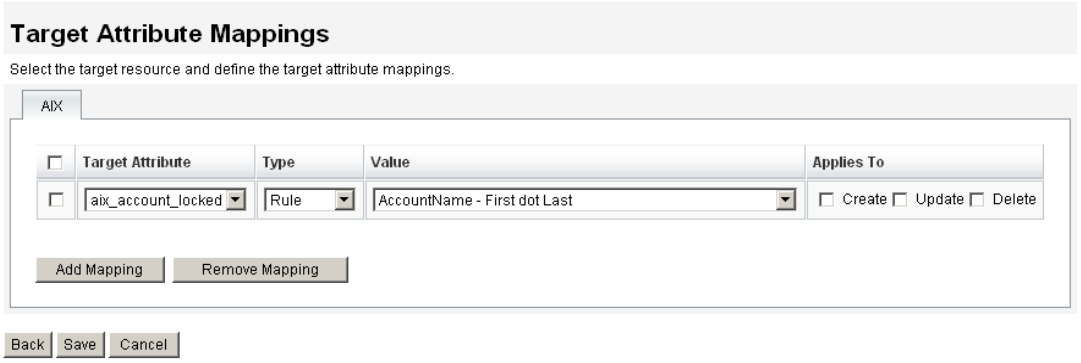


1. 從 [Available Resources] 區域中選取一或多個資源，然後將它們移至 [Target Resources] 區域。
2. 按 **[Next]** 以繼續。[Attribute Mappings] 頁面隨即出現。

目標屬性對映

使用此頁面定義每個目標資源的目標屬性對映。

圖 13-23 Active Sync 精靈：目標屬性對映



1. 從選項清單中選取目標資源。若要新增目標屬性至清單，請按一下 **[Add Mapping]**。
2. 爲每個目標屬性選取屬性、類型及屬性值。
3. 在 [Applies To] 欄位中，選取一或多個將套用對映的動作 (建立、更新或刪除)。
4. 繼續爲每個目標資源選取選項。

若要從清單中移除屬性，請選取列，再按一下 **[Remove Mapping]**。

按一下 **[Save]** 儲存屬性對映並回到 [Resources] 清單。

索引

符號

英文

三畫

四畫

五畫

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

二十畫以上

二十畫以上