Sun Java™ System

Identity Manager 6.0 2005Q4M3
管理指南

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

文件號碼：819-5521

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。

如何在本指南中尋找資訊

本指南分為以下章節：

- 第 1 章 *Identity Manager* **簡介** — 提供有關 Identity Manager 產品和物件的高階資訊。
- 第 2 章 *Identity Manager* **入門** — 介紹 Identity Manager 介面並引導您完成基本的 Identity Manager 作業。
- 第 3 章**使用者和帳號管理** — 詳細說明使用者管理概念和作業。
- 第 4 章**管理指南** — 討論委託管理並提供使用 Identity Manager 管理員、組織和虛擬組織的程序。
- 第 5 章**配置** — 提供有關配置 Identity Manager 物件 (例如角色、資源、策略、權能和管理員角色) 的附加資訊和程序。
- 第 6 章**資料同步化與載入** — 討論用於同步化資料和載入使用者群組的 Identity Manager 工具。
- 第 7 章**安全性** — 說明 Identity Manager 安全功能並提供使用 Identity Manager 的最佳實踐建議。
- 第 8 章**報告** — 詳細說明 Identity Manager 系統的完整服務報告和風險分析功能。
- 第 9 章**作業範本** — 說明如何使用管理員介面來配置特定工作流程運作方式，以此做為編寫自訂工作流程的替代方法。
- 第 10 章 *PasswordSync* — 說明 PasswordSync 功能，此功能可讓 Windows 系統安全地變更和重設使用者密碼，並透過 Identity Manager 對其進行同步化。

相關文件與說明

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 安裝

  逐步說明與參照資訊可協助您升級與配置 Identity Manager 和相關軟體。

- Identity Manager 管理

  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的程序、指導和範例。

- Identity Manager Technical Deployment 簡介

  Identity Manager 產品 (包括物件架構) 的概念性簡介以及對基本產品元件的介紹。

- Identity Manager 工作流程、表單與視圖

  說明如何使用 Identity Manager 工作流程、表單和視圖 (包括有關自訂這些物件所需工具的資訊) 的參照資訊和程序資訊。

- Identity Manager 部署工具

  說明如何使用不同 Identity Manager 部署工具的參照資訊和程序資訊，包括規則和規則程式庫、普通作業和程序、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 資源參照

  說明如何將資源的帳號資訊載入 Identity Manager 並使其同步化的參照資訊和程序資訊。

- Identity Manager 稽核記錄

  說明如何將資源的帳號資訊載入 Identity Manager 並使其同步化的參照資訊和程序資訊。

- Identity Manager 調校、疑難排解與錯誤訊息

  說明 Identity Manager 錯誤訊息和異常並為追蹤和疑難排解工作中可能遇到的問題提供指示的參照資訊和程序資訊。

- Identity Manager 說明

  提供有關 Identity Manager 的完整程序、參照和術語資訊的線上指南與資訊。按一下 Identity Manager 功能表列中的 [Help] 連結即可存取說明。您可以在關鍵欄位上找到相關指示 (欄位特定資訊)。

產品支援

如果在部署或使用 Identity Manager 時遇到問題，請使用以下機制之一與用戶支援聯絡：

- 線上支援網站：http://www.sun.com/service/online/us

- 與維護合約有關的電話分派號碼

我們很樂意收到您的回應！

我們想瞭解您對隨 Identity Manager 一併提供的本指南及其他說明文件的看法。如果您要回饋關於使用本產品和文件的體驗 (無論是正面的還是負面的)，請給我們來信。

Sun Microsystems.
5300 Riata Park Court
Austin, TX 78727
Attn:Identity Manager Information Development

電子郵件：idm-idd@sun.com

目錄

目錄

使用者和帳號管理

管理指南

配置

資料同步化與載入

安全性

報告

作業範本

PasswordSync

lh 參照

線上文件進階搜尋

1 Identity Manager 簡介

Sun Java™ System Identity Manager 系統可以讓您安全並有效地管理帳號與資源的存取。Identity Manager 可提供讓您快速處理定期與每日工作所需之權能與工具，為內部與外部客戶提供卓越的服務。

概述

今日的企業需要 IT 服務為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。

由於此類與日俱增的需求可能產生龐大的管理費用。身為管理員，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。

我們特別開發出 Identity Manager 以協助您在動態的環境中處理這些管理方面的挑戰。在使用 Identity Manager 以分配存取管理費用之後，面對主要挑戰時您將有一套完整的解決方案：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？

一套安全卻又極具靈活性的設計可以讓您根據您企業結構設定 Identity Manager，以面對上述挑戰。藉由將 Identity Manager 物件對映至您管理的實體 (使用者與資源)，您將可以大幅提昇您的作業效率。

Identity Manager 系統的目標

Identity Manager 解決方案可以讓您：

- 對廣泛的系統與資源之帳號存取進行管理。
- 為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內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。擁有 Identity Manager 之後，您即擁有完整的整合功能，可授予、管理與撤銷內部與外部組織中的存取特權。
- 借由**不**保留資料的方式保持資料同步。Identity Manager 解決方案支援上級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
  - 產品不應該因為新增其他需要管理的資源而增加企業的複雜性。

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，使用者是以**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 專用術語中，這些內容即為**資源**。

因為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。

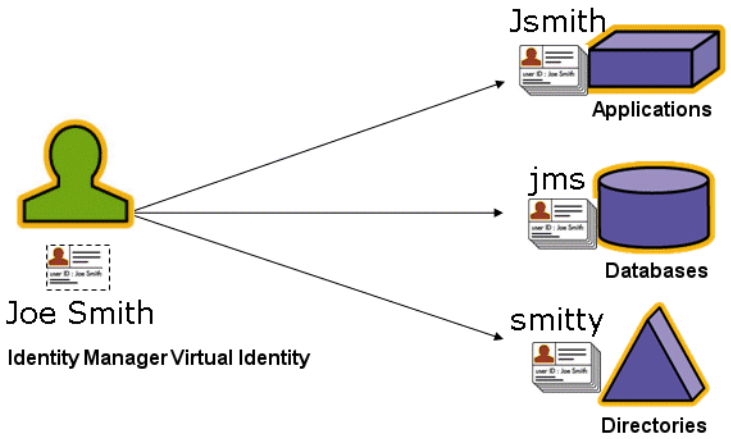


圖 1. Identity Manager 使用者帳號與資源的關係

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。在多數的公司中，使用者按職能機關或部門分組。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 專用術語中，此種群組類型即稱為**組織**。

將使用者分組的另一種方式則是依照類似的特性分類，例如公司關係或職務類別。Identity Manager 將這些群組識別為**角色**。

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

Identity Manager 使用者也直接或間接透過應用**策略**進行管理，策略可設定規則、密碼和使用者驗證選項。

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，您就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。擁有這些更多權限的使用者稱為 Identity Manager **管理員**。

但是委派只有在安全模式中才可運作。為了維持適當的控制層級，Identity Manager 讓您能夠將不同的**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，並且可以追蹤其進度。如需有關工作流程的詳細資訊，請參閱「 Identity Manager 工作流程、表單與視圖」。

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管理與系統部署非常重要。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
- 權能
- 管理員角色

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。
- 為組織的一部份，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為動態的。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特權。Identity Manager 管理員負責管理組織，並指定應用於每個受管理組織中物件的權能範圍。

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。您可以將一個或多個角色指定給每位使用者，或是不指定角色。

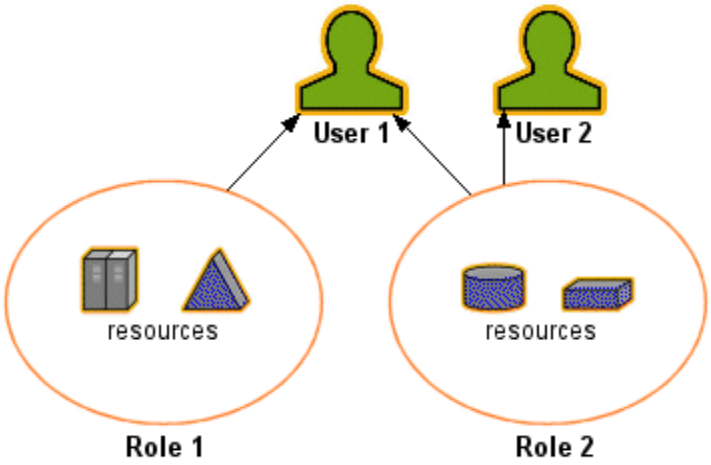


圖 2. 使用者帳號，角色，資源關係

如上圖所示，使用者 1 和使用者 2 藉由被指定為角色 2 而共同存取相同資源。而使用者 1 還可藉由被指定為角色 1 而存取額外資源。

資源與資源群組

Identity Manager 資源會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™)
- 訊息平台 (例如 Microsoft® Exchange)

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範本)
- Identity Manager 參數

Identity Manager 使用者帳號透過以下途徑獲取資源存取：

- 以角色為基礎指定 — 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。

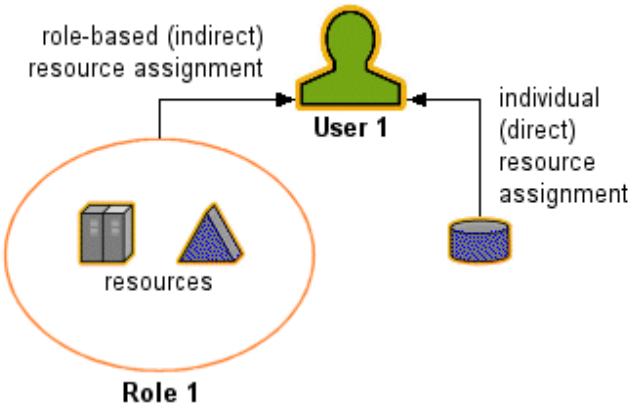


圖 3. 指定資源

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。

組織

組織是用來啟用管理委託的 Identity Manager 容器。它們會定義 Identity Manager 管理員所控制或管理的實體範圍。

組織也可表示與以目錄為基礎的資源的直接連結；這些組織稱為**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。藉由透過虛擬組織鏡像現有目錄結構與成員資格，Identity Manager 可消除重複且耗時的設定步驟。

包含其他組織的組織為**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。

權能

可給每位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執行系統中的特定工作，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，可用於常規的管理功能。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，您可以為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，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。

Object Relationships

下表為 Identity Manager 物件及其相互關係的簡要介紹。

Identity Manager 物件	它是什麼？	它適用於何處？
使用者帳號	Identity Manager 和一個或多個資源的帳號。 使用者資料可從資源載入到 Identity Manager 中。 擁有更多權限的特殊的使用者類別，Identity Manager 管理員。	**角色** 通常，每個使用者帳號都指定給一個或多個角色。 **組織** 使用者帳號作為組織的一部分安排在階層中。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** 會給管理員指定他們所管理組織的權能。
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。	**資源和資源群組** 資源和資源群組會指定給角色。 **使用者帳號** 角色群組具有類似特性的使用者帳號。 **角色** 定義與其他角色之間的關係 (包含或排除)。
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。
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角色指定來「繼承」資源存取權。 **使用者帳號** 資源群組可直接指定給使用者帳號。

Identity Manager 物件	它是什麼？	它適用於何處？
組織	定義管理員所管理實體的範圍；具有階層性。	**資源** 給定組織中的管理員可存取某些資源或所有資源。 **管理員** 組織由具有管理特權的使用者管理 (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** 每個使用者帳號可以指定給一個 Identity Manager 組織以及一個或多個目錄組織。
管理員角色	為指定給管理員的每組組織定義一組唯一的權能。	**管理員** 管理員角色指定給管理員。 **權能和組織** 權能和組織會直接或間接 (動態) 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。

表 1. Identity Manager 物件關係

Identity Manager 專用術語

Identity Manager 介面與指南定義這些專用術語如下：

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 (如建立使用者和管理資源的存取權) 的人員。

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。

業務程序編輯器 (BPE)

Identity Manager 表單、規則和工作流程的圖形檢視。

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 內部的低層級存取權控制。

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。

身份範本

定義使用者的資源帳號名稱。

組織

用來啟用管理委託的 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「適用環境」上下文，主要用於 Identity Manager 的管理作業。

策略

Identity Manager 帳號的建立限制。*Identity Manager* **策略**可建立使用者、密碼和驗證選項，並繫結到組織或使用者。**資源密碼**和**帳號** *ID* 策略設定規則、允許的文字和屬性值，並繫結到個別資源。

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。

資源配接卡

提供 Identity Manager 引擎與資源之間的連結的 Identity Manager 元件。此元件可讓 Identity Manager 管理指定資源上的使用者帳號 (包括建立、更新、刪除、驗證及掃描功能)，以及利用該資源來通過驗證。

資源配接卡帳號

Identity Manager 資源配接卡用來存取受控資源的憑證。

資源群組

為資源集合，可發出建立、刪除及更新使用者資源帳號的命令。

資源精靈

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、身份範本和 Identity Manager 參數。

角色

Identity Manager 中某類使用者之範本或設定檔。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

資源帳號屬性到資源的 Identity Manager 帳號屬性的對映。Identity Manager 帳號屬性可建立到多個資源的共用連結，並由表單參照。

使用者

擁有 Identity Manager 系統帳號的人員。使用者可擁有 Identity Manager 中的某些權能；擁有擴充權能的人即為 Identity Manager **管理員**。

使用者帳號

使用 Identity Manager 建立的帳號。參考 Identity Manager 帳號或 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。

工作流程

一個邏輯上的且可重複的進程，在此進程中，文件、資訊或工作在參與者之間傳送。Identity Manager 工作流程是由多個進程組成，這些程序可以控制使用者帳號的建立、更新、啟用、停用與刪除。

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。此處涵蓋的主題包括：

- Identity Manager 介面
- 說明與指導
- 您可以執行的工作以及應從何處著手

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
- 業務程序編輯器 (BPE)

Identity Manager 管理員介面

Identity Manager 管理介面可以作為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，以及定義 Identity Manager 系統中的權限與存取等級。

介面透過以下方式進行組織：

- **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。

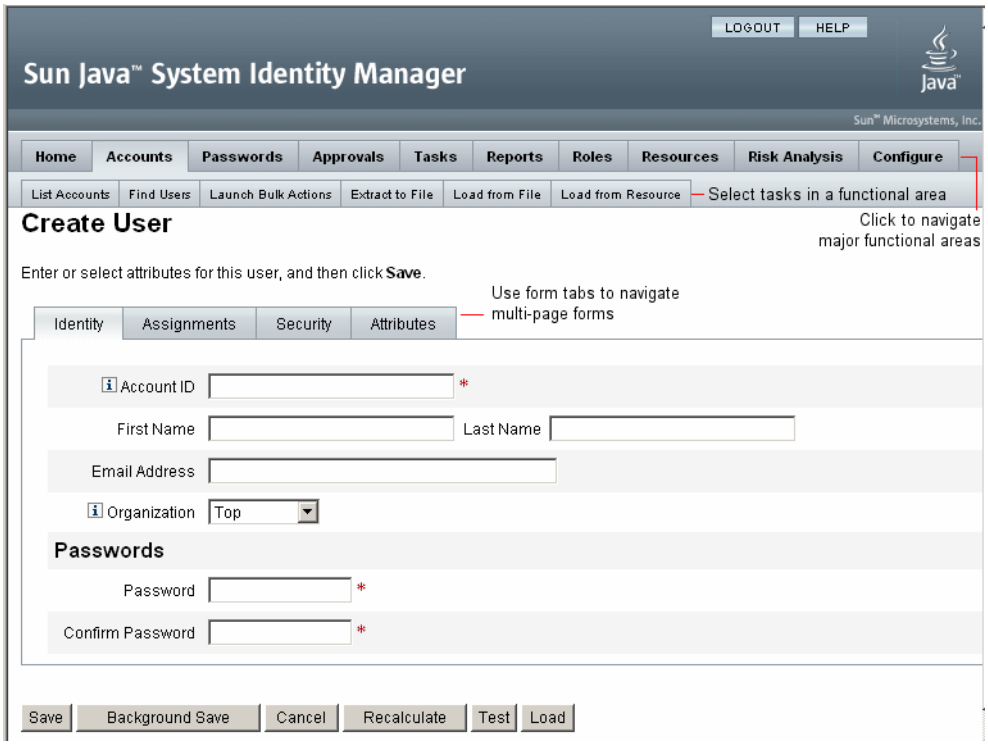


圖 1. Identity Manager 管理員介面

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。此視圖專為不具備管理權能的使用者而設計。

在使用者介面中，使用者可以：

- 變更其密碼
- 執行自我佈建工作
- 管理與其帳號有關的設定檔資訊

此介面經常可以透過自訂的方式來顯示公司專屬的特定視圖，並提供許多自訂選項。

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

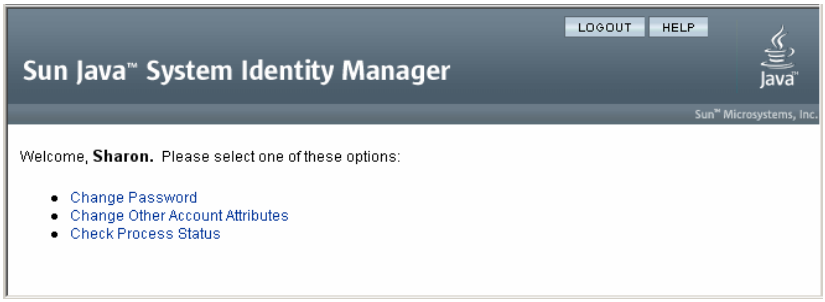


圖 2. Identity Manager 使用者介面

Identity Manager 業務程序編輯器

業務程序編輯器 (BPE) (也稱為「配置編輯器」) 提供了 Identity Manager 表單、規則與工作流程的圖形化視圖。您可以使用 BPE 建立與編輯一些表單，這些表單可以建立能夠用於每個 Identity Manager 頁面的功能。您也可以修改 Identity Manager **工作流程**。工作流程定義使用 Identity Manager 使用者帳號時所遵循的動作順序或者執行的工作。

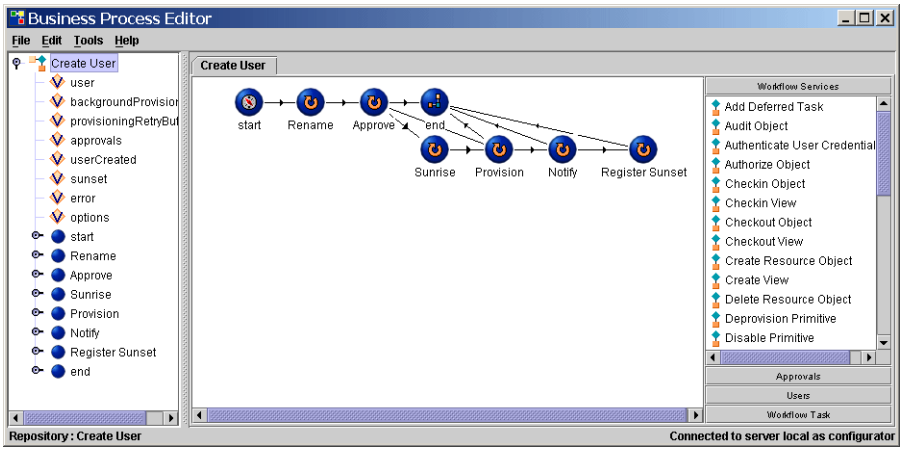


圖 3. 業務程序編輯器 (配置編輯器)

如需有關 BPE 以及將其用於 Identity Manager 工作流程的更多資訊，請參閱「Identity Manager 工作流程、表單與視圖」。

說明與指導

為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與使用者介面頁面的頂部。

圖 4. 說明

在每個 [Help] 視窗的底部為 [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。若要進行搜尋，請：

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。
   - **線上說明** — 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。
   - **文件**（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 **[搜尋]**。

搜尋將傳回連結的搜尋結果。使用 [Previous]/[Next] 或 [First]/[Last] 按鈕可以邊覽列出的結果。

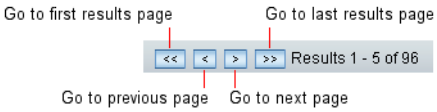


圖 5. 搜尋結果瀏覽

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，如果輸入以下內容進行搜尋：

```
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「**線上文件進階搜尋**」，以取得有關 Identity Manager 的進階文件搜尋功能的更多資訊。

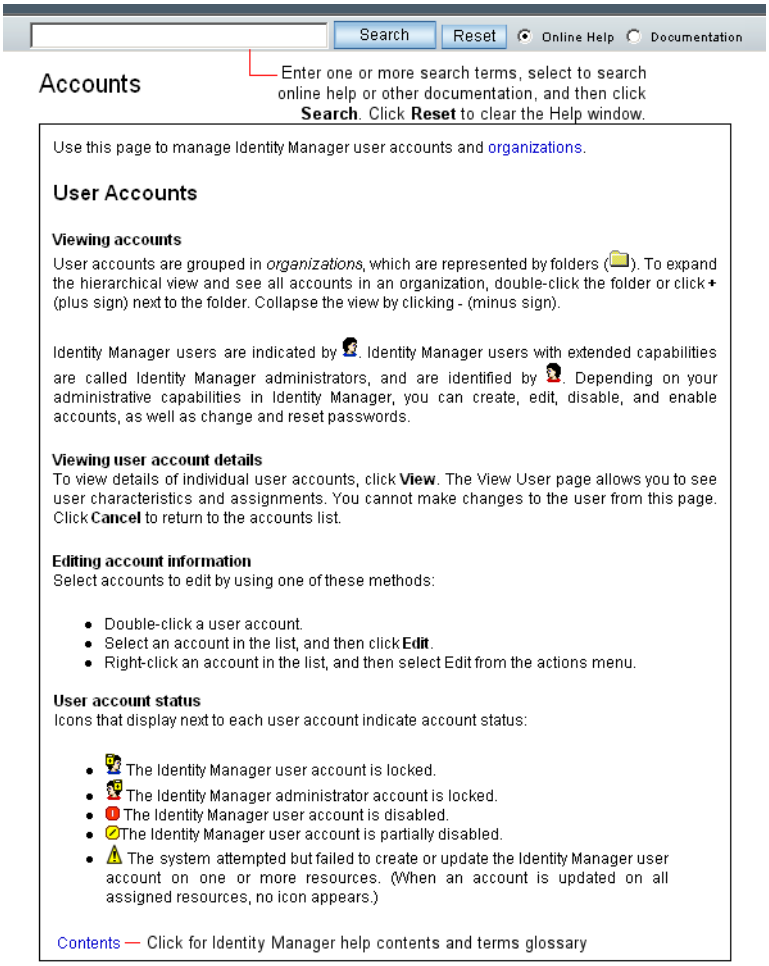


圖 6. Identity Manager Help

Identity Manager 指導

Identity Manager 指導為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：。按一下此圖示可開啟一個視窗並顯示與其關聯的資訊。

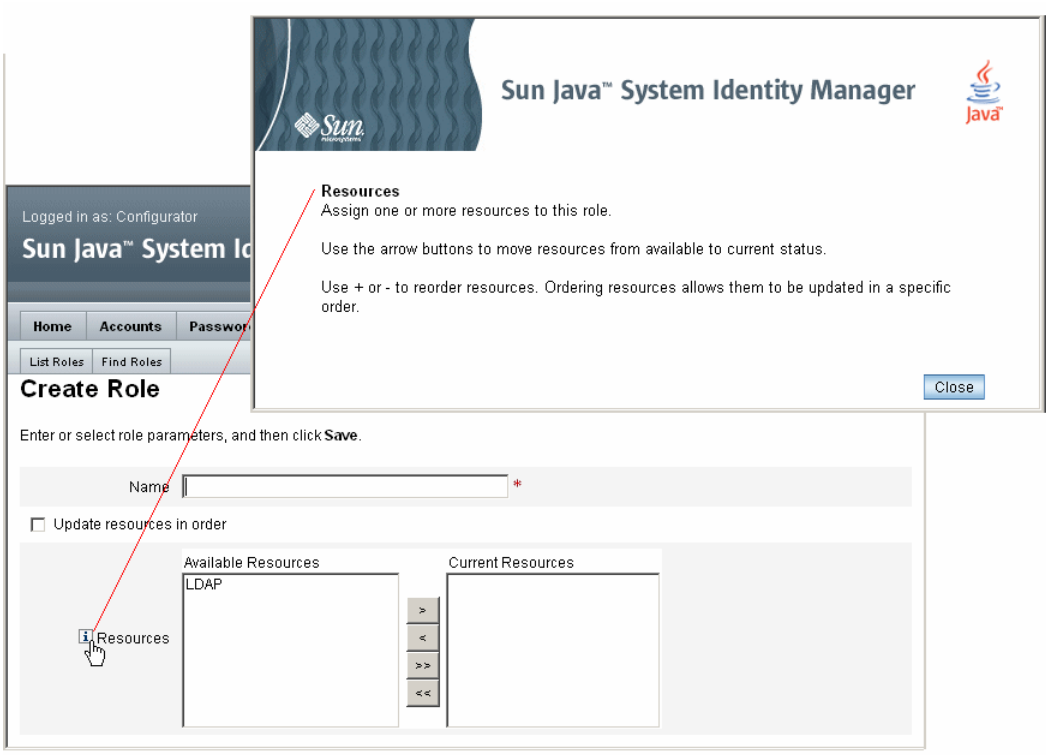


圖 7. Identity Manager 指導

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)。

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	**核准**標籤	
設定使用者驗證 (策略)	**[Configure]** 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] 頁面
指定權能 (透過管理員角色)	**[Accounts]** 標籤，**[List Accounts]** 選項，[Create User] 頁面
設定核准人 (以驗證帳號建立)	• **[Accounts]** 標籤，**[List Accounts]** 選項，[Create Organization] 頁面 • **角色**標籤，建立角色頁面
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)	**資源**標籤
管理資源群組	**[Resource]** 標籤，**[List Resource Groups]** 選項
建立與管理角色	**角色**標籤
尋找角色	**[Roles]** 標籤，**[Find Roles]** 選項
編輯權能	**[Configure]** 標籤，**[Capabilities]** 選項
建立與編輯管理員角色	**[Configure]** 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	**[Configure]** 標籤，**[Policies]** 選項
配置身份屬性	**[Configure]** 標籤，**[Identity Attributes]** 選項
配置變更記錄檔	**[Configure]** 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	**[Resources]** 標籤，**[Reconcile with Resources]** 選項	
稽核、風險分析與報告		
若要執行這個動作：	**移至：**	**若要執行這個動作：**
設定要擷取的稽核事件	**[Configure]** 標籤，**[Audit Events]** 選項	設定要擷取的稽核事件
執行與管理報告	**報告**標籤	執行與管理報告
定義與執行風險分析報告	**風險分析**標籤	定義與執行風險分析報告

表 1. Identity Manager 介面工作參照

下面要查看哪一個章節

熟悉 Identity Manager 介面以及尋找資訊的方法之後，您可能要重點瞭解以下主題之一。本指南中按章節介紹了這些主題：

- 第 3 章 . **使用者和帳號管理**
- 第 4 章 . **管理指南**
- 第 5 章 . **配置**
- 第 6 章 . **資料同步化與載入**
- 第 7 章 . **安全性**
- 第 8 章 . **報告**
- 第 9 章 . **作業範本**
- 第 10 章 . *PasswordSync*

下面要查看哪一個章節

3 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：

- 使用者帳號資料及其儲存方式
- Identity Manager 管理員介面的帳號區域
- 帳號建立與編輯權能，及其他與帳號相關的工作
- 使用者帳號搜尋功能
- 密碼策略與使用者帳號密碼
- 使用者自助
- 使用者認證
- 批次處理帳號動作

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 為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 將使用者資料劃分為四個區域：

- 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。

附註 如需有關設定帳號密碼策略的資訊，請閱讀本章中標題為「**設定密碼策略**」的小節。

下圖說明 [Create User] 頁面的 [Identity] 區域。

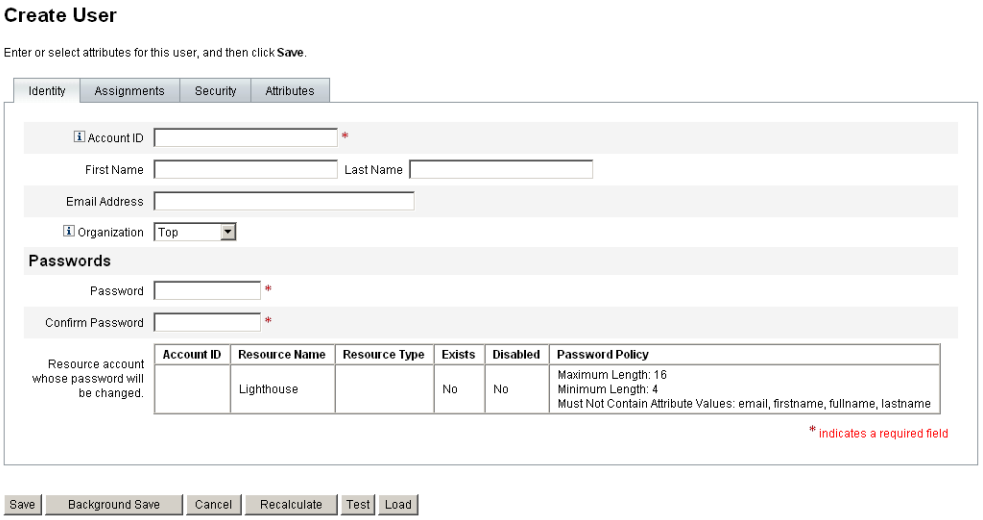


圖 1. 建立使用者 — 身份

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：

- **Identity Manager 帳號策略**指定 — 建立密碼和認證限制。
- **角色**指定 — 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。
- **資源和資源群組**存取 — 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，指定了擴充權能的使用者為 Identity Manager **管理員**。[Security] 區域透過指定以下項，為使用者建立這些擴充權能：

- **管理員角色** — 組合一組特定且唯一的權能和控制的組織，以對管理使用者實現協調指定。
- **權能** — 在 Identity Manager 系統中啟用權限。通常會根據工作責任，為每個 Identity Manager 管理員指定一項或多項權能。
- **控制的組織** — 指定該使用者有權以管理員身份管理的組織。他可以管理已指定組織及階層中處於該組織之下的任何組織中的物件。

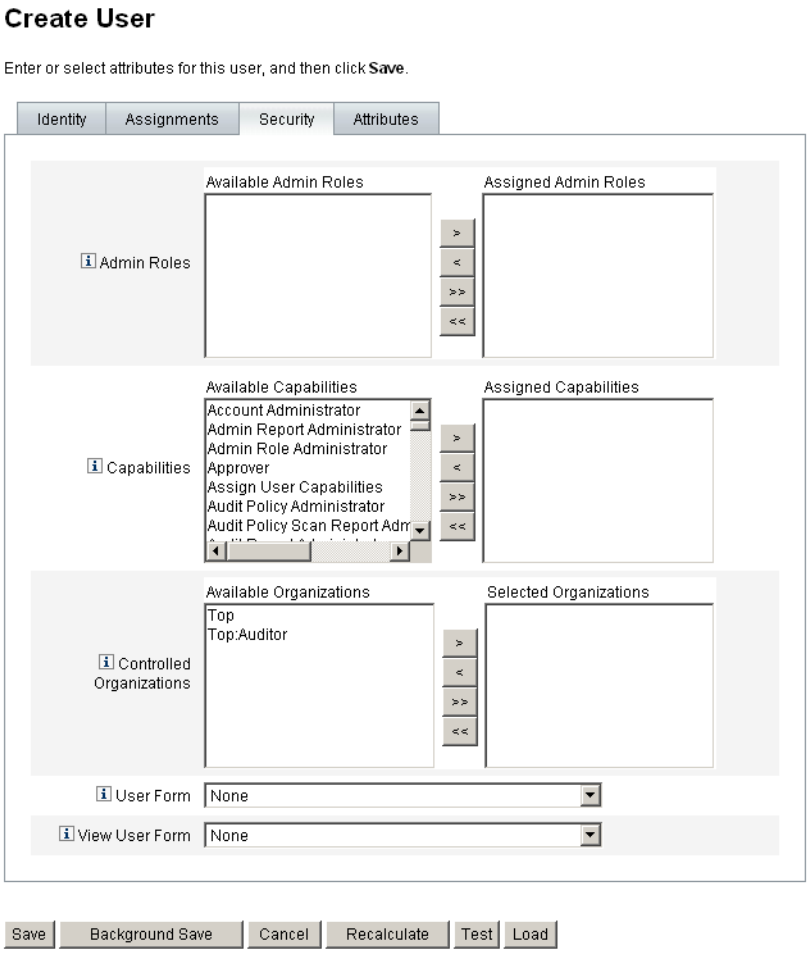


圖 2. 建立使用者 — 安全性

屬性

[Attributes] 區域定義與已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。

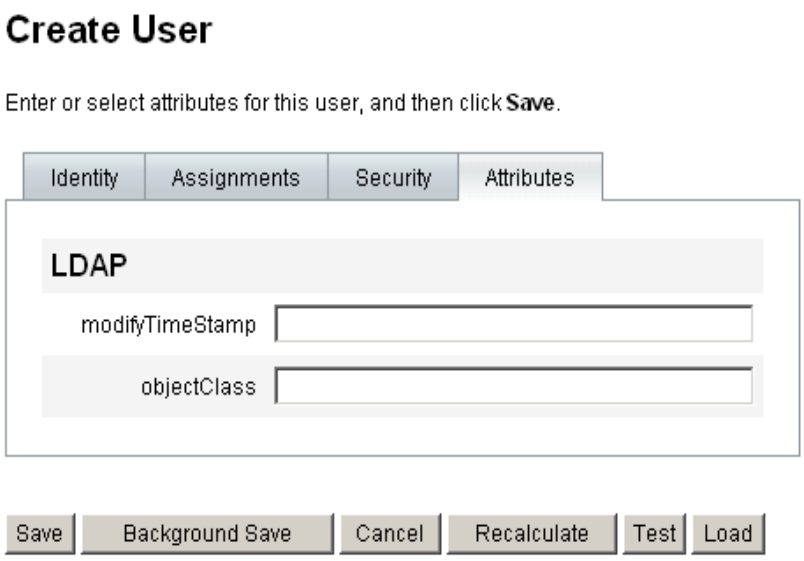


圖 3. 建立使用者 — 屬性

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，請在管理員介面中選取 **[Accounts]**。

帳號清單會顯示所有的 Identity Manager 使用者帳號。帳號會被分組為組織與虛擬組織，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。

附註 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。

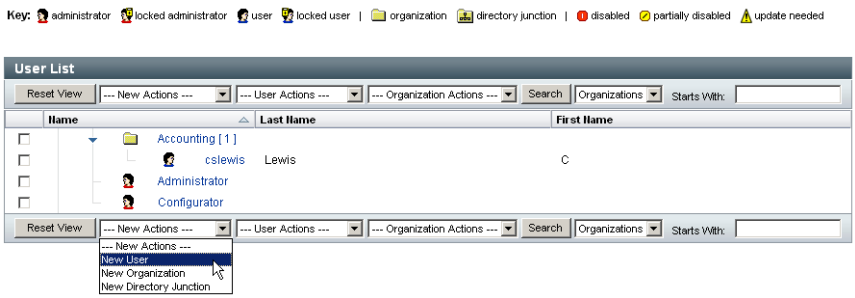


圖 4. 帳號清單

帳號區域中的動作清單

使用動作清單（位於帳號區域的頂部和底部）可以執行一系列動作。動作清單選項分為：

- **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、啟用、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。

在帳號區域中搜尋

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]，在搜尋區域中輸入一個或多個字元，然後按一下 **[Search]**。

使用者帳號狀態

顯示在每一位使用者帳號旁、指示已指定帳號的當前狀態的圖示：

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

從管理員介面的帳號區域，您可以對這些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、啟用、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** — 建立、編輯、更新和刪除
- **Directory Junctions** — 建立

使用者

檢視

若要檢視使用者帳號的詳細資訊，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 **[取消]** 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，請在 [New Actions] 清單中選取 [New User]。

提示 如果您要在組織中 (非頂部) 建立使用者，請選取組織資料夾，然後在 [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 Use] 頁面 (也稱為**使用者表單**) 是一個多頁表單，可讓您設定使用者的：

- **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
- **安全性** — 組織與權能
- **Attributes** — 已指定資源的特定屬性

附註 若要更好地反映業務程序或特定管理員權能，您可針對環境專門配置使用者表單。如需有關使用者表單的更多資訊，請參閱 Identity Manager 工作流程、表單與視圖。

按一下表單標籤可以瀏覽 [建立使用者] 頁面。您可以依任何順序在表單標籤中移動。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	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。

提示 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) 使用者並為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，請選擇其中一個動作：

- 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，然後在 [User Actions] 清單中選取 [Edit]。

建立與儲存變更後，Identity Manager 會顯示 [更新資源帳號] 頁面。此頁面顯示指定給使用者的資源帳號，以及將套用至帳號的變更。選取 [更新全部資源帳號] 將變更套用至已指定的全部資源；或個別選取無、一個、或多個與欲更新的使用者相關的資源帳號。

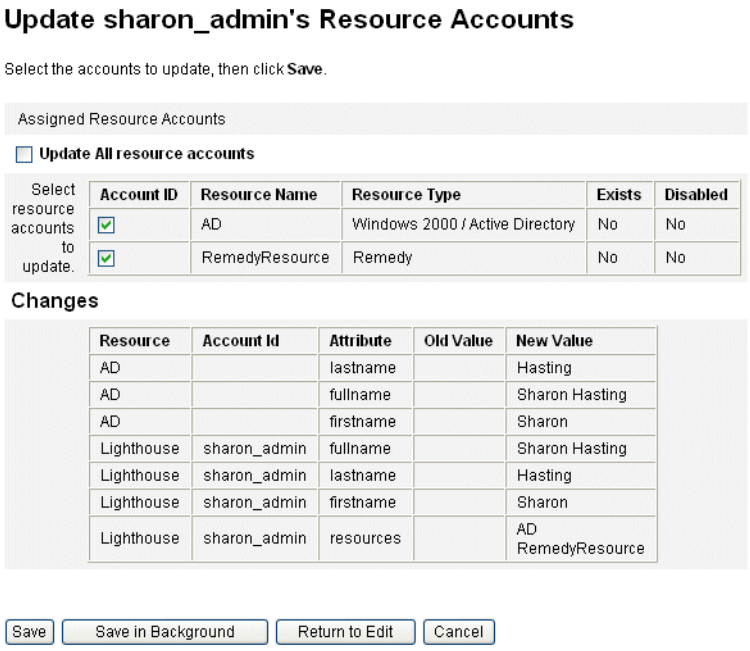


圖 5. 編輯使用者 (更新資源帳號)

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

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。

若要將使用者移動至其他組織，請在清單中選取一個或多個使用者帳號，然後在 [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。因為這個原因，Identity Manager 提供一個單獨功能，來重新命名使用者的 Identity Manager 帳號或者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，然後在 [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。

附註　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)

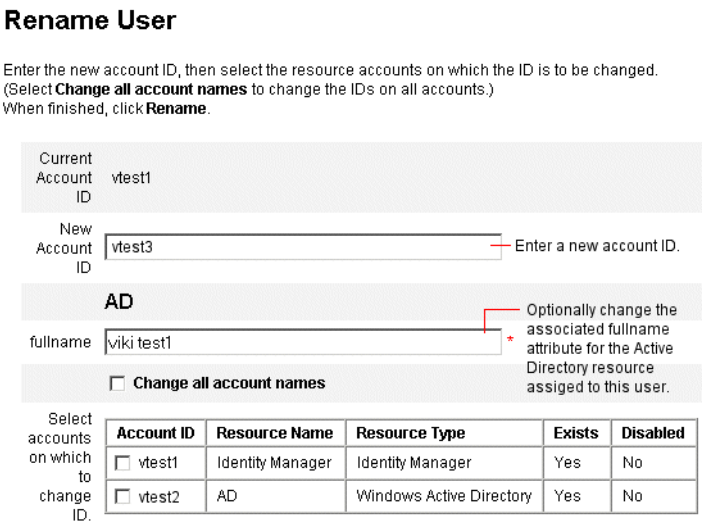


圖 6. 重新命名使用者

停用使用者 ([User Actions]、[Organization Actions])

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。

附註 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，然後在 [User Actions] 清單中選取 [Disable]。

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

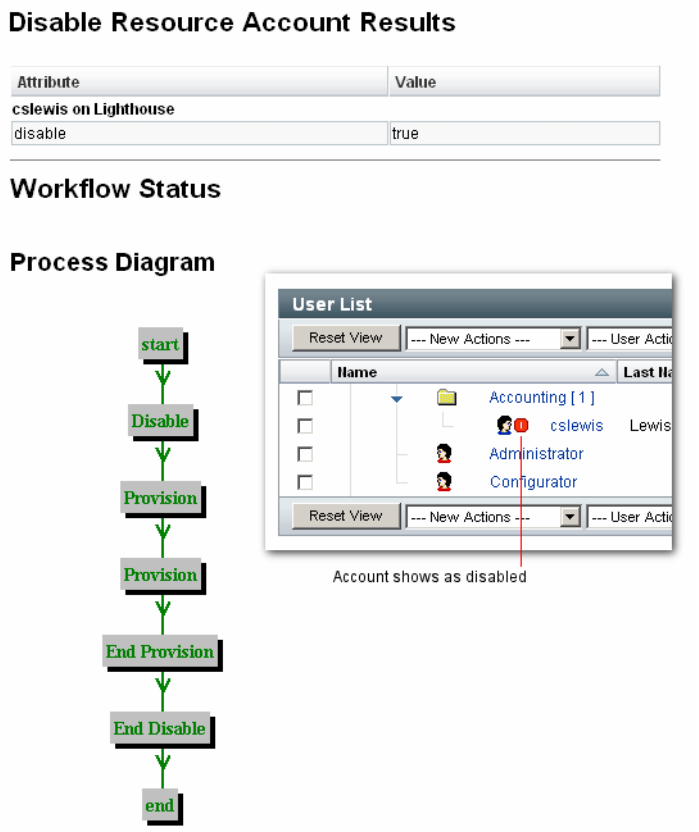


圖 7. 已停用的帳號

停用多個使用者帳號

您可以同時停用兩個或兩個以上 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 [Disable]。

附註 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])

使用者帳號啟用與停用程序相反。對於不支援帳號啟用的資源，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

若要啟用使用者帳號，請在清單中選取此帳號，然後在 [User Actions] 清單中選取 [Enable]。

在顯示的 [啟用] 頁面上，選取要啟用的資源，然後按一下**確定**。Identity Manager 顯示啟用 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

您可以同時啟用兩個或多個 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]。

附註 當您選擇啟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。此程序會啟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為使用者建立的擱置變更傳送至選取的資源。這個情況會在以下狀態發生：

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

當您更新使用者帳號時，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，然後在 [User Actions] 清單中選取 [Update]。

在 [Update Resource Accounts] 頁面中，選取一個或多個要更新的資源，或者選取 [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]** 以作為背景程序執行該動作。

確認頁面會確認送至每個資源的資料。

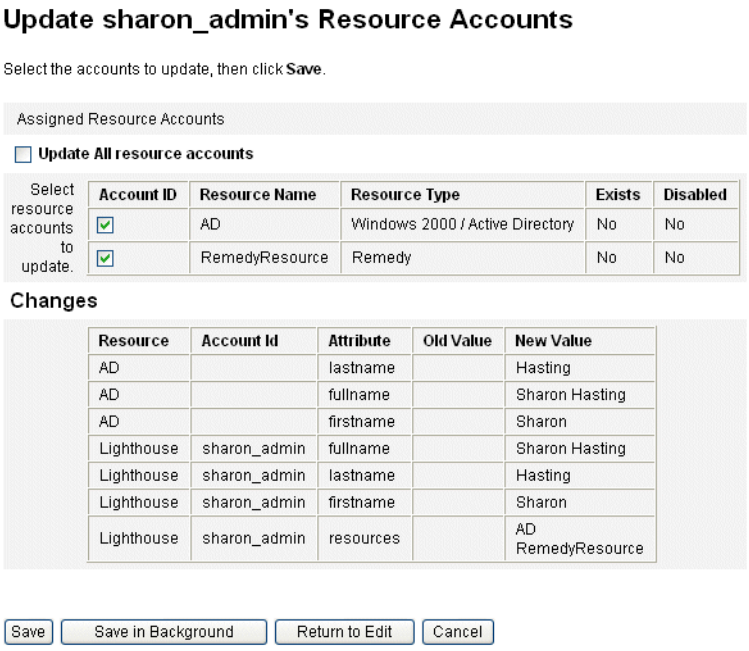


圖 8. 更新資源帳號

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，然後在 [User Actions] 清單中選取 [Update]。

附註 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])

因為使用者登入重試次數已超過為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，將不允許他對任何 Identity Manager 應用程式介面 (包括使用者介面、管理員介面、Forgot My Password、BPE、SOAP 和主控台) 進行認證。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：

- 管理使用者為其解除鎖定。若要成功解除鎖定帳戶，必須為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，使用者帳號將保持鎖定狀態，直到：

- 管理使用者為其解除鎖定。若要成功解除鎖定帳戶，必須為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
- 停用或啟用
- 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 BPE)。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 ([User Actions]、[Organization Actions])

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。

附註 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 [刪除資源帳號] 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 [刪除] 欄位中進行選取，然後按一下**確定**。若要刪除全部資源帳號，請選取 [刪除全部資源帳號] 選項，然後按一下**確定**。

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 [取消指定] 或 [解除連結] 欄位中進行個別選擇，然後按一下**確定**。若要取消指定全部資源帳號，請選取 [取消指定全部資源帳號] 或 [解除連結全部資源帳號] 選項，然後按一下**確定**。

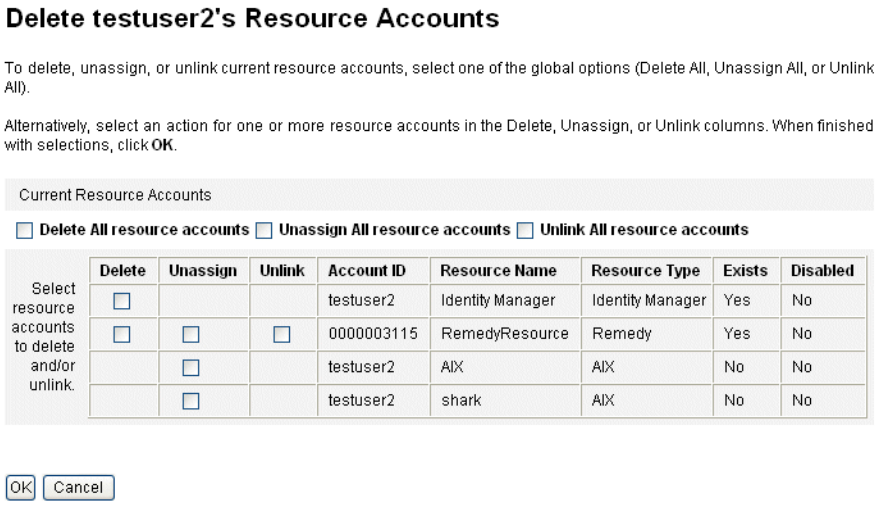


圖 9. 刪除 「使用者帳號」與 「資源帳號」

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。
- 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 (例如啟用、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。

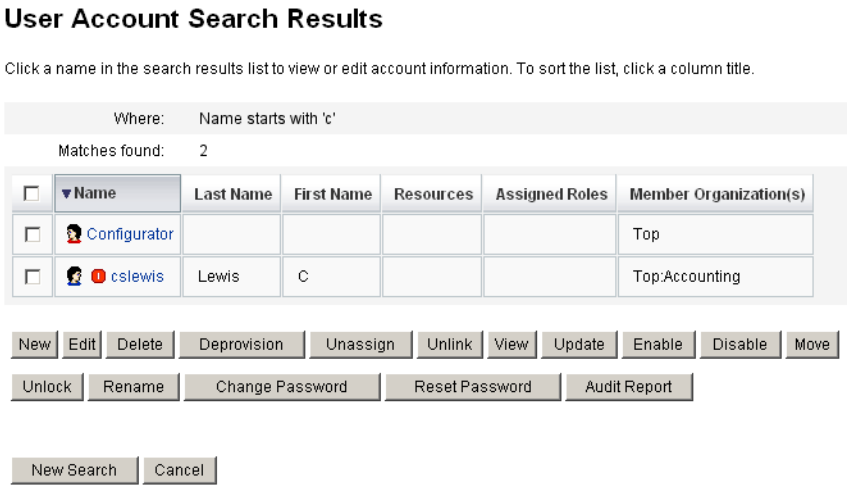


圖 10. 使用者帳號搜尋結果

設定密碼策略

資源密碼策略可用於建立密碼限制。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 **[Configure]**，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。為新策略命名並提供選擇性說明後，您需要為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。請進行選取以啟用規則，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為該類型。

字元類型規則的最少字元數

您也可以設定必須通過驗證的字元類型規則的最少數目。必須通過的最小數目為 1。而最大數目不可超過您已啟用的字元類型規則數目。

提示　若要將必須通過的最少數目設定為最高值，請輸入「全部」。

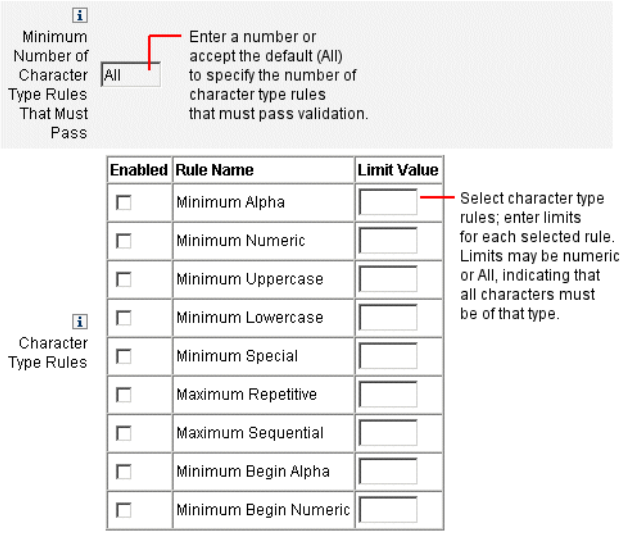


圖 11. 密碼策略 (字元類型) 規則

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 [策略] 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」中標題為 「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 [不可重複使用的舊密碼數目] 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，若輸入的數值為 3，則新密碼不可與目前密碼或其之前使用的兩個密碼相同。

您也可以禁止重複使用與曾經用過的密碼類似的字元。在 [不可重複使用舊密碼中之類似字元的最大數目] 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，若是輸入值為 7，且舊密碼為 password1，則新密碼便不可以是 password2 或 password3。

如果輸入值為 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 [不可重複使用的舊密碼數目] 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。

附註 您也可以透過配置並實作字典策略來排除字詞。如需詳細資訊，請閱讀標題為「**配置**」的一章。

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

附註 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

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

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，會出現 [變更使用者密碼] 頁面。
2. 輸入或搜尋您要變更其密碼的使用者。選擇下列選項之一：
   - 輸入使用者名稱，然後按一下**變更密碼**。
   - 在 [使用者 ID] 欄位中輸入名稱的一個或多個字母，然後按一下**尋找**。Identity Manager 會傳回其 ID 中包含已輸入字元的所有使用者的清單。按一下以選取一名使用者，然後返回 [變更使用者密碼] 頁。

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

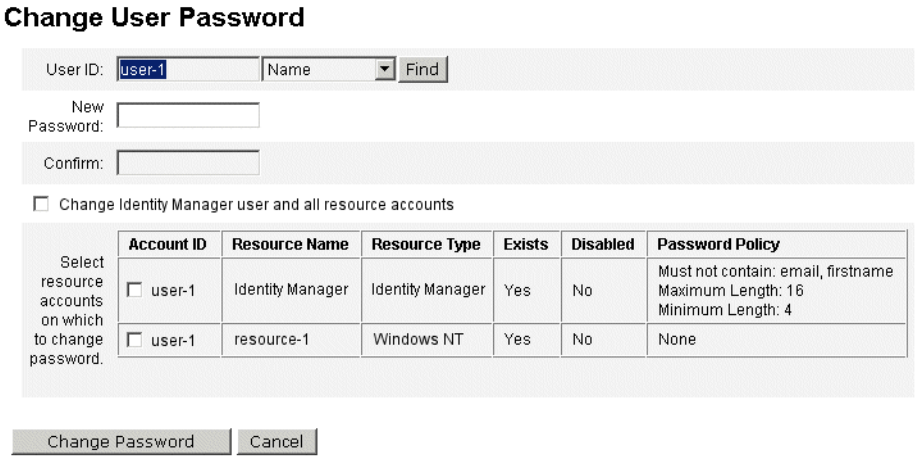


圖 12. 變更使用者密碼

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為您不需指定新密碼。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) 控制數個重設選項，包括：

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

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 帳號策略] 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 [重設使用者密碼表單] 中，您會將 `resourceAccounts.currentResourceAccounts[Lighthouse].expirePassword` 設為 `false` 值。

在 [Lighthouse 帳號策略] 的 [重設選項] 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，然後為使用者設定此日期。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，然後為使用者設定此日期。如果沒有指定值，則變更或重設的密碼將永不過期。如果 tempPasswordExpiry 的值設為 0，密碼會立即過期。

附註 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。

使用者自我探索

Identity Manager「使用者介面」允許使用者**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

若要啟用自我探索，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。若要執行這個動作：

1. 開啟 Identity Manager [系統設定] 頁 (`idm/debug`)。
2. 從 [配置] 類型清單中選取 [配置]，然後按一下**列出物件**。
3. 按一下 [一般使用者資源] 旁的**編輯**來顯示配置物件。
4. 新增 `<String>`***Resource***`</String>`，其中 ***Resource*** 與儲存庫中資源物件的名稱相符。

Checkout Object: Configuration, #ID#Configuration:EndUserResources

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Configuration PUBLIC 'waveset.dtd' 'waveset.dtd'>
<!--  id="#ID#Configuration:EndUserResources" name="End User Resources"-->
 <Configuration id='#ID#Configuration:EndUserResources' name='End User Resources'
creator='Configurator' createDate='1026770940487' lastMod='7' counter='0'>
  <Extension>
    <List>
       <String>NT</String>
    </List>
  </Extension>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Top' name='Top'/>
  </MemberObjectGroups>
</Configuration>
```

Add a line for each resource to be added to user self-discovery selections

Save Cancel

圖 13. 一般使用者資源配置物件

5. 按一下**儲存**。

啟用自我探索後，使用者用 Identity Manager「使用者介面」上的一項新功能表項目表示 (**向 Identity Manager 通知其他帳號**)。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。

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 [建立並編輯使用者] 頁面)。

在帳號策略中設定認證：

1. 從功能表列中，選取 **[Configure]**，然後選取 **[Policies]**。
2. 從策略清單中選取 [預設 Lighthouse 帳號策略]。

   在頁面的 [輔助身份認證策略選項] 區域中會提供認證選項。

重要事項！ 第一次設定時，使用者必須登入 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

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

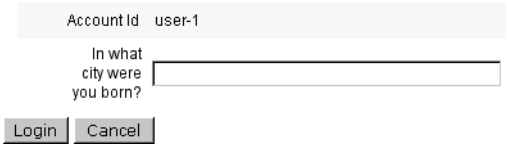


圖 14. 使用者帳號認證

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為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。

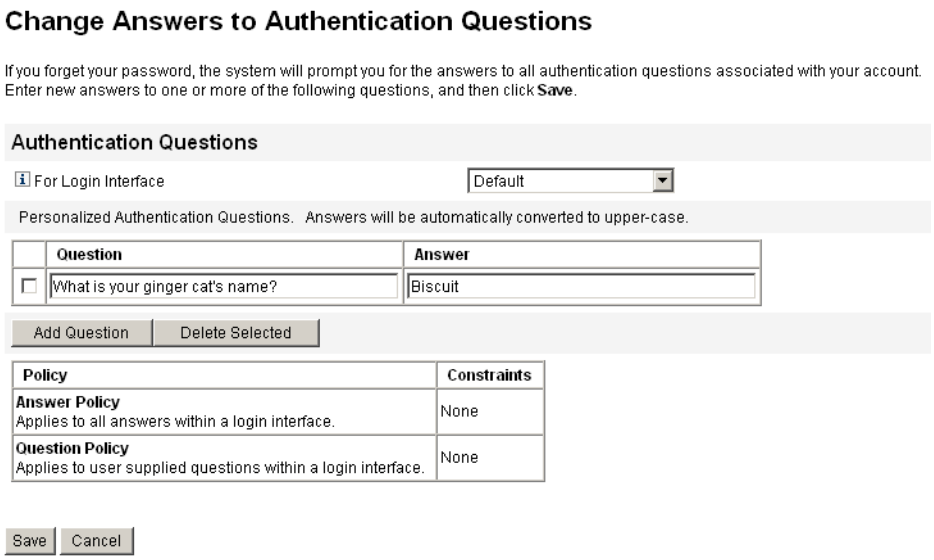


圖 15. 變更回答 — 個性化的認證問題

認證後略過變更密碼質詢

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。您可以將 Identity Manager 配置為略過變更密碼質詢，但是透過設定 bypassChangePassword 系統配置特性，可以略過一個或多個 Identity Manager 應用程式。

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

```
<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屬性，請將其設定如下：

```
<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>
    ...
```

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。您可以發起的批次處理動作為：

- **刪除 —** 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。
- **刪除與解除連結 —** 刪除選取的任何資源帳號，並解除該帳號與使用者的連結。
- **停用 —** 停用選取的所有資源帳號。選取 [以 Identity Manager 帳號為目標] 選項可停用每個使用者的 Identity Manager 帳號。
- **啟用 —** 啟用選取的所有資源帳號。選取 [Target the Identity Manager Account] 選項可啟用每一位使用者的 Identity Manager 帳號。
- **Unassign —** 取消任意選取資源帳號的連結，並移除這些資源上指定的 Identity Manager 使用者帳號。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，您無法取消指定其帳號。
- **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 [尋找使用者] 頁面上搜尋使用者。

啟動批次處理帳號動作

若要啟動批次處理動作，請選取或輸入值，然後按一下**啟動**。Identity Manager 會啟動背景工作以執行批次處理動作。

提示 若要監視批次處理動作的作業狀態，請前往 [作業] 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。若為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** — 啟用資源帳號、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，需要指定的唯一欄位是資源。使用資源欄位可指定哪些資源上的哪些帳號將受影響。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。

以下是幾個此類動作的 CSV 格式範例：

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

Create、Update 和 CreateOrUpdate 指令

如果您正在執行 Create、Update 或 CreateOrUpdate 指令，則您除了指定 [使用者] 與 [指令] 欄位外，還可以指定 [使用者檢視] 中的欄位。使用的欄位名稱是檢視中的屬性之路徑表示式。如需有關使用者檢視中可用屬性的資訊，請參閱「Identity Manager 工作流程、表單與視圖」。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。

範例

以下是建立和更新動作的 CSV 格式範例：

```
command,user,waveset.resources,password.password,password.confi
rmPassword,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。它們又稱為多值欄位。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 (也稱為「管道」字元) 來分隔一個欄位的多個值。您可以指定下列多值語法：

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

對現有的使用者更新多值欄位時，您可能不想將現行欄位的值替代為一或多個新值。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：

```
|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，因為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。

附註 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，則您需要在它前面加上一條反斜線 (\| 或 \\)。

批次處理動作檢視屬性

執行 Create、Update 或 CreateOrUpdate 動作時，「使用者檢視」中有一些屬性只能在批次處理動作處理中使用。您可以在 [使用者表單] 中參考這些屬性，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為 `waveset.bulk.fields.command` 與 `waveset.bulk.fields.user` 的屬性中。
- **waveset.bulk.fieldDirectives.***field_name* — 僅會針對為其指定了指令的那些欄位定義這些屬性。此值為指示字串。
- **waveset.bulk.abort** — 將這個布林屬性設為 true，以中斷目前動作。
- **waveset.bulk.abortMessage** — 將此屬性設為訊息字串，以便在 waveset.bulk.abort 設為 true 時顯示。若未設定此屬性，則會顯示一般中斷訊息。

相互關聯與確認規則

當您沒有可用來填入動作的使用者欄位的 Identity Manager 使用者名稱時，可使用相互關聯與確認規則。若未指定使用者欄位值，啟動批次處理動作時，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。

相互關聯規則

相互關聯規則的輸入是動作欄位的對映。輸出必須為下列其中之一：

- 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為 QueryableAttrNames。

在延伸屬性上進行相互關聯需要特殊配置：

- 必須在 UserUIConfig 中將延伸屬性指定為可查詢 (加入 QueryableAttrNames 清單)。
- Identity Manager 應用程式 (或應用程式伺服器) 可能需要重新啟動，UserUIConfig 變更才會生效。

確認規則

對確認規則的輸入包括：

- 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，您只有在以下情況會需要確認規則：

- 相互關聯規則可能傳回多個符合的使用者
- 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。

4 管理指南

本章將提供在 Identity Manager 系統中執行一系列管理層級工作的資訊與程序，例如：

- 建立 Identity Manager 管理員和委託管理
- 定義組織與虛擬組織
- 建立與管理管理員

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 透過以下指定區別管理員與使用者：

- **擴充權能**。管理員會在每個其管理的組織中，將擴充權能應用至帳號、角色與資源。
- **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。在很多情況中，管理員必須執行帳號管理工作，而該工作對其他使用者或管理員而言是「透明」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，不大可能需要關於其建立使用者帳號的資源的特定資訊；或關於系統內現有角色或組織的特定資訊。

Identity Manager 支援責任分離與此委託管理模式，方法是僅允許管理員「查看」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

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為**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：

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，請在清單中選取一個組織，然後從 [New Actions] 清單中選取 [New Organization]。

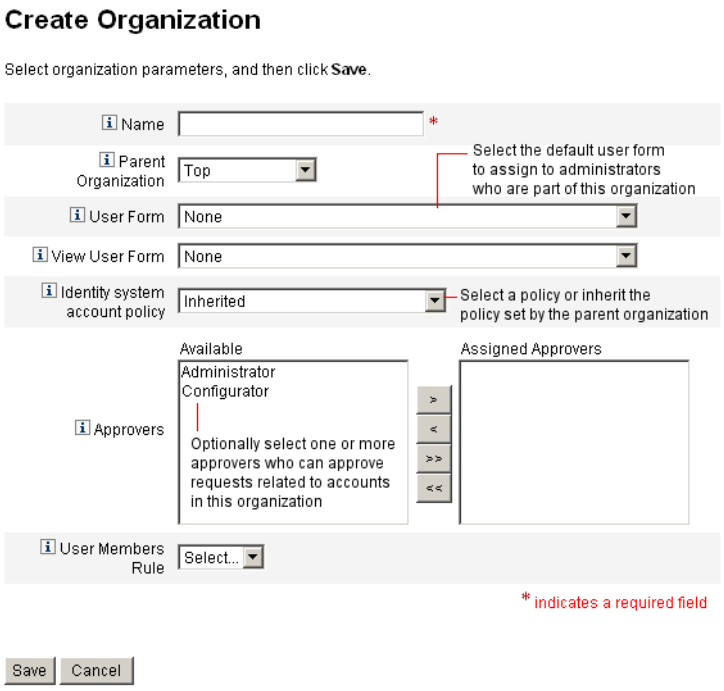


圖 1. 建立組織

指定使用者給組織

每個使用者均為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 [尋找使用者] 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 [建立組織] 頁面的 [使用者成員規則] 欄位選擇使用者成員規則。

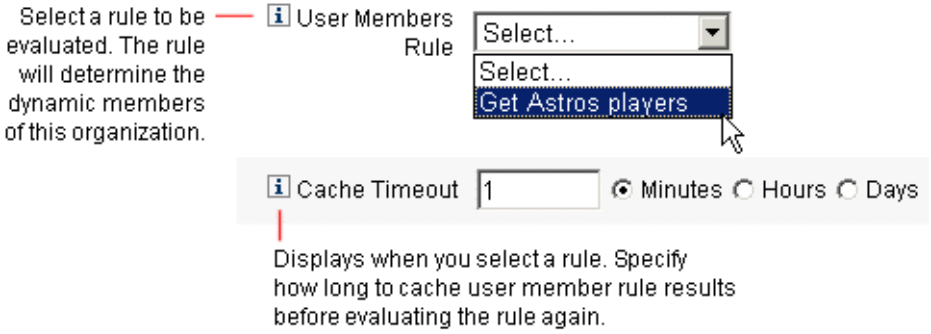


圖 2. 建立組織：使用者成員規則選取

以下範例顯示了您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。

附註 如需關於在 Identity Manager 中建立和使用規則的相關資訊，請參閱 Identity Manager 部署工具。

金鑰定義與內含項

- 欲使某規則出現於 [User Member Rule] 選項方塊中，其 authType 必須設定為 `[authType='UserMembersRule']`。
  - 上下文是目前驗證的 Identity Manager 使用者的階段作業。
  - 對於身為 Windows Active Directory ou 'Houston Astros' 的成員的每個使用者，定義的變數 (`defvar`) 'Astros players' 取得 dn。
  - 對於找到的每個使用者，附加邏輯會將 'Houston Astros' ou 的每個成員使用者的 dn 與使用分號前綴的 Identity Manager 資源名稱串連在一起 (如 ":dogbreath-AD")。
  - 傳回的結果會是與 Identity Manager 資源名稱串連的 dn 的清單，格式為「<dn>:dogbreath-AD」。

使用者成員規則範例

```
<Rule name='Get Astros players'
         authType='UserMembersRule'>
   <defvar name='Astros 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>dogfish-AD</s>
      <map>
         <s>searchContext</s>
         <s>OU=Houston Astros,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>:dogbreath-AD</s>
      </concat>
      </append>
   </dolist>
      <ref>player names</ref>
   </block>
   </defvar>
      <ref>Astros players</ref>
</Rule>
```

指定組織控制

從 [建立使用者] 或 [編輯使用者] 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 [管理角色] 欄位指定一個或多個管理角色，來指定組織的管理控制。

瞭解目錄結合與虛擬組織

目錄結合是一組階層相關的組織，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。

目錄集合中每個組織皆是**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本上下文的容器的鏡射。目錄結合中的其餘虛擬組織為頂層虛擬組織的**直接**或**間接**子系，而且還鏡射一個為已定義資源的基本上下文容器之子系的目錄資源容器。

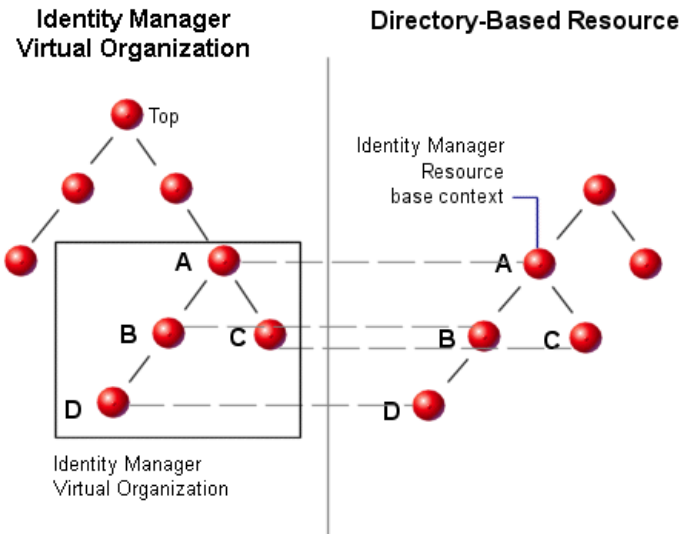


圖 3. Identity Manager 虛擬組織

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]。

   您選取的組織將成為設定的虛擬組織的父系組織。

   Identity Manager 顯示 [建立目錄結合] 頁面。
3. 選取設定虛擬組織的選項：
   - **父系組織** — 這個欄位包含您從 [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**刪除**。

建立管理員

您可以藉由擴充 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)

若要給予使用者管理權限，請選取 **[Accounts]**，以移至 [Identity Manager Accounts] 區域，然後選取 **[Security]** 表單標籤。

選取一或多項以建立管理控制：

- **控制的組織** — 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。
- **權能** — 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。如需更多有關 Identity Manager 權能的資訊或說明，請閱讀 第 5 章，**配置**。
- **使用者表單** — 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。
- **將核准請求轉寄給** — 選取一名使用者，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。

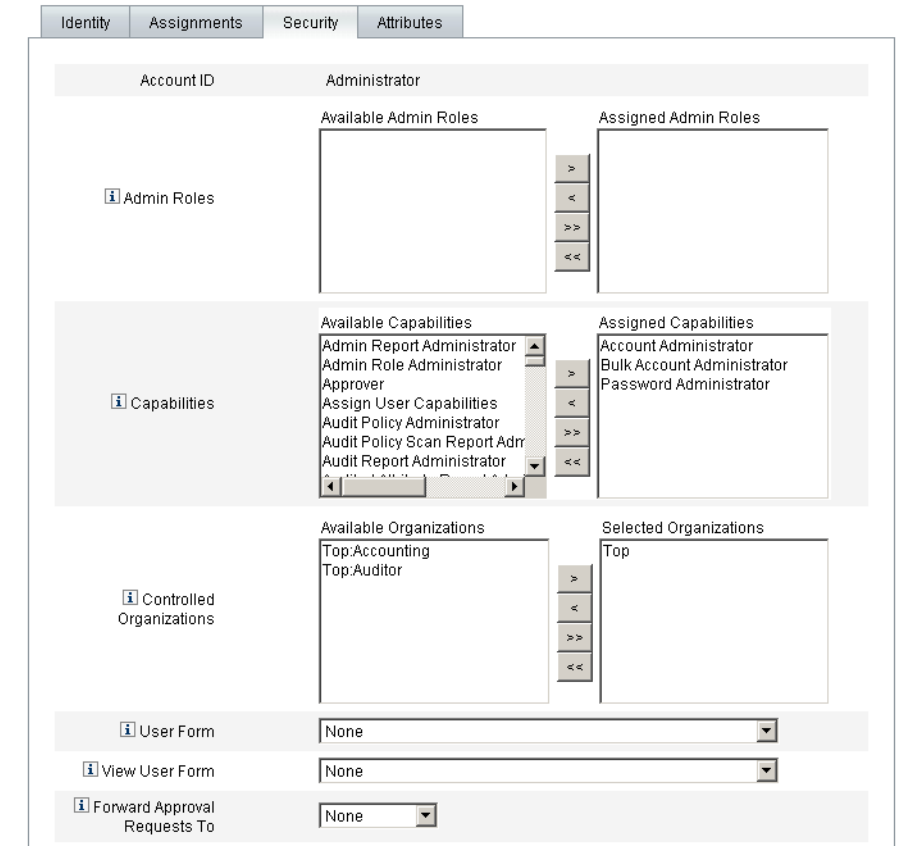

Identity
Assignments
Security
Attributes
Account ID
Administrator
Admin Roles
Available Admin Roles
Assigned Admin Roles
Capabilities
Available Capabilities
Admin Report Administrator
Admin Role Administrator
Approver
Assign User Capabilities
Audit Policy Administrator
Audit Policy Scan Report Adm
Audit Report Administrator
Assigned Capabilities
Account Administrator
Bulk Account Administrator
Password Administrator
Controlled Organizations
Available Organizations
Top:Accounting
Top:Auditor
Selected Organizations
Top
User Form
None
View User Form
None
Forward Approval Requests To
None

圖 4. 建立管理員

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為兩個層級：

- **組織** — 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 會繼承為父組織選取的表單。若此處沒有設定表單，則 Identity Manager 會使用系統配置中設定的預設表單。
- **管理員** — 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 (或若沒有為組織設定表單時，繼承系統配置中設定的預設表單)。

附註 第 5 章，**配置**，說明您可指定的內建 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：

- **帳號區域** — 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。
- **密碼區域** — ，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**尋找**以列出所有相符的項目。

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

附註 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：

- Edit User (account/modify.jsp)
- Change User Password (admin/changeUserPassword.jsp)
- Reset User Password (admin/resetUserPassword.jsp)

請按如下所示在 account/modify.jsp 頁中設定此選項：

```
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

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

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

其中，選項的值可以是 `true` 或 `false`。

變更身份驗證問題的答案

使用 [密碼] 區域可變更您為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]**。

如需關於認證的更多資訊，請參閱**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，可以顯示管理員的某些屬性 (例如電子郵件或全名) 而非帳號 ID。其中包括：

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

若要將 Identity Manager 配置為使用顯示名稱，請將以下內容加入到 UserUIConfig 物件中：

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

例如，若要使用電子郵件屬性來當作顯示名稱，請在 UserUIconfig 中加入：

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

核准

將使用者新增至 Identity Manager 系統時，指定為新帳號**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：

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

附註 您可以將 Identity Manager 配置為數字簽名的核准。如需有關此功能的資訊，請參閱標題為「**配置**」章節中的「**簽署的核准**」。

設定核准人

為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。對於其中設定了核准人的每個種類，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。因為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「業務程序編輯器 (BPE)」來變更核准流程、擷取帳號刪除與擷取更新。

如需關於 BPE、工作流程以及變更核准工作流程的圖示範例的更多資訊，請參閱「Identity Manager 工作流程、表單與視圖」。

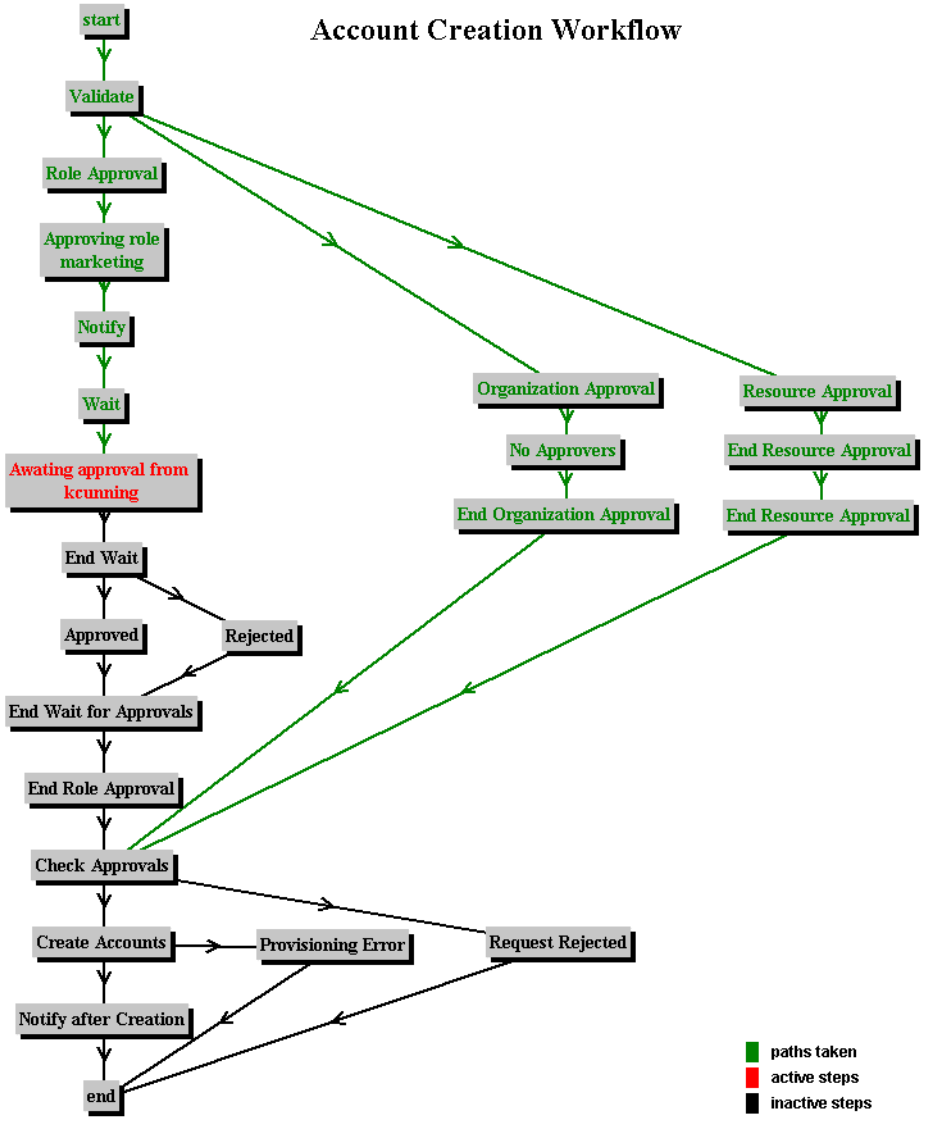

Account Creation Workflow
start
Validate
Role Approval
Approving role marketing
Notify
Wait
Awating approval from kcunning
End Wait
Approved
Rejected
End Wait for Approvals
End Role Approval
Check Approvals
Create Accounts
Provisioning Error
Request Rejected
Notify after Creation
end
Organization Approval
No Approvers
End Organization Approval
Resource Approval
End Resource Approval
End Resource Approval
paths taken
active steps
inactive steps

圖 5. 帳號建立工作流程

5 配置

本章提供有關使用 「管理員介面」設定 Identity Manager 物件的資訊和程序。

在本章中，您可以瞭解關於下列項目的更多內容：

- 建立和編輯 Identity Manager 物件，例如：
  - 角色
  - 資源
  - 變更記錄檔
  - 策略
  - 權能
  - 管理員角色
  - 電子郵件範本
  - 伺服器
- 設定稽核配置群組 (稽核事件)
- 將 Identity Manager 與 Remedy 伺服器整合
- 配置數位簽署的核准

瞭解角色

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，或者不指定為任何角色。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，資源是為使用者特別選定的。

建立或編輯角色時，Identity Manager 會啟動 `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 [管理員介面] 的 [建立和編輯使用者] 頁面將角色指定給使用者。

建立角色

若要建立角色，請：

1. 在功能表列中，選取 **[Roles]**。
2. 在 [角色] 清單頁面中，按一下**新增**。

[建立角色] 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　若要瞭解關於核准程序的詳情，請參閱「管理」一章中的「核准」小節。

- 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 [建立角色] 頁面上的 [指定的資源] 區按一下**設定屬性值**以顯示指定給角色的每一資源的屬性清單。在此 [編輯] 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。

編輯角色

若要對角色進行修改，請：

1. 在功能表列中，選取 **[Roles]**。
2. 在 [角色] 清單頁面中，按一下清單中的角色。

尋找角色

使用 [尋找角色] 區搜尋角色。搜尋功能會傳回符合您搜尋條件的角色清單。

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

備註：

- 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。

若要搜尋角色，請選取 **[Roles]**，然後選取 **[Find Roles]**。

複製角色

您可以使用現有角色中的選項建立新角色。若要執行這個動作，請：

1. 選取要編輯的角色。
2. 在 [名稱] 欄位中輸入新的名稱，然後按一下**儲存**。
   Identity Manager 顯示 [建立或重新命名] 頁面。
3. 按一下**建立**可建立新角色。

重新命名角色

若要重新命名角色，請：

1. 選取要編輯的角色。
2. 在 [名稱] 欄位中輸入新的名稱，然後按一下**儲存**。
   Identity Manager 顯示 [建立或重新命名] 頁面。
3. 按一下**重新命名**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]** 以存取 [Synchronize Identity Manager Roles with Resource Roles] 作業頁面。

瞭解資源

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

資源區

Identity Manager 顯示關於 [資源] 頁中現有資源的資訊。

若要存取資源，請選取功能表列上的 **[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。再按一下該指示器可以摺疊視圖。

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)。

有些資源具有您可以管理的其他物件，包括：

-  組織
-  組織單位
-  群組
-  角色

從資源清單中選取一個物件，然後從以下選項清單之一中進行選取以啟動管理作業：

- **[Resource Actions]** — 在資源上執行一系列動作，包括編輯、啟動同步化、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資源。

建立或編輯資源時，Identity Manager 會啟動 `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 [配置] 區進行管理從 [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 將資源劃分為兩類：

- **Identity Manager 資源** — 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 [受管理？] 欄中選取選項來選擇一個或多個資源，然後按一下**儲存**將其增加到資源清單。
- **自訂資源** — 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**增加自訂資源**，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**儲存**新增資源到 [資源] 清單。

下表列出自訂資源類別。

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 ActiveSync	com.waveset.adapter.ActiveDirectoryActiveSyncAdapter
ClearTrust	com.waveset.adapter.ClearTrustManagerResourceAdapter
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。

附註 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，而是立即啟動資源精靈。

3. 按一下**下一步**開始定義資源。所顯示的「資源精靈」步驟和頁面順序如下：
   - **資源參數** — 設定用於控制認證和資源配接卡運作方式的資源專用參數。輸入參數，然後按一下 **[Test Connection]** 來確保連線有效。確認後，按一下 **[Next]** 以設定帳號屬性。

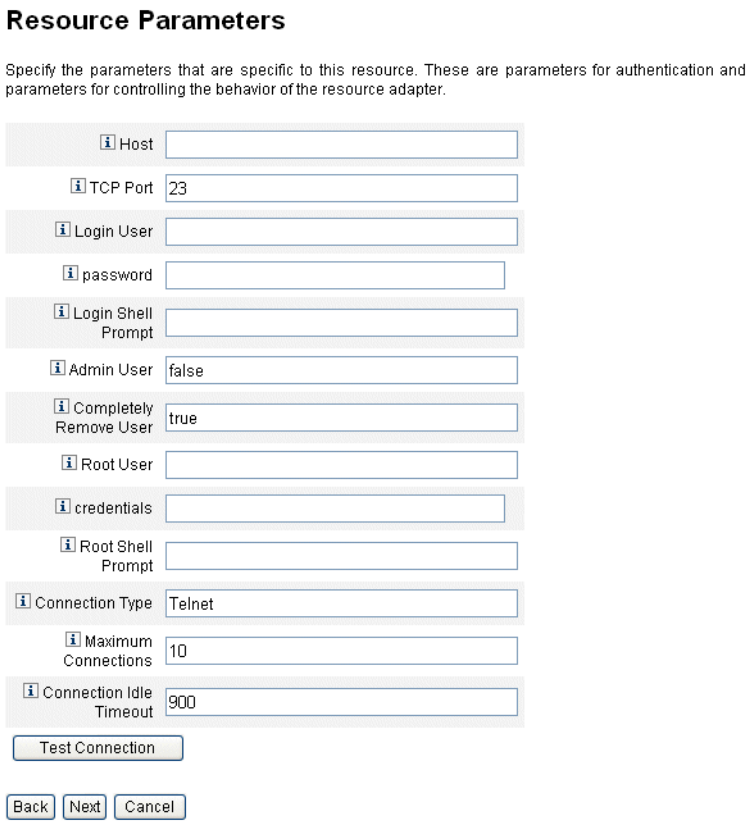


圖 1. 資源精靈：資源參數

   - **帳號屬性（模式對映）** — 將 Identity Manager 帳號屬性對映到資源帳號屬性。

     若要新增屬性，按一下**新增屬性**。選取一個或多個屬性，然後按一下**刪除選取的屬性**從模式對映中刪除屬性。當完成時，按一下**下一步**設定身份識別範本。

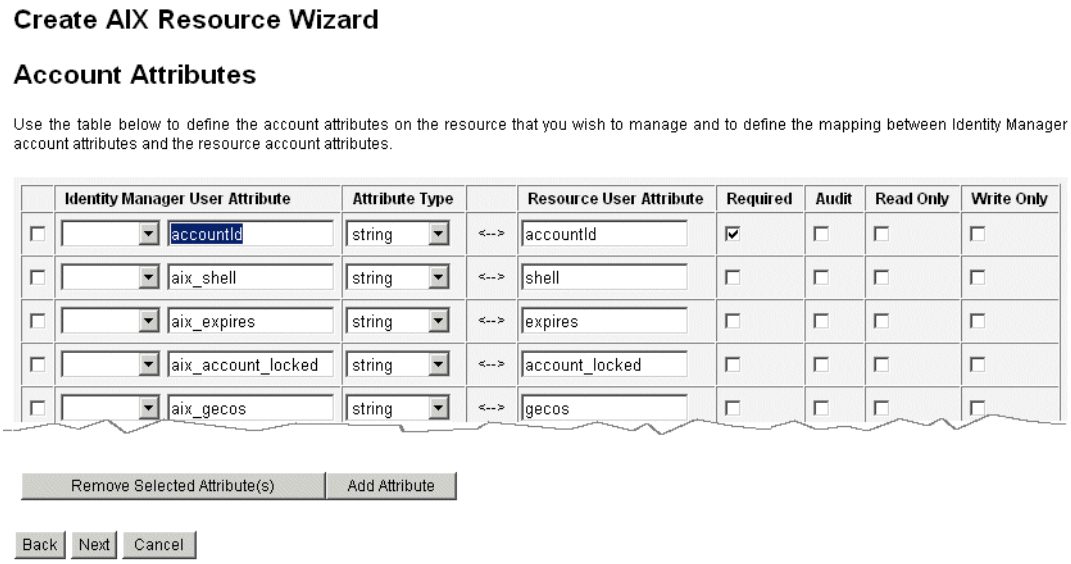


圖 2. 資源精靈：帳號屬性 (模式對映)

- **身份識別範本** — 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 [插入屬性] 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 $ (錢幣符號) 字元。

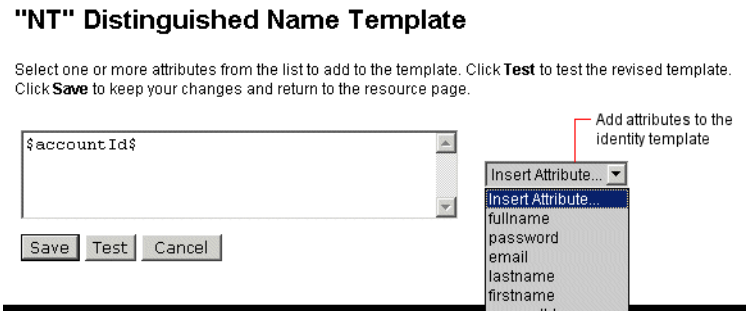


圖 3. 資源精靈：身份識別範本

- **Identity 系統參數** — 設定資源的 Identity Manager 參數，包括重試和策略配置。

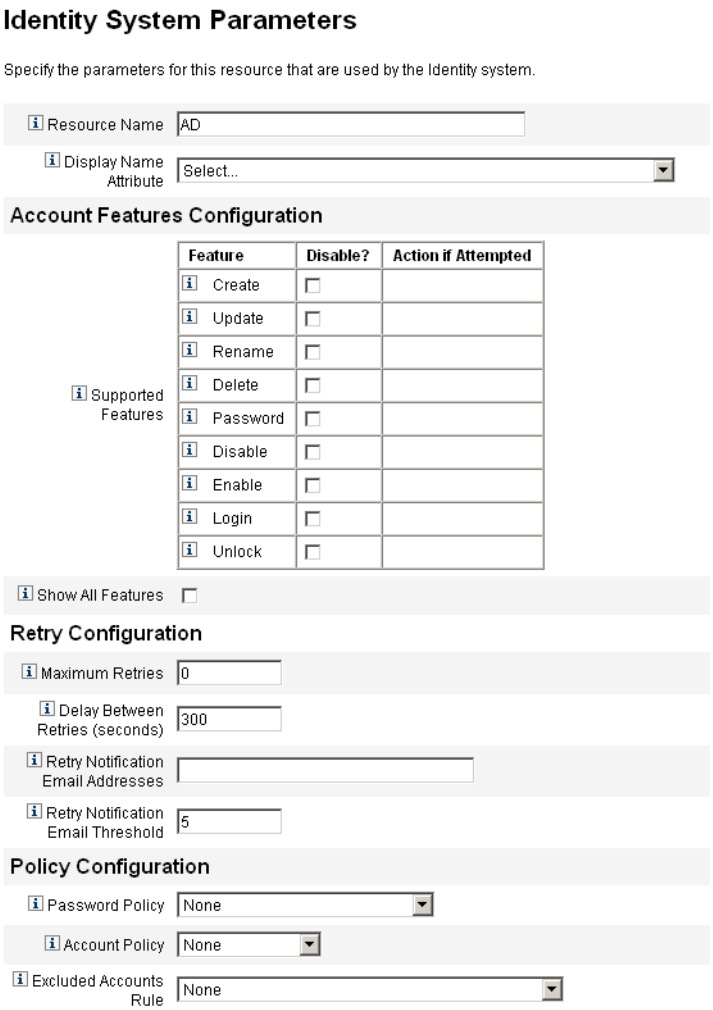


圖 4. 資源精靈：Identity 系統參數

使用**下一頁**和**上一頁**在頁面中移動。當您完成所有選項後，按一下 [儲存] 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採取多種編輯動作。除了在每一 [資源精靈] 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] 來依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的名稱，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。

使用帳號屬性

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

- 將資源屬性限定為只有您的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
- 辨認所需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 (標題為「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 (標題為「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` 屬性對映到 Active Directory 資源屬性 `sn`；在 GroupWise 上，fullname 屬性可以對映到 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**新增**定義資源群組。在定義資源群組時，選項區可讓您選擇並排序選取的資源，以及選取可使用該資源群組的組織。

瞭解變更記錄檔

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 Identity 屬性資訊。將每個變更記錄檔定義為擷取 Identity 屬性某個子集的變更。

當資源上的屬性資料變更後，ActiveSync 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 的標準資源之 ActiveSync 和調解功能不同，因為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` 做為目錄，策略檔案應包含：

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

您必須為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。

附註　編輯安全策略檔案之後，您可能需要重新啟動 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 Identity 屬性，然後才能配置變更記錄檔。

配置 Identity 屬性

使用以下資訊與程序來配置 Identity 屬性，並選取將要套用 Identity 屬性的 Identity 系統應用程式。

處理 Identity 屬性

若要配置 Identity 屬性，請選取 **[Configure]**，然後從 Identity Manager 管理員介面選取 **[Identity Attributes]**。顯示 [Identity Attributes] 頁面。

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

附註　您必須按一下 **[Save]**，才能執行該動作。

選取應用程式

使用 [Enabled Applications] 區域來選取將套用 Identity 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。

附註　若要使用變更記錄檔功能，您必須啟用 ActiveSync 應用程式。

增加和編輯 Identity 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 Identity 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 Identity 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 Identity 屬性的值。將按順序評估這些來源，並將 Identity 屬性設定為第一個非空值。
  - **Resource** — 該值來自於選取資源上的選取屬性。
  - **Rule** — 該值來自於選取規則的評估。
  - **Constant** — 該值設定為提供的常數值。

  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。
- **Attribute Properties** — 使用此區域可設定 Identity 屬性的特性。
  - **Identity Attribute is authoritative** — Identity 屬性的值強制設定在所有的目標上。選取此選項，會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。通常，應該選取此選項。
  - **Store attribute in IDM repository** — 選取此選項，以將 Identity 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 Identity 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 Identity 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 Identity 屬性的目標資源。如果未定義目標，則按一下 **[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]** 來增加該 Identity 屬性並返回至 [Identity Attributes] 頁面。必須在 [Identity Attributes] 頁面上按一下 **[Save]** 來儲存增加的屬性。

增加目標資源

提示 如果 Identity 屬性僅用於變更記錄檔，則不必為 Identity 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」來將資料推入 ActiveSync，則您可以這樣做。 如果沒有目標，則 MetaView 將僅評估 Identity 屬性的值；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 Identity 屬性的目標資源：

- **Target Resource** — 選取應該設定所選 Identity 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選取的 Identity 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 Identity 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]** 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 Identity 屬性

使用匯入 Identity 屬性功能，您可以選取一個或多個表單來匯入並寫入 Identity 屬性值。Identity Manager 將分析匯入的表單值並對 Identity 屬性進行「最佳猜測」；但是在匯入後編輯 Identity 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 Identity 屬性合併。如果未選取，則會在匯入執行之前清除 Identity 屬性。

- **Forms to import** — 從 [Available Forms] 區域中選取一個或多個表單來寫入 Identity 屬性。

  按一下 **[Import]** 來匯入該表單。顯示 [Identity Attributes] 頁面，其中會列出新的或合併的 Identity 屬性。

  按一下 **[Save]** 以儲存 Identity 屬性的變更。

附註 如果有需要校正的 Identity 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]** 以返回至 [Configure] 區域。

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。變更記錄檔定義變更子集 (由 ActiveSync 偵測到並推入 Identity 屬性) 應該寫入記錄。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與變更記錄檔策略，請選取 **[Configure]**，然後從管理員介面功能表列選取 **[ChangeLogs]**。

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

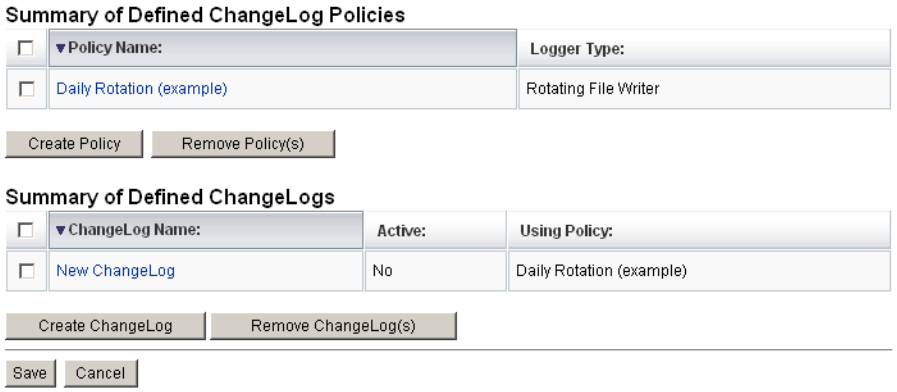


圖 5. 變更記錄檔配置

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 [Identity Manager 配置] 頁面。

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** — 為策略輸入唯一的名稱。
- **Daily Start Time** — 建立每天用來評估週轉開始或變更的時間。使用此策略的變更記錄檔將在該時間啟動新的週轉，並以從該時間評估的增量啟動新的週轉。例如，如果啟動時間設定為午夜 (00:00) 且 [Rotations Per Day] 設定為 3，則記錄檔的前綴將在 00:00、08:00 與 16:00 變更。

  檔案名稱遵循樣式「cl_User_yyyyMMddHHmmss.n.suffix」，其中「HHmmss」是最近啟動週轉的時間。(「.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」做為啟動時間，3 做為週轉數的情況下，如果您在某天上午 9:24 啟動變更記錄檔，則產生的週轉名稱將包含最近啟動週轉的時間 (例如，08:00)。這樣，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) 將啟動。
- **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。如果欄位為非零，則忽略「Maximum Age of a Rotation」設定。

  如果以秒為單位指定週轉的時間長度，且 「Rotations Per Day」欄位為 0，則此值用來確定週轉的期間。

  此值僅限於非負整數值。如果您為 「Rotations Per Day」指定非零數字，則使用該指定的值 (不使用此值)。如果這兩個欄位的值均為 0，則僅套用序列資訊。(在此情況下，也不會使用 [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，則將啟動新記錄檔 (具有相同的週轉前綴，但具有新的序列號)。值 0 表示不使用此限制。會使用所有值為非零的限制欄位 (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，且將行寫入該新檔案。值 0 表示「沒有限制」。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這裡指定的秒數，則會建立新的序列檔案再寫入變更。值 0 表示不使用此限制。其他限制如果為非零，會在該值之前套用。

按一下 **[OK]** 以返回至 [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** — 為變更記錄檔輸入唯一的名稱。
- **Active** — 如果您選取此選項，則在變更記錄檔通過 ActiveSync 資源匯入 Identity 屬性時，它將監視並寫入變更 (ActiveSync 必須為 Identity 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。否則，它必須命名一個實作 com.sun.idm.changelog.ChangeLogFilter 的 Java 類別。此類別必須位於伺服器的類別路徑中，必須具有公共預設建構子。
- **Log these Operations** — 記錄選取類型的事件，包括建立、更新與刪除。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 Identity 屬性名稱。列的順序表示欄的順序。定義欄之後，使用「Up」與「Down」按鈕為其排序。

附註 在每個變更記錄檔中，表格中均有名為「changeType」的默認第一欄。此默認第一欄指出變更的類型。此欄的類型為「Text」。記錄中的資料將是下列值之一：「ADD」、「MOD」或「DEL」。

- **Use the Policy Named** — 從清單中選取定義的變更記錄檔策略以用於記錄。
- **Output Path** — 輸入在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** — 為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

檢視範例，其中詳細說明如何設定 Identity 屬性與變更記錄檔以擷取特定屬性資料集。

範例：定義 Identity 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

附註 * 表示用來關聯記錄的鍵。

這些 Identity 屬性如下定義。

屬性	<==	**來自 Resource.Attribute**
employee	<==	EmployeeInfo.employeeNumber
dept	<==	OrgInfo.departmentNumber
reportsTo	<==	OrgInfo.managerEmpNum
firstname	<==	EmployeeInfo.givename
lastname	<==	EmployeeInfo.givename

屬性	<==	來自 Resource.Attribute
middleInitial	<==	EmployeeInfo.mi
fullname	<==	firstName + “ “ + middleInitial + “ “ + lastName
phoneNumber	<==	EmployeeInfo.phone

範例：配置變更記錄檔

定義 Identity 屬性後，定義稱為 PhoneList ChangeLog 的變更記錄檔。目的是將 Identity 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	Identity 屬性
empId	Text	employee
fullname	Text	fullname
phone	Text	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 Identity 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。

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」為檔案中的每行。

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，變更事件是否為建立、修改或刪除動作。它總是命名為 changeType，並總為類型 T (表示文字)。其值為 ADD、MOD 或 DEL 之一。

每一欄應該準確具有一個唯一的項目識別碼 (主鍵)。一般為檔案中的第二欄。

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

列

定義檔案 「模式」的前兩個標頭列之後，剩餘的列為屬性的值。值以第一列中欄位的順序顯示。變更記錄檔套用自 Identity 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

文字值寫入為字串，但有兩種例外：

- 如果值包含，(逗號)，則透過插入 \ (反斜線) 字元，Identity Manager 可轉譯值中的逗號。例如，如果完整名稱的值為 `Mouse, Mickey`，則 Identity Manager 寫入
  `Mouse\, Mickey` 做為值。
- 如果值包含 \ (反斜線) 字元，則 Identity Manager 會另加一個 \ 來轉譯該 \ 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。如果檔案需要換行，則使用二進位值類型。

二進位值

二進位值以 Base64 進行編碼。

多文字值

多文字值與文字值寫入方式相似，但用逗號分隔並使用 [與] 括住。

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) 資料在檔案中顯示為字串：

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

- 二進位 (B) 資料顯示為 base64 編碼。

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

- 多文字 (MT) 顯示為：

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

- 多文字 (MB) 顯示為：

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

附註 Base64 字母不包含 ，(逗號)、[(左括號) 或] (右括號) 字元，或者換行。

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* 為此記錄啟動或自動重建的時間。具有相同時間戳記的檔案視為同一「週轉」。
- *sequenceNumber* 為單增長數字，用來將週轉分割為檔案子集，並由位元、行或秒的最大數目控制。每個檔案子集稱為一個「序列」檔案。
- *suffix* 為變更記錄檔配置中定義的檔案副檔名，通常為 `.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

如果策略定義週轉為：

- 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 DEL 行僅包含 accountId 值。
- 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：
  - 在午夜啟動週轉，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 (時間分別為 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；它可以是以大小為基礎、以數字作業為基礎或以時間為基礎。

- 每個變更記錄檔都可以代表後端系統中的記錄。為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，他們需要確保後端資源 (或程序檔)，特別是對於 ADD 與 DEL，可以：

  - 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。) 如果程序檔從開啟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。

瞭解策略

請閱讀本節以獲得關於配置策略的資訊和程序。

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。

您需在 [策略] 頁中建立並編輯 Identity Manager 策略。在功能表列中，選取 **[Configure]**，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。

策略分類如下：

- **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 and Edit Organization] 以及 [Create and Edit User] 頁面，您可將 Identity 系統帳號策略指定給組織或使用者。

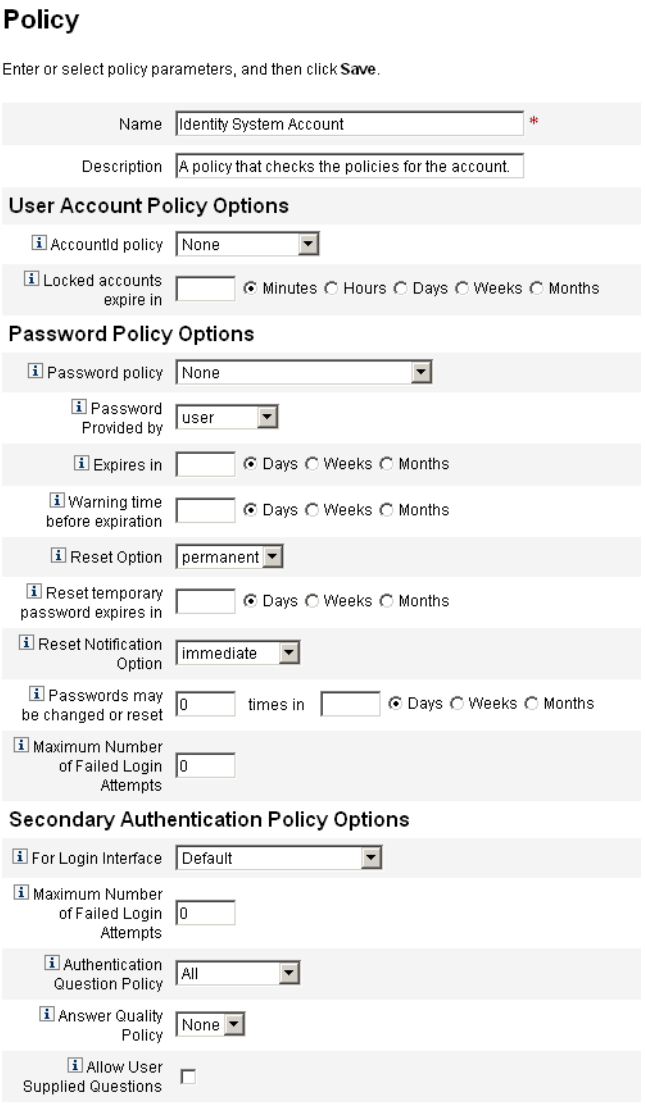


圖 6. Identity Manager 策略

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** — 決定如何向使用者顯示認證問題，使用者是否可以提供他自己的認證問題，並建立可以向使用者顯示的問題庫 (最多 10 項)。

- **String Quality Policies** — 字串品質策略包含策略類型，例如密碼、AccountID 與認證，並設定長度規則、字元類型規則與允許的文字與屬性值。這種類型的策略繫結到每個 Identity Manager 資源，並在每一資源頁中設定。

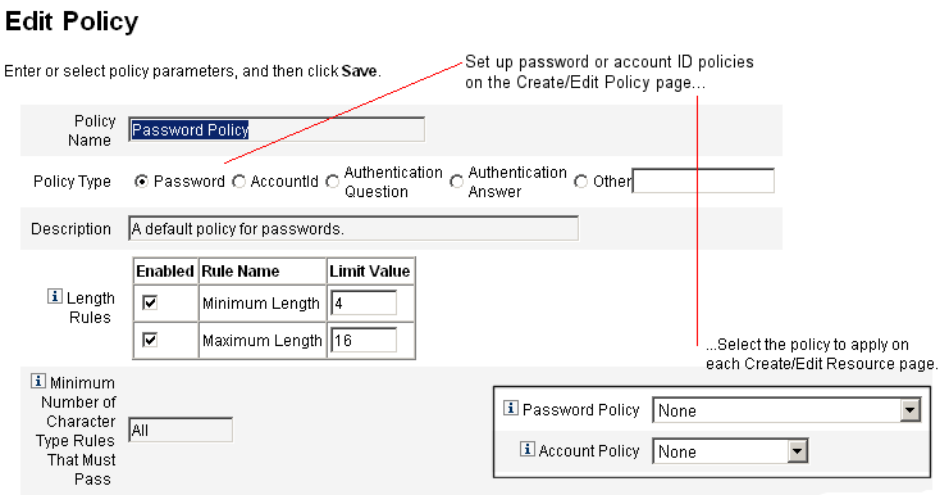


圖 7. 建立 / 編輯密碼策略

您可以為密碼和帳號 ID 設定的選項和規則包括：

- **Length rules** — 決定最小和最大長度。
- **Character type rules** — 設定字母、數字、大寫、小寫、重複及連續字元允許的最小和最大值。
- **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為專屬密碼。為了安全起見，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** — 指定不能用做 ID 或密碼部分的文字和屬性。

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 [管理員介面] 密碼 [編輯策略] 頁中的 [不得包含文字] 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**配置字典**顯示 [字典配置] 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**測試**以測試資料庫連線。
5. 如果連線測試成功，請按一下**載入文字**來載入字典。

附註　載入作業可能得花費幾分鐘才能完成。

6. 按一下**測試**確認字典已正確載入。

執行字典策略

從 Identity Manager 策略區執行字典策略。在 [策略] 頁面中，按一下以編輯密碼策略。在 [編輯策略] 頁面中，選取 [根據字典文字檢查密碼] 選項。執行之後，將根據字典來檢查所有變更和產生的密碼。

瞭解權能

權能為 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 使用者都需要為其指定權能；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。

為您指定的權能會掌控您可存取 Identity Manager 管理介面的哪些區域。所有 Identity Manager 管理使用者可以存取特定的 Identity Manager 區域，包括：

- **首頁**和**說明**標籤
- **密碼** 標籤 (只限**變更我的密碼**和**變更我的答案**子標籤)
- **報告** (限於和管理員的特定責任相關的類型)

權能類別

Identity Manager 如下定義類別：

-  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**，表示您無法編輯它們。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 **[Configure]**。
2. 選取 **[Capabilities]** 以顯示 Identity Manager 權能清單。

建立權能

若要建立權能，請按一下**新增**。

編輯權能

若要編輯非保護的權能，在清單中按一下滑鼠右鍵，然後選取**編輯**。

附註 您無法編輯內建權能；不過您可以用不同的名稱儲存它們以建立您自己的權能，或是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 (以不同的名稱儲存它以建立新的權能)：

- 以滑鼠右鍵按一下清單中的權能，然後選取 [另存新檔]。
- 輸入新名稱，然後按一下**確定**。

您可以編輯新權能，即使複製的權能受到保護。

指定權能

從 [建立和編輯使用者] 頁將權能指定給使用者。

附註 您也可以透過指定管理員角色 (您透過 [安全性] 區所設定) 將權能指定給使用者。詳細資訊請參閱瞭解管理員角色。

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
- 指定使用者權能
- 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
  - 啟用使用者
  - 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

批次帳號管理員

- 核准人
- 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
  - 批次啟用使用者
  - 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
- 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
  - 批次啟用使用者
  - 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

權能管理員

變更帳號管理員

- 核准人
- 指定使用者權能
- 變更使用者帳號管理員
  - 停用使用者
  - 啟用使用者
  - 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 / 匯出管理員

登入管理員

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
- 配置稽核

- 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

資源管理員

- 資源群組管理員
- 變更 Active Sync 資源管理員
- 控制 Active Sync 資源管理員

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

檢視組織

- 列出組織

檢視資源

- 列出資源

Waveset 管理員

權能定義

下表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。

所有的權能會允許使用者或管理員存取**變更我的密碼**和**變更我的答案**子標籤（**密碼**標籤中）。

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。	**帳號** — **列出帳號**、**尋找使用者**、**擷取至檔案**、**從檔案載入**、**從資源載入**子標籤 **密碼** — 所有子標籤 **核准** — 所有子標籤 **作業** — 所有子標籤
管理員報告管理員	建立、編輯、刪除和執行管理員報告。	**報告** — **管理報告**、**執行報告**子標籤（僅限管理員報告）
管理員角色管理員	建立、編輯和刪除管理員角色。	**配置** — **管理員角色**子標籤
核准人	核准或拒絕由其他使用者發起的請求。	**核准** — 所有子標籤
指定使用者權能	變更使用者的權能指定（指定和取消指定）。	**帳號** — **列出帳號**（僅編輯）、**尋找使用者**子標籤。 必須以另一項使用者管理員權能指定（例如，「建立使用者」或「啟用使用者」）。
稽核報告管理員	建立、編輯、刪除和執行稽核報告。	**報告** — 僅限稽核報告
批次帳號管理員	對使用者執行一般和批次作業，包括指定權能。	**帳號** — 所有子標籤 **密碼** — 所有子標籤 **核准** — 所有子標籤 **作業** — 所有子標籤
批次變更帳號管理員	對現有使用者執行一般與批次處理作業，包括指定權能，但刪除作業除外。	**帳號** — **列出帳號**、**尋找使用者**、**啟動批次處理動作**子標籤。無法建立或刪除使用者。 **密碼** — 所有子標籤 **核准** — 所有子標籤 **作業** — 所有子標籤

批次變更使用者帳號管理員	對現有使用者執行一般和批次作業，但刪除作業除外。	**帳號** — **列出帳號**、**尋找使用者**、**啟動批次處理動作**子標籤。無法建立、刪除或指定給使用者的權能。 **密碼** — 所有子標籤 **作業** — 所有子標籤
批次建立使用者	指定資源和發起使用者建立請求 (對於個別使用者並使用批次作業)。	**帳號** — **列出帳號** (僅建立)、**尋找使用者**、**啟動批次處理動作**子標籤 **作業** — 所有子標籤
批次刪除使用者	刪除 Identity Manager 使用者帳號；取消佈建、取消指定與取消連結資源帳號 (對於個別使用者並使用批次作業)。	**帳號** — **列出帳號** (僅建立)、**尋找使用者**、**啟動批次處理動作**子標籤 **作業** — 所有子標籤
批次刪除 IDM 使用者	刪除現有 Identity Manager 使用者帳號 (對於個別使用者並使用批次作業)。	**帳號** — **列出帳號** (僅刪除)、**尋找使用者**、**啟動批次處理動作**子標籤 **作業** — 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]** (僅取消佈建)、**[Find Users]**、**[Launch Bulk Actions]** 子標籤 **作業** — 所有子標籤
批次停用使用者	停用現有使用者和資源帳號 (對於個別使用者並使用批次作業)。	**帳號** — **列出帳號** (僅停用)、**尋找使用者**、**啟動批次處理動作**子標籤 **作業** — 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)。	**帳號** — **列出帳號** (僅啟用)、**尋找使用者**、**啟動批次處理動作**子標籤 **作業** — 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]** (僅取消指定)、**[Find Users]**、**[Launch Bulk Actions]** 子標籤 **作業** — 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]** (僅取消連結)、**[Find Users]**、**[Launch Bulk Actions]** 子標籤 **作業** — 所有子標籤
批次更新使用者	更新現有使用者和資源帳號 (對於個別使用者並使用批次作業)。	**帳號** — **列出帳號** (僅更新)、**尋找使用者**、**啟動批次處理動作**子標籤 **作業** — 所有子標籤

批次使用者帳號管理員	對使用者執行所有一般和批次作業。	**帳號** — 所有子標籤 **密碼** — 所有子標籤 **作業** — 所有子標籤
權能管理員	建立、修改和刪除權能。	**配置** — **權能**子標籤
變更帳號管理員	對現有使用者執行所有作業，包括指定權能，但刪除作業除外。不包括批次作業	**帳號** — 所有子標籤。無法刪除使用者。 **密碼** — 所有子標籤 **核准** — 所有子標籤 **作業** — 所有子標籤 **報告** — 在範圍內建立管理員與使用者報告、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。	**作業** — **尋找作業**、**所有作業**、**執行作業**子標籤 **資源** — 對於 Active Sync 資源：編輯動作功能表，編輯 Active Sync 參數
變更密碼管理員	變更使用者和資源帳號密碼。	**帳號** — **列出帳號**、**尋找使用者**子標籤 (僅限「變更密碼」 **密碼** — 所有子標籤 **作業** — 所有子標籤。僅限「匯出密碼掃描」作業 (從**執行作業**子標籤)
變更密碼管理員 (需要驗證)	在成功驗證使用者身份認證問題答案後，變更使用者和資源帳號密碼。	**帳號** — **列出帳號**、**尋找使用者**子標籤 (僅限「變更密碼」；必須先驗證再進行下一個動作) **密碼** — 所有子標籤 **作業** — 所有子標籤。僅限「匯出密碼掃描」作業 (從**執行作業**子標籤)
變更資源密碼管理員	變更資源管理員帳號密碼。	**Tasks** — 所有子標籤 **資源** — **列出資源**子標籤。僅變更密碼 (從動作功能表中的**管理連線 --> 變更密碼**)

變更使用者帳號管理員	對現有使用者執行所有作業，但刪除作業除外。不包括批次作業	**帳號** — **列出帳號**、**尋找使用者**子標籤 無法建立、刪除或指定給使用者的權能。 **密碼** — 所有子標籤 **作業** — 所有子標籤
配置稽核	配置在系統中所稽核的活動。	**配置** — **稽核事件**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)	**作業** — **尋找作業**、**全部作業**、**執行作業** **資源** — 對於 Active Sync 資源：Active Sync 動作功能表 (所有選擇)
建立使用者	指定資源和發起使用者建立請求。不包括批次作業	**帳號** — **列出帳號** (僅建立)、**尋找使用者**子標籤 **作業** — 所有子標籤
刪除使用者	刪除 Identity Manager 使用者帳號；取消佈建、取消指定與取消連結資源帳號。不包括批次處理作業。	**帳號** — **列出帳號** (僅刪除)、**尋找使用者**子標籤 **作業** — 所有子標籤
刪除 IDM 使用者	刪除 Identity Manager 使用者帳號。不包括批次處理作業。	**帳號** — **列出帳號** (僅刪除)、**尋找使用者**子標籤 **作業** — 所有子標籤
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]** (僅取消佈建)、**[Find Users]** 子標籤 **作業** — 所有子標籤
停用使用者	停用現有的使用者和資源帳號。不包括批次作業	**帳號** — **列出帳號** (僅停用)、**尋找使用者**子標籤 **作業** — 所有子標籤
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	**帳號** — **列出帳號** (僅啟用)、**尋找使用者**子標籤 **作業** — 所有子標籤
匯入使用者	從定義的資源匯入使用者。	**帳號** — **擷取至檔案**、**從檔案載入**、**從資源載入**子標籤
匯入 / 匯出管理員	匯入和匯出所有類型的物件。	**配置** — **匯入交換檔案**子標籤
授權管理員	設定 Identity 系統產品授權	提供 `lh 授權`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。	**配置** — **登入**子標籤
組織管理員	建立、編輯和刪除組織。	**帳號** — **列出帳號**子標籤 (僅限編輯和建立組織與目錄結合、刪除組織)
密碼管理員	變更和重設使用者與資源帳號密碼。	**帳號** — **列出帳號** (僅限列出、變更及重設密碼)、**尋找使用者**子標籤 **密碼** — 所有子標籤 **作業** — 所有子標籤
密碼管理員 (需要驗證)	在成功驗證使用者的身份認證問題答案後，變更和重設使用者與資源帳號密碼。	**帳號** — **列出帳號** (僅限列出、變更及重設密碼；必須先驗證再進行下一個動作)、**尋找使用者**子標籤 **密碼** — 所有子標籤 **作業** — 所有子標籤
策略管理員	建立、編輯和刪除策略。	**配置** — **策略**子標籤
調解管理員	編輯調解策略和控制調解作業。	**作業** — 所有子標籤 (檢視調解作業)。 **資源** — **列出資源**子標籤。
調解報告管理員	建立、編輯、刪除和執行調解報告。	**報告** — **執行報告** (僅限帳號索引報告)、**管理報告**子標籤
調解請求管理員	管理調解請求。	**作業** — 所有子標籤 **資源** — **列出資源**子標籤 (僅限列出及調解功能)。
Remedy 整合管理員	修改 Remedy 整合配置。	**作業** — 所有子標籤 (檢視作業，執行角色同步化)。 **配置** — **Remedy 整合**子標籤
重新命名使用者	重新命名現有的使用者和資源帳號。	**帳號** — 列出帳號子標籤 (列出範圍中的所有帳號、重新命名使用者)
報告管理員	配置稽核設定和執行所有報告類型。	**作業** — 所有子標籤 (檢視作業，執行角色同步化)。 **報告** — 所有子標籤

重設密碼管理員	重設使用者和資源帳號密碼。	**帳號** — **列出帳號、尋找使用者**子標籤 (僅限 「重設密碼」 **密碼** — 所有子標籤 **作業** — 所有子標籤。僅限 「匯出密碼掃描」作業 (從**執行作業**子標籤)
重設密碼管理員 (需要驗證)	在成功驗證使用者的身份認證問題答案後，重設使用者和資源帳號密碼。	**帳號** — **列出帳號、尋找使用者**子標籤 (僅重設密碼；必須先驗證再進行下一個動作) **密碼** — 所有子標籤 **作業** — 所有子標籤。僅限 「匯出密碼掃描」作業 (從**執行作業**子標籤)
重設資源密碼管理員	重設資源管理員帳號密碼。	**作業** — **尋找作業**、**所有作業**、**執行作業**子標籤 **資源** — **列出資源**子標籤。僅重設資源 (從動作功能表中的 **[Manage Connection] --> [Reset Password]**)
資源管理員	建立、修改和刪除資源。	**報告** — 資源使用者報告及資源群組報告會傳回範圍外資源上的錯誤。 **資源** — **列出資源**子標籤 (編輯全域策略、編輯參數、資源群組。無法管理連線或資源物件)。
資源群組管理員	建立、編輯和刪除資源群組。	**資源** — **列出資源群組**子標籤
資源物件管理員	建立、修改和刪除資源物件。	**作業** — **尋找作業**、**所有作業**、**執行作業**子標籤 (檢視與資源物件有關的作業)。 **資源** — **列出資源**子標籤 (僅限列出及管理資源物件)。
資源密碼管理員	變更和重設資源代理帳號密碼。	**作業** — **尋找作業**、**所有作業**、**執行作業**子標籤 **資源** — **列出資源**子標籤。僅變更密碼 (從動作功能表中的**管理連線 --> 變更密碼**)
資源報告管理員	建立、編輯、刪除和執行資源報告。	**報告** — 所有子標籤 (僅限資源報告)

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。	**作業** — **尋找作業**、**所有作業**、**執行作業**子標籤 (同步化角色) **角色** — 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。	**報告** — 僅限角色報告
執行管理員報告	執行管理員報告。	**報告** — 僅限管理報告。
執行稽核報告	執行稽核報告。	**報告** — 僅限稽核記錄報告及使用情況報告
執行調解報告	執行調解報告。	**報告** — 僅限稽核記錄報告及使用情況報告
執行資源報告	執行資源報告。	**報告** — 僅限稽核記錄報告及使用情況報告
執行風險分析	執行風險分析。	
執行角色報告	執行角色報告。	**報告** — 僅限角色報告
執行作業報告	執行作業報告。	**報告** — 僅限作業報告
執行使用者報告	執行使用者報告。	**報告** — 僅限使用者報告
安全管理員	建立具有權能的管理員、管理加密金鑰、登入配置和策略。	**帳號** — **列出帳號** (刪除、建立、更新、編輯、變更及編輯密碼)、**尋找使用者**子標籤 (稽核報告) **密碼** — 所有子標籤 **作業** — **尋找作業**、**所有作業**、**執行作業**子標籤 **報告** — 所有子標籤 **資源** — **列出資源** (列出及控制資源物件)。 **配置** — **策略**、**登入**子標籤
作業報告管理員	建立、編輯、刪除和執行作業報告。	**報告** — 建立及管理作業報告
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]** (僅取消指定)、**[Find Users]** 子標籤 **作業** — 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]** (僅取消連結)、**[Find Users]** 子標籤 **作業** — 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。	**帳號** — **列出帳號** (僅解除鎖定)、**尋找使用者**子標籤。 **作業** — **尋找作業**、**所有作業**、**執行作業**子標籤
更新使用者	編輯現有使用者和發起使用者更新請求。	**帳號** — 編輯和更新使用者 **作業** — 管理現有作業 (從**全部作業**子標籤)
使用者帳號管理員	對使用者執行所有作業。	**帳號** — **列出帳號**、**尋找使用者**、**擷取至檔案**、**從檔案載入**、**從資源載入**子標籤。無法指定使用者權能 (在**列出帳號**子標籤上的**安全性**表單標籤)。 **作業** — **尋找作業**、**所有作業**、**執行作業**子標籤
使用者報告管理員	建立、編輯、刪除和執行使用者報告。	**報告** — 執行使用者報告。
檢視使用者	檢視個別使用者詳細資訊。	**帳號** — 從清單選取使用者以檢視個別使用者帳號資訊。不允許執行變更動作。
Waveset 管理員	執行系統範圍的作業，如修改系統配置物件。	**作業** — 所有子標籤。同步化角色、編輯來源配接卡範本，並排程報告。 **報告** — 所有子標籤 **資源** — 列出資源 (僅列出，不允許變更動作) **配置** — **稽核事件**、**電子郵件範本**、**表單與程序對映**子標籤

表 1. Identity Manager 權能說明

瞭解管理員角色

管理員角色能指定管理員所管理的一組組織之唯一權能集。會給管理員角色指定各種權能和受控組織，隨後便可將該角色指定給管理使用者。

指派給管理員角色的權能和組織可為：

- **Direct** — 此選項可讓您將特定權能、控制的組織或將這兩者指定給管理員角色。
- **Dynamic** (間接) — 此選項使用權能和控制的組織**規則**動態決定，指定的使用者每次登入 Identity Manager 時，透過管理員角色賦予該使用者的權能和控制的組織。

附註　關於設定這些規則的關鍵資訊，請參閱權能規則與控制的組織規則。

您可以指定一或多個管理員角色給每位使用者。而同一個管理員角色可以指定給一或多個使用者。

使用者管理員角色

Identity Manager 包含內建管理員角色，標題為「User」。依預設，它不包含權能或控制的組織指定，且無法刪除。此管理員角色在登入時默認指定給所有使用者 (一般使用者與管理員)

您可以透過管理員介面編輯使用者管理員角色 (選取 **[Configure]**，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、所屬的部門或是否為管理員) 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」的模式。

然而，當使用者應該具有特定權限在工作流程外或工作流程內存取一個或多個物件時，則透過使用者管理員角色動態指定權能和控制的組織，會啟動對這些物件的動態、細致認證。

範例

以下範例中的步驟說明如何在動態環境中使用使用者管理員角色。

1. 建立 ou 的兩個 Active Directory：
   - "Chicago Cubs" && "New York Yankees"
2. 在每個 ou 中建立三個 Active Directory 使用者，使用以下屬性集：
   - Chicago Cubs:
     - Dusty Baker (title = 'manager', manager = '')
     - Kerry Woods (title = 'pitcher', manager = 'Dusty Baker')
     - Mark Prior (title = 'pitcher', manager = 'Dusty Baker')
   - New York Yankees
     - Joe Torre (title = 'manager', manager = '')
     - Alex Rodriguiz (title = '3rd', manager = 'Joe Torre')
     - Derek Jeter (title = 'shortstop', manager = 'Joe Torre')
3. 將以下規則指定給使用者管理員角色：
   - capabilitesRule ==> If Team Manager Assign Account Admin Capability
   - controlledOrganizationsRule ==> If Team Manager Assign Control of My Team
4. 建立 Identity Manager 組織 (名為 「My Team」) 並指定：
   - userMembersRule ==> Get My Team

當使用者登入時，則：

- 如果使用中的目錄 Active Directory 使用者標題為 「manager」，則他將被指定 「帳號管理員」權能及 「My Team」組織的控制權。
- 如果 AD 使用者標題不是 「manager」，則他不會被指定任何權能或控制任何組織。
- 如果登入使用者的標題為 「manager」，則當 「My Team」組織開啟後，「Get My Team」規則將在 Active Directory 上呼叫 getResourceObjects，請求所有 「manager」為 accountInfo.accounts[AD].accountId 的使用者立即登入。

此設定將使管理員登入使用者介面來管理他們的雇員，並禁止雇員登入使用者介面後執行管理功能。

建立和編輯管理員角色

若要建立或編輯管理員角色，必須要為您指定「管理員角色管理員」權能。若要存取管理員角色區，按一下**配置**，然後按一下**管理員角色**。[管理員角色] 清單頁可讓您建立、編輯和刪除 Identity Manager 中的管理員角色。

若要編輯現有的管理員角色，請按一下清單中的名稱。按一下**新增**建立管理員角色。Identity Manager 會顯示 [建立管理員角色] 頁，您可以於其中指定新管理員角色的權能和範圍。

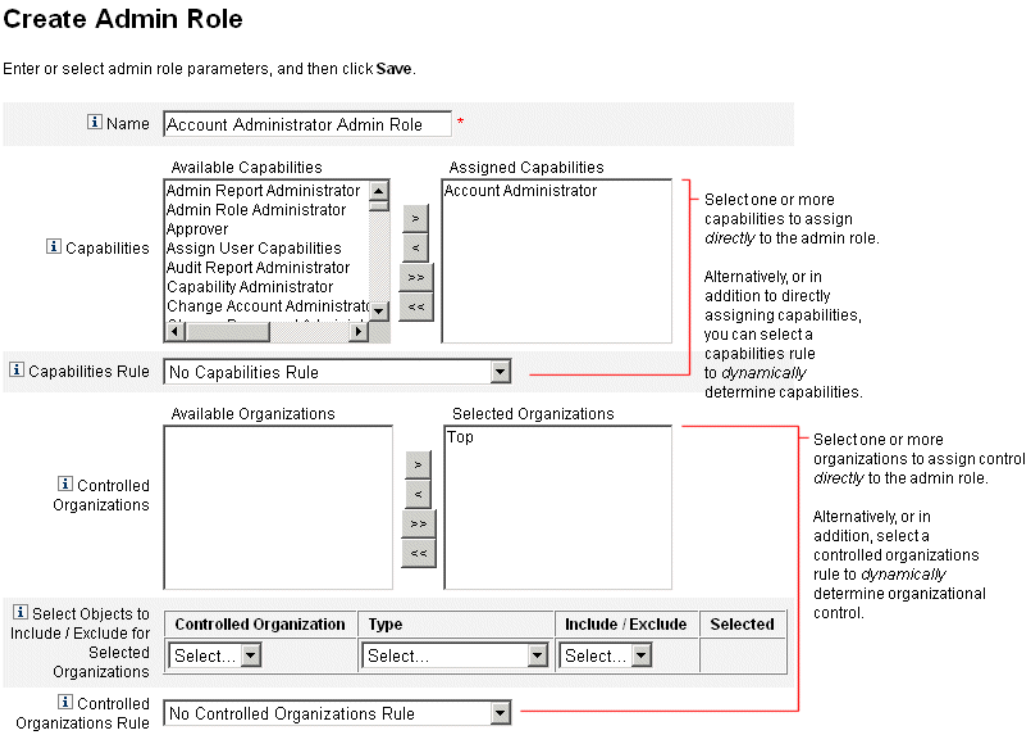


圖 8. 管理員角色：建立頁

設定控制組織的範圍

對於包含在管理員角色中的每個直接指定的控制組織，您可以定義使用者可於其中執行動作的物件範圍。您可以選擇包括或排除一個或多個物件，這些物件通常可用於每個由使用者控制的組織。

例如，您可以選擇限制可在組織內建立、更新並刪除使用者的使用者之存取權，該組織包括組織內特定資源子集範圍內的各種資源。若要這麼做，您可以用這些特性建立管理員角色：

- 名稱 — NT 使用者管理員
- 權能 — 建立使用者、更新使用者、刪除使用者
- 控制的組織 — **組織名稱**
- 包括的資源 — NT

若要這麼做，在 [建立管理員角色] 頁的 [選取要包含 / 排除的物件] 區中進行選取。

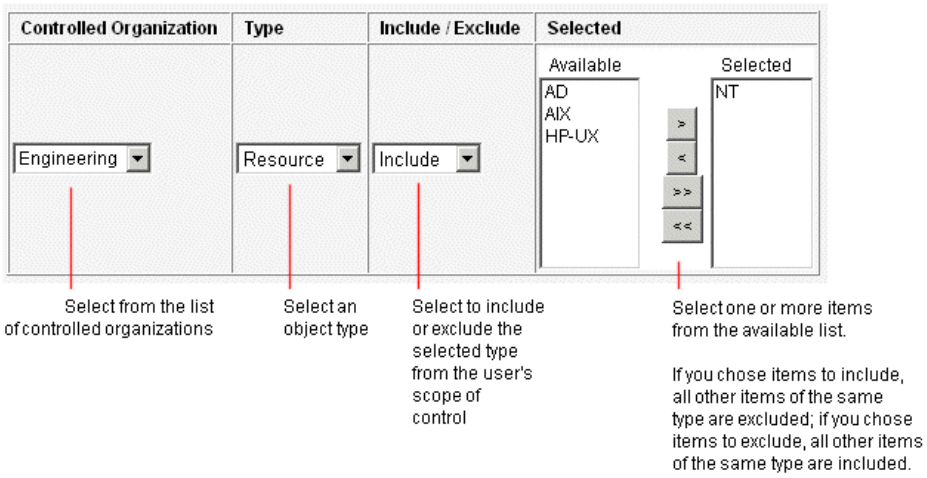


圖 9. 管理員角色：針對控制組織的包含 / 排除選項

如果您將一個項目同時包含在包含與排除清單中，則將會從管理員角色中將其排除。

將使用者表單指定給管理員角色

您可將使用者表單指定為管理員角色的一個屬性。被指定管理員角色的管理員在其管理員角色控制的組織中建立或編輯使用者時，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為其成員的組織，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指定給管理員，或透過管理員角色間接指定，則會使用指定給管理員的成員組織的使用者表單（從管理員的成員組織開始，直到「頂層」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。

權能規則與控制的組織規則

下列範例顯示您如何設定權能規則或控制的組織規則，這些規則可以動態控制指定的權能或是賦予給使用者（已為其指定管理員角色）的控制組織。

附註 如需有關在 Identity Manager 中建立和使用規則的資訊，請參閱「Identity Manager 部署工具」。

權能規則：金鑰定義與內含項

- 權能規則必須包含 authType=’ CapabilitiesRule’項目。這是確保您可以從管理員角色頁中選取規則所必需的。
- 上下文是目前認證的 Identity Manager 使用者的使用者視圖。
- 在下列範例規則中，定義的變數 (defvar)「user groups」在名為「ranger-AD」的 Windows Active Directory 伺服器上取得目前認證的 Identity Manager 使用者的帳號，並傳回使用者目前為其所屬成員的群組清單。
- 條件邏輯 (cond) 檢查目前認證的 Identity Manager 使用者是否為「manager」群組的成員。如果是，則會為使用者指定 Identity Manager 權能「登入管理員」和「資源管理員」。如果不是，則不會指定任何 Identity Manager 權能。

範例權能規則

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Rule PUBLIC 'waveset.dtd' 'waveset.dtd'>
<Rule authType='CapabilitiesRule' name='If Manager'>
   <block>
      <defvar name='user groups'>
         <get>
            <invoke name='getResourceObject'
              class='com.waveset.ui.FormUtil'>
         <ref>context</ref>
            <s>ranger-AD</s>
            <s>User</s>
         <ref>accountInfo.accounts[ranger-AD].accountId</ref>
         <map>
            <s>searchAttrsToGet</s>
               <list>
            <s>memberOf</s>
               </list>
         </map>
         </invoke>
            <s>user.attributes.memberOf</s>
         </get>
      </defvar>
   <cond>
      <contains>
         <ref>user groups</ref>
            <s>CN=manager,DC=dev-ad,DC=waveset,DC=com</s>
      </contains>
      <list>
         <s>Login Administrator</s>
```

```
         <s>Resource Administrator</s>
      </list>
   </cond>
   </block>
   <MemberObjectGroups>
      <ObjectRef type='ObjectGroup'
id='#ID#ObjectGroup:Waveset'        name='Waveset'/>
   </MemberObjectGroups>
</Rule>
```

控制的組織規則：金鑰定義

- 控制的組織規則必須包含 authType=’ ControlledOrganizationsRule’ 項目。這可讓您從管理員角色頁中選取規則。
- 上下文是目前認證的 Identity Manager 使用者的使用者視圖。
- 在下列範例規則中，定義的變數 (defvar)「user groups」在名為「ranger-AD」的 Windows Active Directory 伺服器上取得目前認證的 Identity Manager 使用者的帳號，並傳回使用者目前為其所屬成員的群組清單。
- 條件邏輯 (cond) 檢查目前認證的 Identity Manager 使用者是否為「manager」群組的成員。如果是，則會為使用者指定 Identity Manager「Waveset」組織的控制權。如果不是，則不會指定任何組織控制權。

範例控制組織規則

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Rule PUBLIC 'waveset.dtd' 'waveset.dtd'>
<Rule authType='ControlledOrganizationsRule' name='Get managed
departments'>
   <block>
      <defvar name='user groups'>
         <get>
            <invoke name='getResourceObject'
              class='com.waveset.ui.FormUtil'>
            <ref>context</ref>
               <s>ranger-AD</s>
               <s>User</s>
            <ref>accountInfo.accounts[ranger-
AD].accountId</ref>
            <map>
               <s>searchAttrsToGet</s>
            <list>
               <s>memberOf</s>
```

```
            </list>
            </map>
         </invoke>
            <s>user.attributes.memberOf</s>
         </get>
      </defvar>
   <cond>
      <contains>
      <ref>user groups</ref>
         <s>CN=manager,DC=dev-ad,DC=waveset,DC=com</s>
   </contains>
      <list>
         <s>Waveset</s>
      </list>
     </cond>
   </block>
   <MemberObjectGroups>
   <ObjectRef type='ObjectGroup' id='#ID#ObjectGroup:Waveset'
       name='Waveset'/>
   </MemberObjectGroups>
</Rule>
```

瞭解電子郵件範本

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：

- **帳號建立核准** — 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。
- **帳號建立通知** — 傳送已使用指定的特定角色建立帳號的通知。在 [建立角色」或 [編輯角色] 頁面的 [通知收件人] 欄位中選取一或多位管理員時，系統將傳送此通知。
- **密碼重設** — 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。
- **密碼同步化通知** — 通知使用者已在所有資源上成功完成密碼變更。通知會列出已成功更新的資源，並指出密碼變更請求的來源。
- **密碼同步化失敗通知** — 通知使用者在所有資源上未成功完成密碼變更。通知會提供錯誤清單並指出密碼變更請求的來源。

- **調解帳號事件**、**調解帳號事件**、**調解摘要** — 分別從「通知調解回應」、「通知調解開始」和「通知調解完成」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。
- **報告** — 將產生的報告傳送給指定的收件者清單中的收件者。
- **請求資源** — 將已請求資源的通知傳給資源管理員。當管理員從 [資源] 區域中請求資源時，系統會傳送此通知。
- **重試通知** — 傳送通知給管理員，說明對資源所進行的特定作業嘗試失敗達到指定的次數。
- **風險分析** — 傳送風險分析報告。將一或多名電子郵件收件人指定為資源掃描的部分時，系統將傳送此報告。
- **臨時密碼重設** — 將已提供給帳號的臨時密碼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。

自訂電子郵件範本

您可以自訂電子郵件範本以便為收件人提供特定的方向，告知對方如何完成作業或檢視結果。例如，您可能想要自訂 [帳號建立核准] 範本，將核准人導向帳號核准頁面：

請前往 http://host.example.com:8080/idm/approval/approval.jsp 來核准為 $ （完整名稱） 所建立的帳號。

若要自訂「帳號建立核准」範本：

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 [帳號建立核准] 範本：

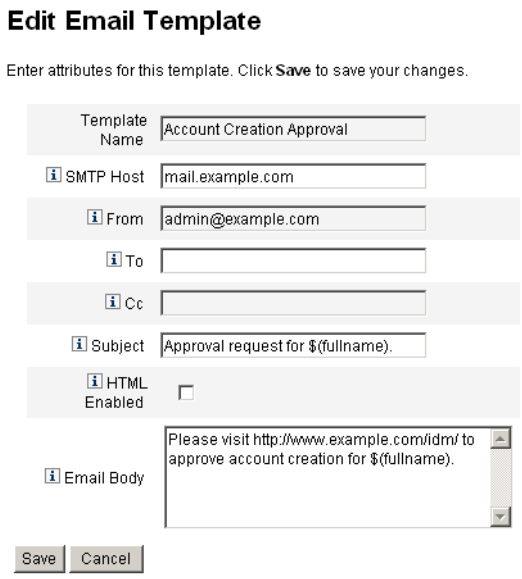


圖 10. 自訂電子郵件範本

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

附註 您也可以使用 「業務程序編輯器」 (BPE) 修改電子郵件範本。如需有關 BPE 的詳細資訊，請參閱 「Identity Manager 部署工具」。

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。若要啟用 HTML 格式的內容，請選取 [啟用 HTML] 選項。

電子郵件內文中允許的變數

您也可以在電子郵件範本內文中包含變數的參照，格式為 $(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。

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

表 2. 電子郵件範本變數

稽核群組配置

設定稽核配置群組可讓您記錄和報告您選取的系統事件。

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 Events]**。

[稽核事件] 頁會顯示稽核配置群組的清單，這些群組可能分別包含一或多個事件。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配置群組以顯示 [編輯稽核配置群組] 頁面。此頁可讓您選取要在系統稽核記錄中當作稽核配置群組的一部份來記錄的稽核事件類型。

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。若要執行這個動作，請將該物件類型的 [動作] 欄中的項目從 [可用的] 移至 [已選取的] 區域，然後按一下 **確定**。

新增事件到稽核配置群組

若要將事件增加到群組，請按一下 **[New]**。Identity Manager 會在頁面底部新增事件。從 [物件類型] 欄的清單中選取物件類型，然後將新物件類型的 [動作] 欄中的一或多個項目從 [可用的] 區域移至 [已選取的] 區域。按一下 **[確定]**，將事件增加到群組中。

Remedy 整合

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

在管理員介面的兩個區域中設定 Remedy 整合：

- **Remedy 伺服器設定** — 透過從資源區域建立 Remedy 資源來設定 Remedy 配置。在設定資源後，測試連線以確保啟用整合。
- **Remedy 範本** — 在設定 Remedy 資源後，定義 Remedy 範本。若要如此，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啟 Remedy 票證。如需有關配置工作流程的更多資訊，請參閱「Identity Manager 工作流程、表單與視圖」。

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。若要如此，請選取 **[Configure]**，然後選取 **[Servers]**。

若要編輯個別伺服器的設定，請選取 [配置伺服器] 頁面中清單內的伺服器。Identity Manager 會顯示 [編輯伺服器設定] 頁面，在此您可以編輯調解器和排程程式設定。

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取消選取 [使用] 預設選項來指定設定值：

- **平行資源限制** — 指定調解器可以同時處理的最大資源數目。
- **最小工作者執行緒數** — 指定調解器會一直持續作用的執行緒數目。
- **最大工作者執行緒數** — 指定調解器可以使用的最大處理中執行緒數目。調解器只會啟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 [編輯伺服器設定] 頁上的**排程程式**以顯示排程程式選項。您可以接受預設值或取消選取 [使用] 預設選項來指定設定值：

- **Scheduler Startup** — 選取排程程式的啟動模式：
  - **Automatic** — 伺服器啟動時即啟動。這是預設的啟動模式。
  - **Manual** — 伺服器啟動時啟動，但在手動啟動之前保持暫停狀態。
  - **Disabled** — 伺服器啟動時不啟動。
- **Tracing Enabled** — 選取此選項即可啟動標準輸出的排程程式除錯追蹤。
- **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**儲存**來儲存伺服器設定的變更。

編輯預設伺服器設定

預設伺服器設定功能可讓您為所有的 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**編輯預設伺服器設定**。[編輯預設伺服器設定] 頁面顯示與個別伺服器設定頁面一樣的選項。

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 [使用] 預設選項。

按一下**儲存**來儲存伺服器設定的變更。

簽署的核准

使用以下資訊與程序來設定數位簽署的核准。執行以下作業的步驟與範例：

- 配置簽署的核准 (伺服器端與用戶端)
- 將憑證與 CRL 增加至 Identity Manager
- 簽署核准

配置簽署的核准

遵循下列步驟來配置簽署的核准。

伺服器端配置

啟用伺服器端配置：

1. 在系統配置中，設定 `security.nonrepudiation.signedApprovals=true`
2. 將您的認證機構 (CA) 的憑證增加為可信任的憑證。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 做為可信任的憑證：

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

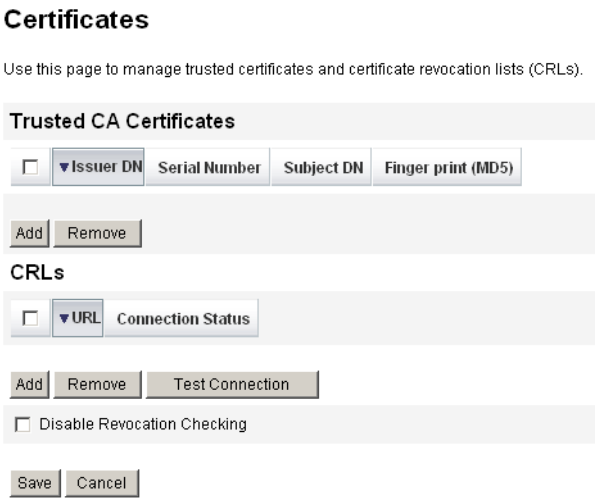


圖 11. 憑證

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) 為被撤銷或無效的憑證序列號之清單。
- CA CRL 的 URL 可以為 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]** 以確認該 URL。
6. 按一下**儲存**。
7. 使用 jarsigner 簽署 applets/ts1.jar。

附註 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。

用戶端配置

遵循下列步驟來啟用用戶端配置：

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，並使用管理權限登入。
2. 選取 [Request a certificate]，然後按一下 **[Next]**。
3. 選取 [Advanced request]，然後按一下 **[Next]**。
4. 按一下**下一步**。
5. 選取憑證範本使用者。
6. 選取下列選項：
   a. Mark keys as exportable
   b. Enable strong key protection
   c. Use local machine store
7. 按一下 **[Submit]**，然後按一下 **[OK]**。
8. 按一下 **[Install this certificate]**。
9. 選取 [Run] —> [mmc] 來啟動 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. 按一下 **[Next]**，然後按一下 **[Finish]**。
    e. 按一下 **[Close]**。
    f. 按一下 **[確定]**。
    g. 移至 [Certificates]—>[Personal]—>[Certificates]。
    h. 以滑鼠右鍵按一下 [Administrator All Tasks]ó>[Export]。
    i. 按一下**下一步**。
    j. 按一下 **[Next]** 來確認匯出私密金鑰。
    k. 按一下**下一步**。
    l. 提供密碼，然後按一下 **[Next]**。
    m. 將 ***CertificateLocation*** 歸檔。
    n. 按一下 **[Next]**，然後按一下 **[Finish]**。按一下 **[OK]** 來確認。

簽署核准

遵循下列步驟來簽署核准。

1. 從 Identity Manager 管理員介面，選取 **[Approvals]**。
2. 從清單中選取核准。
3. 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。
4. 按一下 **[Always]**。

   Identity Manager 將顯示一個註有日期的核准摘要。
5. 輸入或按一下 [Browse] 來尋找金鑰庫的位置 (伺服器端配置程序的步驟 10m 提供此位置)。
6. 輸入金鑰庫密碼 (伺服器端配置程序的步驟 10l 提供此密碼)。
7. 按一下 **[Sign]** 來核准請求。

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。)

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]** 來儲存報告，並返回至 [Run Reports] 頁面。
7. 按一下 **[Run]** 來執行該核准報告。
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

6 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。

本章主題

在本章中，您將學習關於下列項目的更多內容：

- Identity Manager 資料同步化工具 (探索、調解和 ActiveSync)
- 如何使用探索、調解和 ActiveSync 功能使資料保持常新

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。

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	ActiveSync (多重資源實施)

探索

Identity Manager 帳號探索功能有助於推進快速部署與加速帳號建立的作業。這些功能的說明如下：

- **擷取至檔案** — 將資源介面傳回的資源帳號擷取至檔案 (CSV 或 XML 格式)。在將資料匯入 Identity Manager 之前，您可以處理這個檔案。
- **從檔案載入** — 讀取檔案 (CSV 或 XML 格式) 中的帳號並將其載入 Identity Manager。
- **從資源載入** — 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**下載**。Identity Manager 顯示 [檔案下載] 對話方塊，您可以在此對話方塊中選擇儲存或檢視擷取的檔案。

提示　如果您選擇開啟檔案，則可能需要選取檢視檔案的程式。

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，資料檔案一般為 CSV 格式。

關於 CSV 檔案格式

待載入的帳號常在試算表 (如 Excel) 中列出，並儲存為逗號分隔值 (CSV) 格式，以便載入 Identity Manager。CSV 檔案內容必須遵循以下格式指導原則：

行 1 — 列出每個欄位的欄標題或模式屬性 (以逗號分隔)。

行 2 到結尾 — 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：

```
firstname,middleinitial,lastname,accountId,asciipassword,EmployeeID,Department,Ph
John,Q,Example,E1234,E1234,1234,Operations,555-222-1111
Jane,B,Doe,E1111,E1111,1111,,555-222-4444
```

在本範例中，第二位使用者 (Jane Doe) 不隸屬於任何部門。缺少的值以相鄰逗號 (,,) 表示。

若要載入帳號：

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

   Identity Manager 顯示 [從檔案載入] 頁面，讓您可以先指定載入選項後再繼續：

   - **使用者表單** — 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。
   - **帳號相互關聯規則** — 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。
   - **帳號確認規則** — 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 [無確認規則]，Identity Manager 會接受所有可能的所有者而不進行確認。

附註 在您的環境中，如果相互關聯規則只會為各個帳號選取最多一位所有者，則您不需使用確認規則。

- **僅載入相符帳號** — 選取此選項可僅將符合現有 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。
- **更新屬性** — 選取此選項會將目前 Identity Manager 使用者屬性值替代為載入帳號的屬性值。
- **合併屬性** — 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 [更新屬性] 選項。
- **結果層級** — 選取一個臨界值，達到該臨界值時，載入程序便會記錄帳號的個別結果：
  - **僅在出錯時** — 僅當載入帳號發生錯誤訊息時才記錄個別結果。
  - **警告與出錯時** — 載入帳號發生警告或錯誤訊息時記錄個別結果。
  - **參考性與其他** — 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，您必須為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為基礎；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。

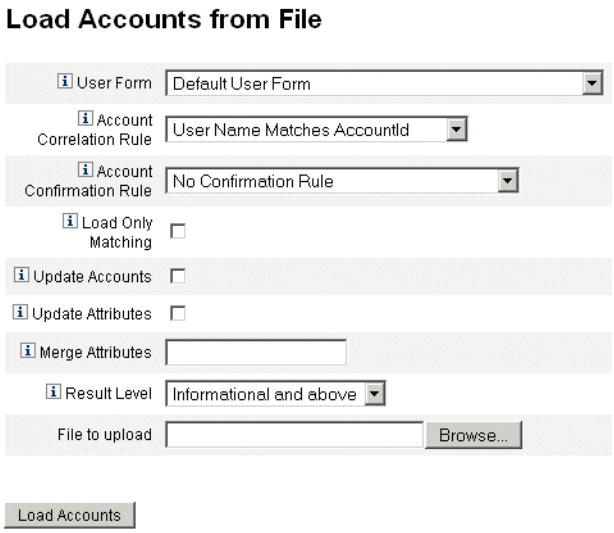


圖 1. 從檔案載入

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當檔案載入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，那麼就會停止剖析。

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]**。

附註 Identity Manager 讓您可以先指定載入選項後再繼續。[從資源載入] 頁面中的載入選項及產生的動作與 [從檔案載入] 頁面的相同。

調解

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。

由於調解是針對進行中的比較而設計，因此它：

- 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)
- 能夠提供遞增模式 (探索始終為完整模式)。
- 可偵測原生變更 (探索則不行)

您也可以將調解配置為在資源處理的下列各點啟動強制工作流程：

- 在調解任何帳號之前
- 在每個帳號中
- 在調解所有帳號之後

從 [資源] 區域存取 Identity Manager 調解功能。[資源] 清單會顯示每個資源上次調解的時間以及其目前的調解狀態。

關於調解策略

調解策略可讓您按照資源為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 options] 清單中，選取 [Edit Reconciliation Policy]。

   Identity Manager 顯示 [編輯調解策略] 頁面，您可以在其中選取如下策略：

   - **調解伺服器** — 在叢集環境中，每個伺服器都可以執行調解。指定要對策略中的資源執行調解的 Identity Manager 伺服器。
   - **調解模式** — 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：
     - **完整式調解** — 針對完整性進行最佳化處理，但速度會變慢。
     - **漸進式調解** — 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 [不調解] 可停用對目標資源的調解。
   - **完整式調解排程** — 如果啟用了完整模式調解，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 [繼承] 選項可繼承更高層級策略中的指定排程。
   - **漸進式調解排程** — 如果啟用了漸進式調解，它會按固定的排程自動執行。指定應對策略中的資源執行漸進式調解的頻率。選取 [繼承] 選項可繼承更高層級策略中的指定排程。

附註　並非所有資源都支援漸進式調解。

   - **屬性層級調解** — 可以配置調解，使其偵測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**調解後的帳號屬性**內所指定的屬性所作的原生變更。
   - **帳號相互關聯規則** — 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。

- **帳號確認規則** — 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 [無確認規則]，Identity Manager 會接受所有可能的所有者而不進行確認。

附註 在您的環境中，如果相互關聯規則只會為各個帳號選取最多一位所有者，則您不需使用確認規則。

- **代理管理員** — 指定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 [沒有代理管理員] 選項。選取此選項後，調解結果可供檢視，但不會執行回應動作或工作流程。

- **狀況選項** (與回應) — 調解可識別幾種狀況類型。在 [回應] 欄中指定調解應採取的任何動作：
  - **確認** — 預期的帳號已存在。
  - **刪除** — 預期的帳號不存在。
  - **找到** — 調解程序在指定資源中找到了相符帳號。
  - **缺少** — 在指定給使用者的資源上找不到相符帳號。
  - **衝突** — 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。
  - **未指定** — 調解程序在未指定給使用者的資源中找到了相符帳號。
  - **不相符** — 帳號與任何使用者均不相符。
  - **爭議** — 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)：
  - **根據資源帳號建立新的 Identity Manager 使用者** — 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。
  - **為 Identity Manager 使用者建立資源帳號** — 重建缺少的資源帳號，使用使用者表單重新產生資源帳號屬性。
  - **刪除資源帳號**與**停用資源帳號** — 刪除 / 停用資源的帳號。
  - **將資源帳號連結至 Identity Manager 使用者**與**取消資源帳號與 Identity Manager 使用者的連結** — 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。
- **調解前工作流程** — 可以配置調解，使其在調解資源前先執行使用者特定的工作流程。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 [不執行工作流程]。

- **視帳號而定的工作流程** — 可以配置調解，使其在回應資源帳號的狀況後執行使用者特定的工作流程。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 [不執行工作流程]。
- **調解後工作流程** — 可以配置調解，使其在完成資源調解後執行使用者特定的工作流程。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 [不執行工作流程]。

按一下**儲存**來儲存策略變更。

啟動調解

啟動調解作業時有兩個選項可以使用：

- 調解排程 — 您可在 [編輯調解策略] 頁面中設定調解排程，該排程會按固定間隔執行調解。
- 立即調解 — 立刻執行調解。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。如果該策略已經為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 [resource]，然後從 [Resource Actions] 清單中，選取 [Cancel Reconciliation]。

檢視調解狀態

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

- **不明** — 狀態不明。最近一次調解作業的結果無法使用。
- **停用** — 調解已停用。
- **失敗** — 最近一次的調解作業無法完成。
- **成功** — 最近一次的調解順利完成。
- **完成時有錯誤發生** — 最近一次的調解已完成，但完成時有錯誤發生。

附註　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。

附註　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 **[搜尋]** 來尋找符合所有搜尋條件的帳號。

- **資源帳號名稱** — 選取這個選項，選取一個修飾鍵 (開頭為、包含或是)，然後輸入部分或完整的帳號名稱。
- **資源為其中之一** — 選取這個選項，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中的已調解帳號。
- **所有者** — 選取這個選項，選取一個修飾鍵 (開頭為、包含或是)，然後輸入部分或完整的所有者名稱。若要搜尋無主帳號，請搜尋處於「不相符」(UNMATCHED) 或「爭議」(DISPUTED) 狀況的帳號。
- **狀況為其中之一** — 選取這個選項，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帳號。

按一下 **[搜尋]** 來根據您的搜尋參數來搜尋帳號。若要限制搜尋結果，您可選擇在 [將結果限制為前] 欄位中指定數目。預設限制為前 1000 個找到的帳號。

按一下 **[重設查詢]** 以清除頁面並選取新選項。

檢查帳號索引

還可以檢視所有 Identity Manager 使用者帳號，並可選擇為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 (不論其是否為 Identity Manager 使用者所擁有)。此資訊按資源或 Identity Manager 組織分組。若要變更此檢視，請從 [變更索引檢視] 清單中選擇一個檢視。

使用帳號

若要使用資源中的帳號，請選取 [按資源分組] 索引檢視。Identity Manager 會顯示每種資源類型的資料夾。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。

附註　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。

使用使用者

如要使用 Identity Manager 使用者，請選取 [按使用者分組] 索引檢視。在此檢視中，Identity Manager 使用者和組織會以與 [帳號清單] 頁面類似的階層顯示。若要察看目前指定給 Identity Manager 中的使用者的帳號，請瀏覽至該使用者，然後按一下使用者名稱旁邊的指示器。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。

ActiveSync 配接卡

Identity Manager ActiveSync 功能可使儲存在**授權外部資源**（如應用程式或資料庫）的資訊與 Identity Manager 使用者資料同步化。為 Identity Manager 資源設定使用中的同步化可讓它「偵聽」或輪詢授權資源是否發生變更。

設定使用中的同步化

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）引導您為資源設定使用中的同步化。

若要啟動 Active Sync 精靈，從資源清單中選取資源，然後在 [Resource Actions] 選項清單中，選取 [Active Sync Wizard]。

[Active Sync 精靈同步化模式] 頁面隨即出現。

同步化模式

[Synchronization Mode] 頁面可讓您決定在使用中的同步化設定期間，可以選擇的配置選項的範圍。

從這些選項中選取：

輸入表單用法 — 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 [預先存在的輸入表單] (預設值)，請為下列選項做出選擇：
  - **輸入表單** — 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。
  - **處理規則** — 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為何，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。

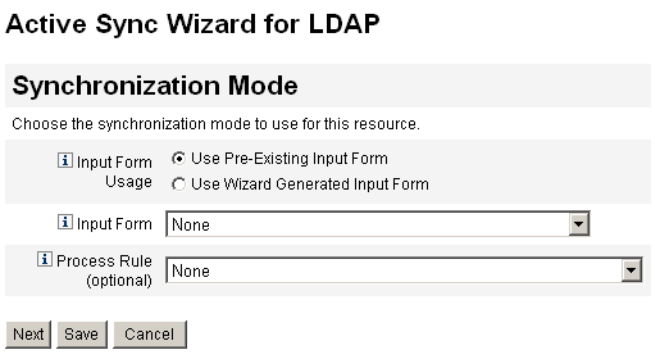


圖 2. Active Sync 精靈：同步化模式，預先存在的表單選擇

- 如果您選取 [使用由精靈產生的輸入表單]，請為下列選項做出選擇：
  - **配置模式** — 選取為 Active Sync 精靈使用基本模式，或是使用進階模式。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。
  - **處理規則** — (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為何，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。
  - **處理後表單** — (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。

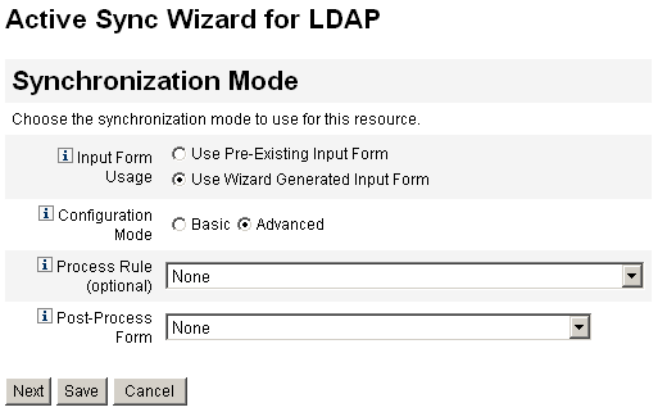


圖 3. Active Sync 精靈：同步化模式，精靈產生的表單選擇

按一下**下一步**繼續執行精靈。[Active Sync 執行設定] 頁面隨即出現。

執行設定

此頁面可讓您建立 Active Sync 的設定：

- 啟動
- 輪詢
- 記錄

啟動設定

選擇如何啟動 Active Sync：

- **啟動類型** — 選取下列選項之一：
  - **自動**或**以容錯轉移方式自動啟動** — 當 Identity 系統啟動時，啟動授權來源。
  - **手動** — 需要管理員啟動授權來源。
  - **停用** — 停用資源。
- **代理管理員** — 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開始日期與時間，則輪詢會在指定時間開始。如果設定了在過去發生的輪詢開始日期與時間，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」
- 將資源設定為每週輪詢一次，開始日期為 2005 年 7 月 4 日 (週一)，時間為上午 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。但是，建議您設定開始日期及時間；否則，每次重新啟動應用程式伺服器時，所有針對「使用中的同步化」配置的資源將立即開始輪詢。

選擇如何設定輪詢：

- **輪詢間隔** — 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。
- **輪詢開始日期** — 輸入第一個排定之間隔要開始的日期 (格式為 yyyyMMdd)。
- **輪詢開始時間** — 輸入第一個排定間隔開始的當天時間 (格式為 `HH:mm:ss`)。

記錄設定

選擇如何設定記錄資訊及層級：

- **最多記錄封存數量** — 如果此值大於 0，將會保留最近的 N 個記錄檔案。如果此值為零，將會重複使用單個記錄檔案。如果此值為 -1，則永不捨棄任何記錄檔案。
- **最長記錄有效期間** — 超過此段期間之後，將歸檔現用的記錄。如果時間為零，則不會執行定期封存。如果 [最多記錄封存數量] 為零，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 [最大記錄檔案大小] 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。
- **記錄檔案路徑** — 輸入要在其中建立現用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。
- **最大記錄檔案大小** — 以位元組為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 [最多記錄封存數量] 為零，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 [最長記錄有效期間] 中所指定的有效期間標準無關。

- **記錄層級** — 輸入記錄的層級：
  - 0 — 不記錄
  - 1 — 錯誤
  - 2 — 資訊
  - 3 — 詳細的
  - 4 — 除錯

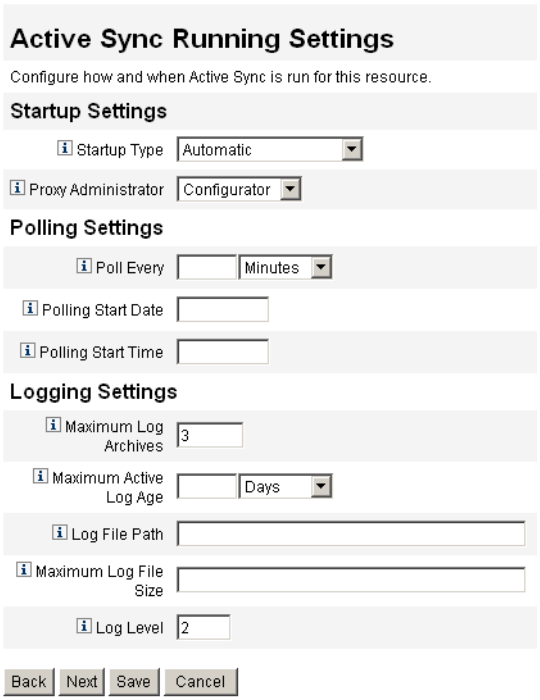


圖 4. Active Sync 精靈：執行設定

按一下**下一步**繼續執行精靈。[一般 Active Sync 設定] 頁面隨即出現。

一般 Active Sync 設定

使用此頁面指定一般 Active Sync 配置參數。

資源特定設定

附註 可用的資源特定設定會隨資源類型不同而有所不同。下列一或多個選擇可能不會出現。下列設定適用於 LDAP 資源。

- **要同步的物件類別** — 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。
- **要同步之帳號的 LDAP 篩選器** — 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。
- **要同步的屬性** — 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。若為空白 (預設值)，將會處理所有變更。
- **變更記錄區段大小** — 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。
- **變更數字屬性名稱** — 在變更記錄項目中輸入變更數字屬性的名稱。
- **篩選變更依據** — 輸入要從變更中篩選出來的目錄管理員名稱 (RDN)。符合此清單中之項目的 modifiersname 屬性變更將會被篩選出來。

標準值是此配接卡為避免迴圈而使用的管理員名稱。項目的格式應該為 cn=Directory Manager。

常用設定

- **相互關聯規則** — 選擇性地指定相互關聯規則，以置換資源調解策略中所指定的相互關聯規則。相互關聯規則會使資源帳號與 Identity 系統帳號相互關聯。
- **確認規則** — 選擇性地指定確認規則，以置換資源調解策略中所指定的確認規則。
- **解決處理規則** — 選擇性地指定當輸入的記錄有多個相符項目時所要執行的 TaskDefinition 之名稱。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。
- **刪除規則** — 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。
- **建立不相符的帳號** — 為 true 時，配接卡將嘗試建立在 Identity 系統中找不到的帳號。為 false 時，配接卡會根據 [解決處理規則] 傳回的處理程序來對帳號執行動作。

- **在建立事件時指定 Active Sync 資源** — 選取此選項時，Active Sync 來源資源將指定給偵測到建立事件時建立的使用者。
- **全域寫入** — 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)。
- **重設時忽略過去的變更** — 當配接卡首次啟動或重設時，選取忽略過去的變更。若要重設配接卡，請刪除配置物件 `IAPI_resourceName`。並非所有配接卡都可以使用此選項。
- **輪詢前工作流程** — 選取要在每個輪詢前立即執行的選擇性工作流程。
- **輪詢後工作流程** — 選取要在每個輪詢後立即執行的選擇性工作流程。

按一下**儲存**或**下一步**，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**儲存**，以完成精靈選擇並回到 [資源] 清單。
- 如果您正在使用由精靈產生的輸入表單，請按**下一步**以繼續。
  - 如果您正在使用**基本**配置模式，則會顯示 [目標資源] 頁面。(在本章節中直接跳至**目標資源**。)
  - 如果您正在使用**進階**配置模式，則會顯示 [事件類型] 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為在 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、啟用及重新命名。

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：

- **無** — 不忽略任何 Active Sync 事件。
- **規則** — 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。
- **條件** — 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 [編輯條件] 以使用 [條件面板] 定義條件。

用於確定事件類型的選項如下：

- **無** — 沒有用於確定事件類型的方法。
- **規則** — 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。
- **條件** — 使用條件來確定事件類型。在選取此選項之後，請按一下 [編輯條件] 以使用 [條件面板] 定義條件。

按一下**下一步**繼續執行精靈。[程序選擇] 頁面隨即出現。

程序選取

使用此頁面，設定當為特定 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：

- **規則** — 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)。

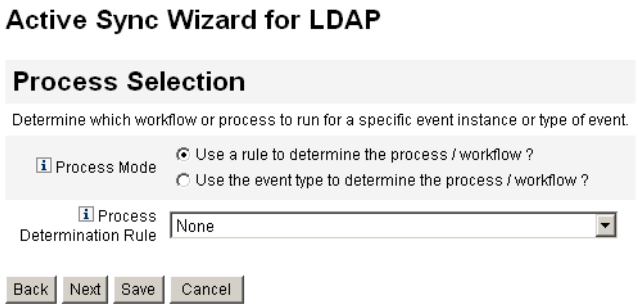


圖 5. Active Sync 精靈：程序選擇 (規則)

- **事件類型** — 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。

  在選取此選項之後，選取要對每個列出的事件類型執行的工作流程或程序。

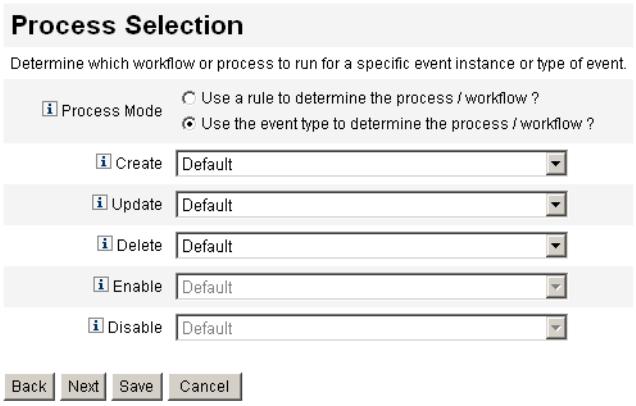


圖 6. Active Sync 精靈：程序選擇 (事件類型)

按一下**下一步**繼續執行精靈。[目標資源] 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。

從 [可用資源] 區域中選取一或多個資源，然後將它們移至 [目標資源] 區域。

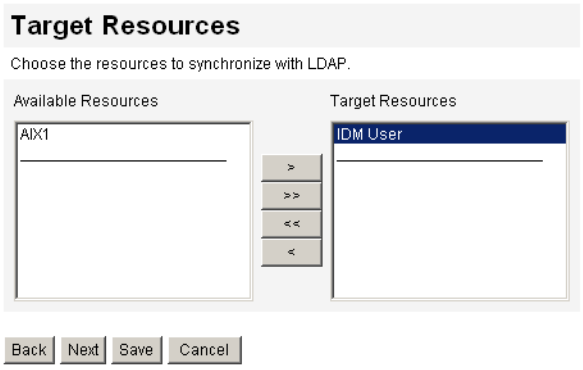


圖 7. Active Sync 精靈：目標資源

按一下**下一步**以繼續。[目標屬性對映] 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。

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**新增對映**。

為每個目標屬性選取屬性、類型及屬性值。在 [套用到] 欄位中，選取一或多個將套用對映的動作 (建立、更新或刪除)。

對每個目標資源重複步驟 1-3。若要從清單中移除屬性，請選取列，再按一下**移除對映**。

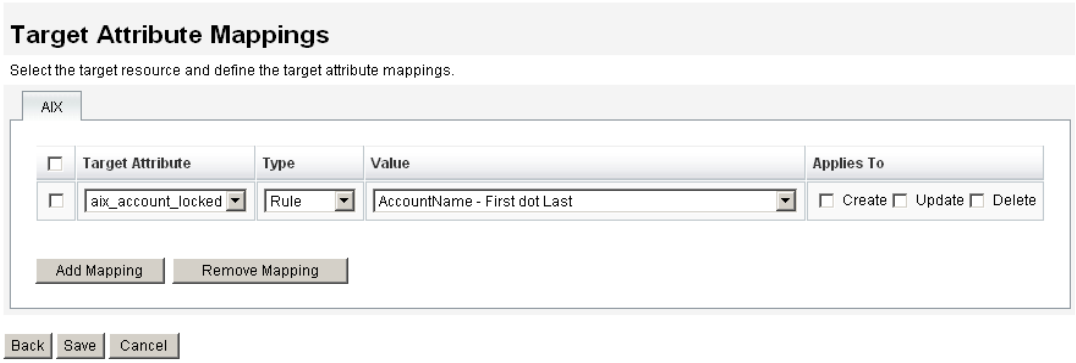


圖 8. Active Sync 精靈：目標屬性對映

按一下**儲存**儲存屬性對映並回到資源清單。

編輯 ActiveSync 配接卡

在編輯 ActiveSync 配接卡之前，您應該停止使用中的同步化。從 [執行設定] 頁面中，選取 [停用] 作為 [啟動類型]。將出現一則警告訊息，指出已停用使用中的同步化。

附註　停用資源的使用中的同步化將導致在儲存資源時停止 Active Sync 作業。

叢集環境中的使用中的同步化

「錯誤」狀態指示器只會呈現在為資源執行使用中的同步化的 Identity Manager 伺服器。

調校 ActiveSync 配接卡效能

由於使用中的同步化是背景作業，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
- 指定會在該處執行配接卡的主機
- 啟動與停止
- 管理配接卡記錄

透過資源清單管理 ActiveSync 配接卡。選取 ActiveSync 配接卡，然後從 [Resource Actions] 清單中存取啟動、停止與狀態更新控制動作。

變更輪詢間隔

- 輪詢間隔決定 ActiveSync 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，如果配接卡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，可將它們設定為每 10 秒執行。

指定會在該處執行配接卡的主機

若要指定將在該處執行配接卡的主機，請編輯 `waveset.properties` 檔案。在這個檔案中，您可以編輯：

- 設定 `sources.hosts=hostname1,hostname2,hostname3`。如此會列出執行 ActiveSync 配接卡的電腦的主機名稱。配接卡將會在此欄位中第一個可用的主機上執行。

  或

- 設定 `sources.hosts=localhost`

設定後者會使配接卡在配置了該配接卡的伺服器上執行。

附註　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。

可以將需要更多記憶體與 CPU 週期的 ActiveSync 配接卡配置為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、手動啟動或自動啟動 ActiveSync 配接卡，就如同它們是 NT 中的服務一樣。同樣須將它們指定為以 Identity Manager 管理員身份執行。此管理員將會詳查 ActiveSync 配接卡能夠執行的存取，並會以執行變更的管理員身份在稽核記錄中列出。選擇性屬性包括記錄檔案大小與路徑、記錄層級。

如果將配接卡設定為自動，當應用程式伺服器重新啟動時，配接卡也會重新啟動。當您啟動配接卡時，它會立刻執行並在指定的輪詢間隔來臨時執行。如果您停止配接卡，下次配接卡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。配接卡記錄在除錯問題與監視配接卡程序進度時非常有用。

每個配接卡各有其記錄檔案、路徑和記錄層級。您可以在 [執行設定] 頁面上指定這些值。

刪除配接卡記錄

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作為歸檔之用。

7 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。

安全性功能

Identity Manager 可藉由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。
- **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「**報告**」，以取得有關報告功能的更多資訊。)
- **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，您登出後，即無法透過瀏覽器的「上一頁」功能存取先前造訪過的頁面。

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 http:///*localhost*:8080/idm/user 為一般使用者提供密碼變更自助功能
  - 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

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**（為每個指定的資源設定認證，並為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 時使用的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了多個已定義登入模組群組，則 Identity Manager 會檢查套用至每個登入模組群組中的**登入限制規則**，以決定要處理哪個群組。

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)。

附註 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。

```
<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，您可以為每個 Identity Manager 登入階段作業設定逾時值 (限制)。選取時、分和秒數後，再按一下 **[儲存]**。您建立的限制會顯示在登入應用程式清單中。

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。為安全起見，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** — 此登入模組為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** — 此登入模組為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 配置為傳遞至 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 搜尋屬性為：

  ```
  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 使用者成為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。

警告 建議您，如果將 Identity Manager 登入配置為可藉由認證登入多個系統，則為 Identity Manager 認證目標的所有系統上，帳號的使用者 ID 和密碼皆須相同。

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 [使用者登入] 表單中所輸入者不符，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 (例如兩個針對相同實體主機定義的資源，或代表 NT 或 AD 網域環境中受信任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為**共用資源**。

將資源設為共用之後，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 皆定義為共用資源 (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。

用來指定這個系統配置物件屬性的格式是：

```
<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 **[Tools]**，然後選取 **[Internet Options]**。
2. 選取 **[Content]** 標籤。
3. 在 [憑證] 區域中，按一下**憑證**。
4. 選取用戶端認證，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

為 X509 憑證認證配置 Identity Manager：

1. 以 [配置者] 的身份 (或具同等權限的身份) 登入 [管理員介面]。
2. 選取 **[Configure]**，然後選取 **[Login]**，以顯示 [Login] 頁面。
3. 按一下**管理登入模組群組**，顯示 [登入模組群組] 頁面。
4. 在清單中選取登入模組群組。
5. 在 [指定登入模組 ...] 清單中，選取 [Identity Manager X509 憑證登入模組]。Identity Manager 會顯示 [修改登入模組] 頁面。
6. 設定登入成功需求。可接受的值如下：
   - **Required** — 此登入模組為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** — 此登入模組為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**儲存**返回 [修改登入模組] 頁面。
9. 或者，重新安排登入模組的順序 (如果登入模組群組中已指定多個登入模組)，再按一下**儲存**。
10. 如果尚未指定，則將登入模組群組指定給登入應用程式。在 [登入模組群組] 頁面上，按一下 [返回登入應用程式]，再選取登入應用程式。將登入模組群組指定給應用程式後，按一下**儲存**。

附註 如果將 `waveset.properties` 檔案中的 `allowLoginWithNoPreexistingUser` 選項設為 true 值，則當配置 [Identity Manager X509 憑證登入模組] 後，會提示您選取 [新的使用者名稱規則]。在使用關聯的 [Login Correlation Rule] 找不到使用者時，可使用此規則確定如何命名新建立的使用者。

[New User Name Rule] 與 [Login Correlation Rule] 具有相同的可用輸入引數。它會傳回單一的字串，此字串會成為用於建立新 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，名為 `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 [Login Correlation Rule] 確定如何將憑證資料對映至適當的 Identity Manager 使用者。Identity Manager 包括一個內建的相互關聯規則，名為 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：

- 它的 `authType` 屬性必須設定為 `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，登入相互關聯規則必須傳回 `AttributeCondition`，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
```

以下為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，傳回一或多個 `AttributeConditions` 清單。[Identity Manager X509 憑證登入模組] 會使用這些清單找到相關的 Identity Manager 使用者。

在 `idm/sample/rules` 中有登入相互關聯規則的範例，名為 `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. 啟用 `SessionFactory` 追蹤，檢視 http 屬性的完整清單，並決定 X509Certificate 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 憑證登入模組中 `<LoginConfigEntry>` 的 `<AuthnProperty>` 名稱變更為正確的名稱。
4. 儲存，然後重試。

您也需要先移除 Identity Manager X509 憑證登入模組，然後重新加入到登入應用程式中。

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。

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「管理伺服器加密」作業進行配置。

伺服器加密金鑰問題與回覆

請閱讀以下各節，以取得有關伺服器加密金鑰來源、位置、維護和使用的常見問題的回覆。

伺服器加密金鑰來自何處？

伺服器加密金鑰是對稱的 triple-DES 168 位元金鑰。伺服器支援兩種類型的金鑰：

- **預設金鑰** — 此金鑰已編譯為伺服器代碼。
- **隨機產生的金鑰** — 此金鑰可以在初始伺服器啟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 提供了名為「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為 「目前」金鑰，則任何要加密的新資料都將使用該伺服器金鑰。

附註 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，則伺服器將無法解密資料。如果從其他儲存庫匯入包含加密資料的物件，則必須先匯入關聯的伺服器加密金鑰，以確保可以成功匯入該物件。

為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 「管理伺服器加密」作業重新加密所有帶有 「目前」伺服器加密金鑰的現有加密資料。

如何保護伺服器金鑰？

如果伺服器未配置為使用基於密碼的加密 (PBE) — PKCS#5 加密 (透過 `pbeEncrypt` 屬性或 「管理伺服器加密」作業在系統配置物件中設定)，則使用預設金鑰加密伺服器金鑰。對於安裝的所有 Identity Manager，預設金鑰都是相同的。

如果伺服器配置為使用 PBE 加密，則每次啟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) 做為 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。

若要啟用伺服器金鑰的 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，如果該伺服器配置為使用 PBE 金鑰，則將解密這些金鑰。然後，如果該伺服器配置為使用 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，初始握手都將產生新的隨機 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，方法是使用做為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

- **預設模式** — 伺服器至閘道的初始協定握手使用編譯為伺服器代碼的預設 168 位元 triple-DES 金鑰加密。
- **安全模式** — 產生針對共用儲存庫的隨機 168 位元金鑰 triple-DES 閘道金鑰，並做為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。啟動時，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 提供了名為「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 [System Configuration] 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。如果伺服器配置為使用 PBE 加密，則將使用 PBE 產生的金鑰加密閘道金鑰。如果該選項為 False，則將使用預設金鑰對其進行加密。請參閱前面標題為「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。請參閱前面標題為「**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 加密將這些金鑰加密。只有具有 「安全管理員」權能的使用者才可以執行 「管理伺服器加密」作業，可以從**作業**標籤存取該作業。

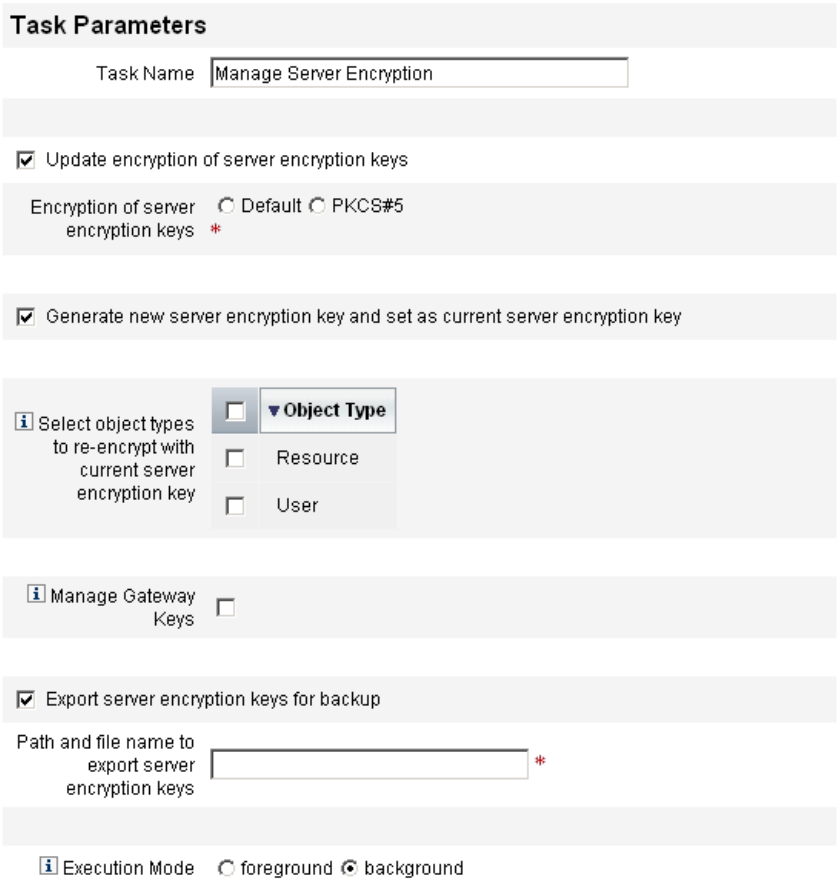


圖 1. 管理伺服器加密作業

選取 **[Run Tasks]**，然後從清單中選取 [Manage Server Encryption]，以為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：
  - **Generate a new key and synchronize all gateways** — 在最初啟用安全閘道環境時，請選取此選項。此選項會產生新的閘道金鑰，並傳送給所有閘道。
  - **Synchronize all gateways with current gateway key** — 選取此選項可同步化任何新的閘道，或是尚未收到新的閘道金鑰的閘道。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為 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。

附註 如果您要使用 PKCS#5 加密，而且選擇產生和設定新的伺服器加密金鑰的話，您也應選取此選項。除此之外，您還應該將匯出的金鑰儲存在可移除的媒體上，並存放在安全的位置 (請勿放在網路上)。

- **執行模式** — 選取是在背景 (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

身為 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為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。
- 開啟稽核以追蹤 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 階段作業逾時設定為預設值 30 分鐘。您可以編輯屬性來變更此值；但您應該將該值設定為一個較低的值以增加安全性。不要將該值設定為高於 30 分鐘。

  若要變更階段作業逾時值：

  1. 編輯 `web.xml` 檔案，該檔案位於應用程式伺服器目錄樹中的 `idm/WEB-INF` 目錄中。
  2. 變更下列行中的數值：

```
<session-config>
  <session-timeout>30</session-timeout>
</session-config>
```

8 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。

閱讀本章節以獲得有關說明如何使用 Identity Manager 報告功能的資訊和程序。您可以瞭解：

- Identity Manager 報告類型，包括稽核記錄報告、即時報告、摘要報告、系統記錄報告和使用情況報告。
- 如何建立、編輯、執行和用電子郵件傳送報告
- 如何下載報告資訊

使用報告

在 Identity Manager 中，將報告視為一類特殊的作業。因此，可以在 Identity Manager 管理員介面的兩個區域中使用報告：

- **Reports** — 在此區域中，您可以定義、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] 區域排程和處理報告工作。

報告

多數與報告相關的活動是在 [執行報告] 頁面中執行，在該頁面中您可以：

- 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 Microsoft Excel) 中使用。

若要檢視此頁面，請從功能表列中選取 **[Reports]**。螢幕上將顯示 **[Run Reports]** 子標籤頁面。

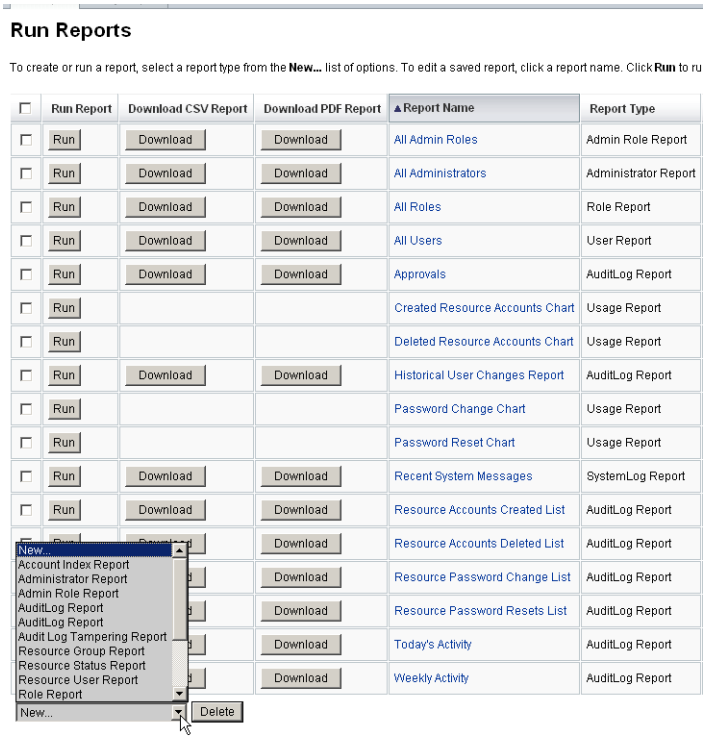


圖 1. 執行報告頁面選擇

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 (也稱為報告複製)

建立報告

若要建立報告：

1. 從功能表列中，選取 **[Reports]**。
2. 從**新增**選項清單中選取報告類型。

Identity Manager 會顯示 [定義報告] 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。輸入新的報告名稱並調整報告參數 (選擇性)，然後按一下**儲存**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** — 以可攜式文件格式 (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 [執行報告] 頁面 (報告清單) 來執行此報告

排程報告

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為以固定間隔執行，而做出不同的選擇：

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

下載報告資料

從 [執行報告] 頁面的下列其中一欄中，按一下 [下載]：

- **Download CSV Report** — 以 CSV 格式下載稽核報告輸出。儲存之後，您即可以在其他應用程式 (如 Microsoft Excel) 中開啟與使用報告。
- **Download PDF Report** — 以可攜式文件格式下載稽核報告輸出。

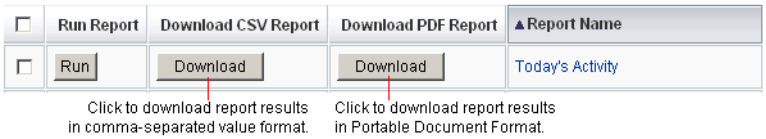


圖 2. 下載報告

配置報告輸出的字型

對於以可攜式文件格式 (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取，請按一下 **[Configure]**，然後選取 **[Reports]**。可使用以下選取：

- **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 / 目錄中並重新啟動伺服器，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。如果選取這些字型中的一種，則檢視報告的機器上必須能夠使用這種字型。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。

附註　內嵌字型會極大地增加文件的大小。

按一下 **[Save]** 以儲存報告配置選項。

報告類型

Identity Manager 有數種報告類型，其中包括：

- 稽核記錄
- 即時
- 摘要
- 系統記錄
- 使用情況

稽核記錄

稽核報告會以系統稽核記錄中擷取的事件為基礎。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、密碼變更與重設及自我佈建的活動。

附註 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。若要執行此動作，請從功能表列中選取 **[Configure]**，然後選取 **[Audit Events]**。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。如需更多關於設定稽核配置群組的資訊，請參閱第 5 章中的**稽核群組配置**。

若要定義稽核記錄報告，請從 [Run Reports] 頁面的報告選項清單中選取 [AuditLog Report]。

您設定與儲存報告參數後，請即從 [執行報告] 清單頁面中執行報告。按一下**執行**以產生一個包含與儲存的條件相符的所有結果的報告。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，包括使用者成員資格。
- **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] 頁面的報告選項清單中選取該選項。

您設定與儲存報告參數後，請即從 [執行報告] 清單頁面中執行報告。按一下**執行**以產生一個包含與儲存的條件相符的所有結果的報告。

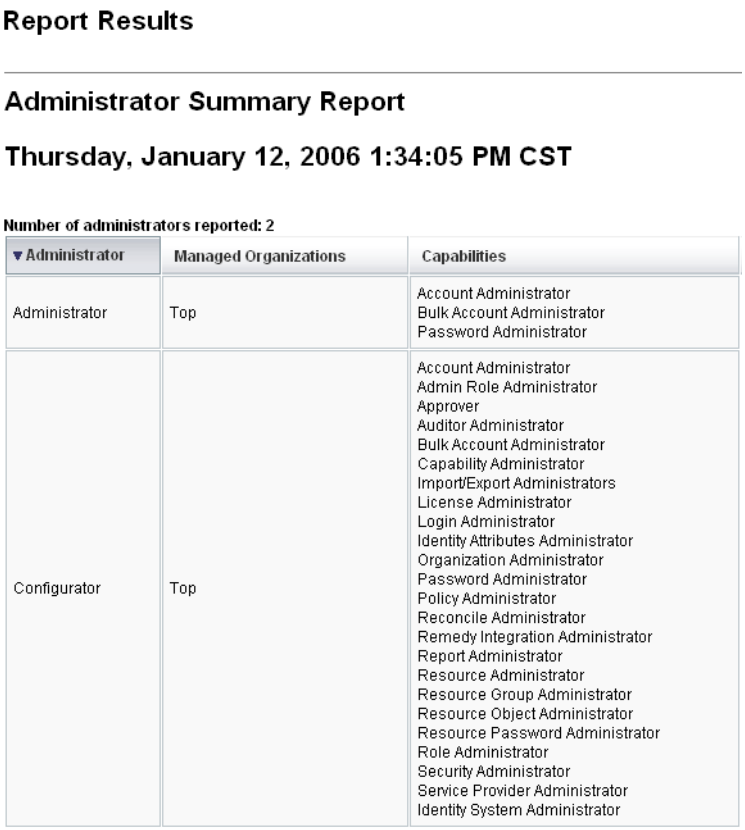
摘要報告

摘要報告類型包括：

- **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** — 報告處於擱置的工作和已完成的工作。您可以藉由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、開始日期與狀態。
- **User** — 檢視使用者、為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、角色、組織或指定資源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。

在 [執行報告] 清單頁面執行摘要報告。

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。



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

圖 3. 管理員摘要報告

系統記錄

系統記錄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 (預設為 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。

附註 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 *lh* **參照**中的 *syslog* **指令**。

若要定義系統記錄報告，請從 [Run Report] 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] 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 [執行報告] 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。

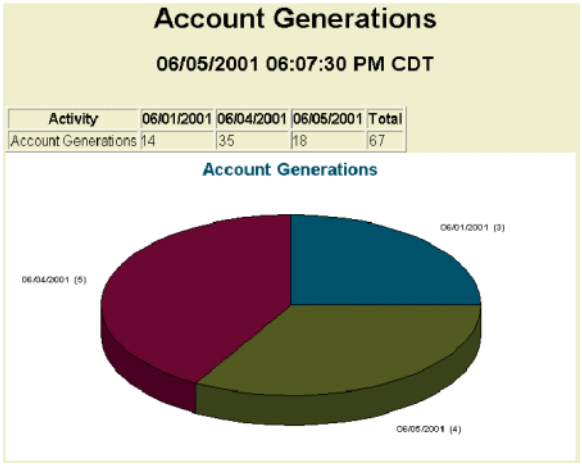


圖 4. 使用情況報告 (產生的使用者帳號)

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。為了獲得最佳的控制，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。

附註 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 「業務程序編輯器」修改這些表單。如需有關配置 Identity Manager 表單的更多資訊，請參閱 Identity Manager Technical Reference。

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

您可以將報告限制為只掃描選取的資源；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為以指定間隔執行。

1. 按一下**排程作業**，然後選取要執行的報告。
2. 在 [建立作業排程] 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**儲存**以儲存排程。

9 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，做為編寫自訂工作流程的替代方法。

Identity Manager 提供了以下作業範本，您可對其進行配置：

- **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。

請閱讀以下章節，以取得有關使用作業範本的資訊：

- 啟用作業範本 — 說明如何在您的系統中啟用作業範本。
- 配置作業範本 — 說明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

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：

1. 從 [Identity Manager Administrator] 介面中，選取 **[Tasks]**，然後選取 **[Configure Tasks]**。

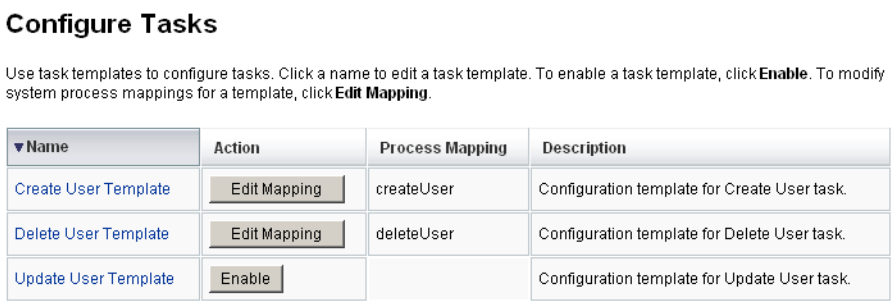


圖 1. 配置作業

[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** — 如果您尚未啟用範本，則顯示此按鈕。
  - **Edit Mapping** — 啟用範本之後會顯示此按鈕。

  啟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]** 以開啟範本的 [Edit Process Mappings] 頁面。

   例如，對於 [Create User Template]，會顯示以下頁面：

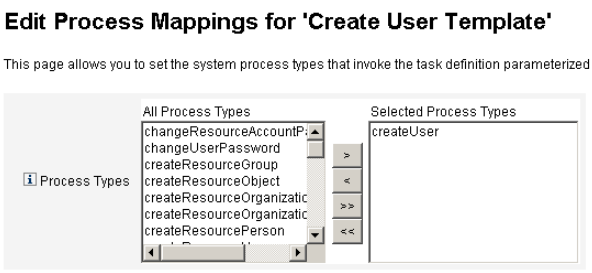


圖 2. [Edit Process Mappings] 頁面

附註 預設程序類型 (在此情況下，為 `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，請勿為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。

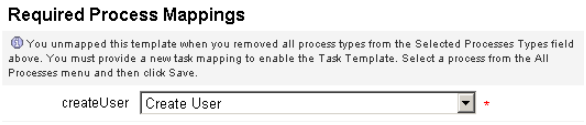


圖 3. [Required Process Mappings] 區段

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

附註 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。

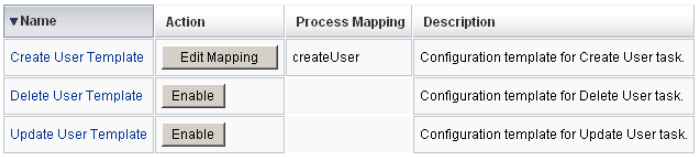


圖 4. 更新的配置作業表

4. 為剩餘的每個範本重複該對映程序。

備註：

- 您可以透過選取 **[Configure]** > **[Form and Process Mappings]** 來驗證對映。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。

程序類型	將程序名稱對映到
createUser	Create User Template
deleteUser	Delete User Template
updateUser	Update User Template

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

- 如果您將 **`Template`** 輸入 [Process Name Mapped To] 欄 (如表中所示)，則還可以直接從此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** — 開啟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** — 開啟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** — 開啟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。

   下表說明每個標籤、其用途以及哪些範本使用該標籤。

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
稽核	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 5 頁的「配置 [General] 標籤」
   - 第 8 頁的「配置 [Notification] 標籤」
   - 第 13 頁的「配置 [Approvals] 標籤」
   - 第 28 頁的「配置 [Provisioning] 標籤」
   - 第 29 頁的「配置 [Sunrise and Sunset] 標籤」
   - 第 34 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。

附註 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]

開啟 [Edit Task Template Create User Template] 或 [Edit Task Template Update User Template] 後，依預設會顯示 [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。

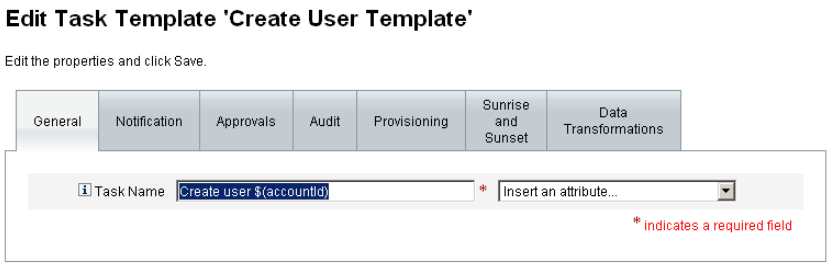


圖 5. [General] 標籤：Create User Template

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]** 功能表會提供目前為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]

開啟 [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** — 啟用此按鈕可以防止帳號被刪除。
   - **Only if user has no linked accounts after deprovisioning** — 啟用此按鈕，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** — 啟用此按鈕，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的取消佈建作業，如下所示：
   - **Delete All** — 啟用此方塊，可以刪除所有指定資源中代表該使用者的全部帳號。
   - **Unassign All** — 啟用此方塊，可以取消指定給該使用者所有資源帳號。無法刪除資源帳號。
   - **Unlink All** — 啟用此方塊，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。

附註 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)，如下所示：
   - **Delete** — 啟用此方塊，可以刪除資源中代表該使用者的帳號。
   - **Unassign** — 啟用此方塊，該使用者將不再直接指定到資源。無法刪除資源帳號。
   - **Unlink** — 啟用此方塊，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。

附註 如果您需要為不同的資源單獨指定取消佈建策略，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，因為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，因為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。

附註 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為「瞭解電子郵箱範本」的小節。

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

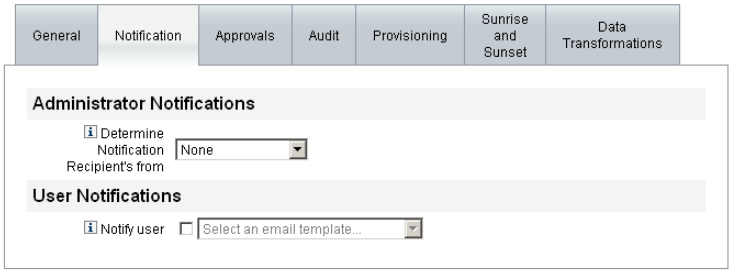


圖 6. [Notification] 標籤 Create User Template

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** 9-9 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** 9-10 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** 9-11 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** 9-12 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：

附註　此屬性必須解析為可表示單一帳號 ID 的字串或解析為帳號 ID 的清單。

1. 從 **[Determine Notification Recipients from]** 功能表中選取 **[Attribute]**，將會顯示以下新選項：

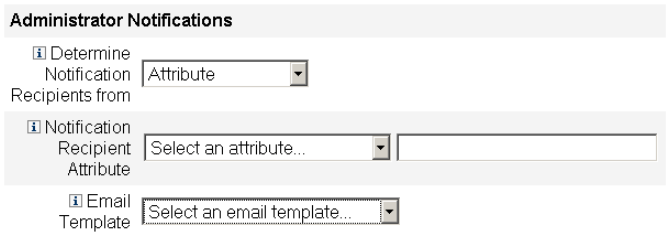


圖 7. 管理員通知：屬性

   - **Notification Recipient Attribute** — 提供用於確定收件者帳號 ID 的屬性清單 (目前為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：

附註 評估之後，此規則必須傳回代表單一帳號 ID 的字串或其元素為帳號 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：

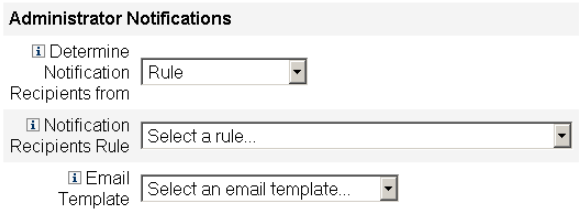


圖 8. 管理員通知：規則

   - **Notification Recipient Rule** — 提供目前為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，以指定通知電子郵件的格式。

透過查詢指定收件者

附註　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：

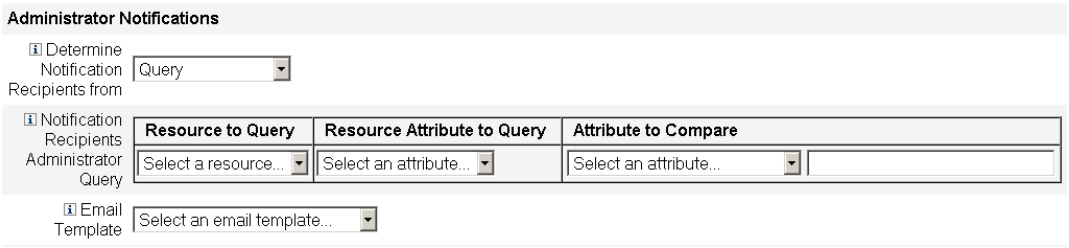


圖 9. 管理員通知：查詢

   - **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** — 提供目前為系統定義的資源清單。
     - **Resource Attribute to Query** — 提供目前為系統定義的資源屬性清單。
     - **Attribute to Compare** — 提供目前為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：

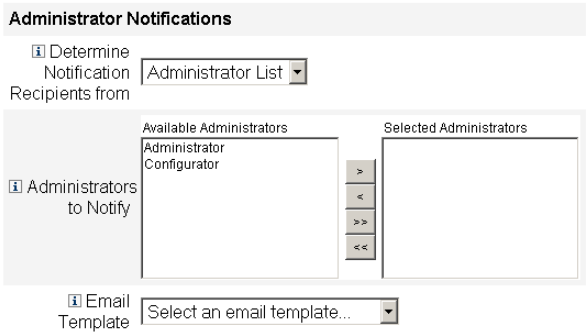


圖 10. 管理員通知：管理員清單

- **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、被更新或被刪除，請啟用 **[Notify user]** 核取方塊，然後從該功能表中選取電子郵件範本。

圖 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。

附註 如果您為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 [Approval] 頁面管理使用者介面

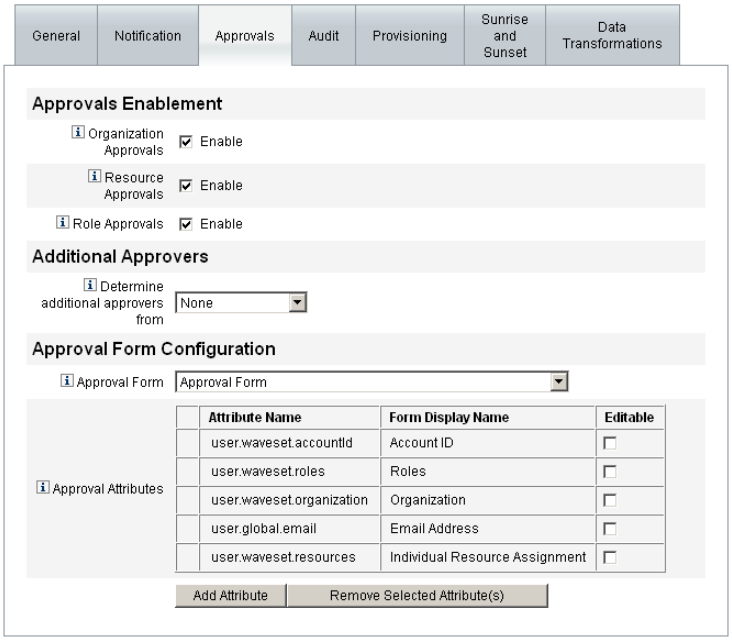


圖 12. [Approvals] 標籤 Create User Template

若要配置核准，請使用以下步驟：

1. 完成 [Approvals Enablement] 區段 (請參閱第 14 頁的「啟用核准」)。
2. 完成 [Additional Approvers] 區段 (請參閱第 15 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 23 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。

附註 依預設，這些核取方塊對於 [Create User Template] 和 [Update User Template] 已啟用，但對於 [Delete User Template] 已**停用**。

- **Organization Approvals** — 啟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** — 啟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** — 啟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 將如何為建立使用者、刪除使用者或更新使用者作業確定附加核准人。此功能表上的選項包括：

選項	說明
None (預設)	執行作業不需要附加核准人。
屬性	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。
規則	透過評估指定的規則，導出收件者的帳號 ID。
查詢	透過查詢特定資源，導出收件者的帳號 ID。
管理員清單	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 15 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 16 頁)
- 透過規則 (第 17 頁)
- 透過查詢 (第 18 頁)
- 透過管理員清單 (第 19 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]**。

附註 此屬性必須解析為可表示單一帳號 ID 的字串或解析為帳號 ID 的清單。

將顯示以下新選項：

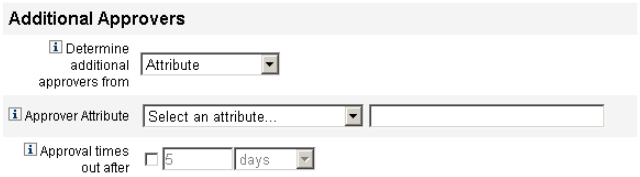


圖 13. 附加核准人：屬性

- **Approver Attribute** — 提供用於確定核准人帳號 ID 的屬性清單（目前為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。

附註 **Approval times out after** 設定將影響初始核准和提升核准。

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 20 頁的**配置核准逾時**，以取得說明。
   - 如果您不想指定逾時時間段，則可以繼續執行第 23 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]**。

附註 評估之後，此規則必須傳回代表單一帳號 ID 的字串或其元素為帳號 ID 的清單。

將顯示以下新選項。

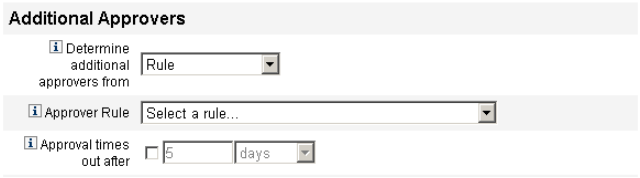


圖 14. 附加核准人：規則

- **Approver Rule** — 提供目前為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。

附註 **Approval times out after** 設定將影響初始核准和提升核准。

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** 9-20 頁的「**配置核准逾時**」，以取得說明。
   - 如果您不想指定逾時時間段，則可以繼續執行第 23 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

附註 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：

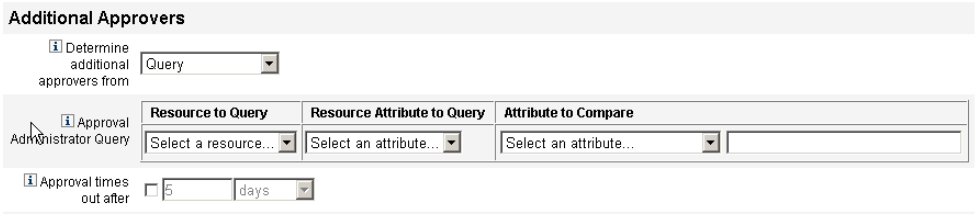


圖 15. 附加核准人：查詢

- **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** — 提供目前為系統定義的資源清單。
  - **Resource Attribute to Query** — 提供目前為系統定義的資源屬性清單。
  - **Attribute to Compare** — 提供目前為系統定義的屬性清單。
- **Approval times out after** — 提供指定核准逾時的方法。

附註 **Approval times out after** 設定將影響初始核准和提升核准。

2. 如下所示，建構一個查詢：
   a. 從 **[要查詢的資源]** 功能表中選取資源。
   b. 從 **[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** 9-20 頁的「**配置核准逾時**」，以取得說明。
   - 如果您不想指定逾時時間段，則可以繼續執行第 23 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：

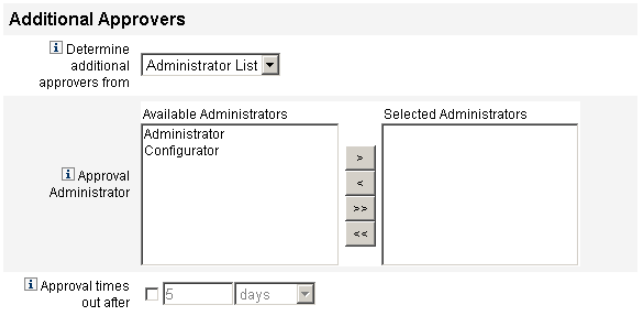


圖 16. 附加核准人：管理員清單

- **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。

附註 **Approval times out after** 設定將影響初始核准和提升核准。

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** 9-20 頁的「**配置核准逾時**」，以取得說明。
   - 如果您不想指定逾時時間段，則可以繼續執行第 23 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. 啟用該核取方塊。

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

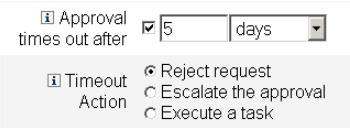


圖 17. [Approval Timeout] 選項

2. 使用 **[Approval times out after]** 文字欄位和功能表可以指定逾時時間期間，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，表示您要為逾時指定多少秒、分鐘、小時或天。

附註 **Approval times out after** 設定將影響初始核准和提升核准。

3. 啟用以下 **[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。

     啟用此按鈕後，將顯示新的選項，因為您必須指定 Identity Manager 將如何為提升核准確定核准人。繼續閱讀**第** 9-21 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。

     啟用此按鈕，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** 9-23 頁的「**執行作業**」，以取得說明。

提升核准

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

圖 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為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。

附註 此屬性必須解析為可表示單一帳號 ID 的字串或解析為帳號 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。

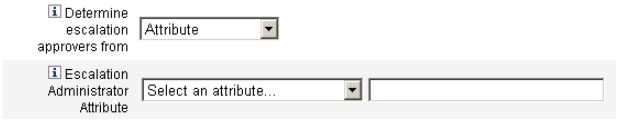


圖 19. [Escalation Administrator Attribute] 功能表

- **Rule** — 透過評估指定的規則，確定核准人帳號 ID。

附註 評估之後，此規則必須傳回代表單一帳號 ID 的字串或其元素為帳號 ID 的清單。

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

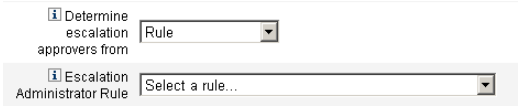


圖 20. [Escalation Administrator Rule] 功能表

- **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 **[要查詢的資源]** 功能表中選取資源。

b. 從 **[要查詢的資源屬性]** 功能表中選取屬性。

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

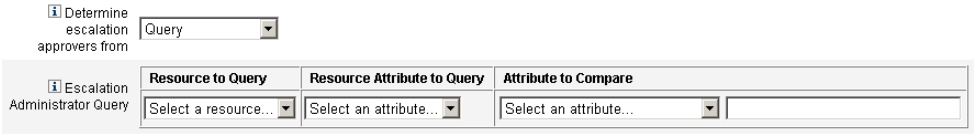


圖 21. [Escalation Administrator Query] 功能表

- **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：

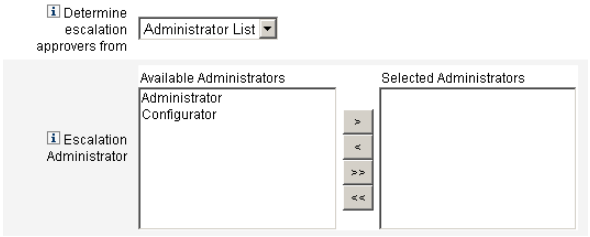


圖 22. [Escalation Administrator] 選取工具

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

啟用 [Timeout Action] **[Execute a task]** 按鈕後，**[Approval Timeout Task]** 功能表將如下顯示：

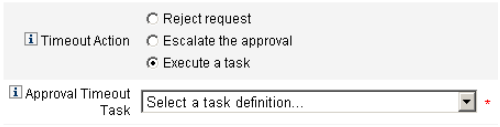


圖 23. [Approval Timeout Task] 功能表

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

附註 [Delete User Template] 不包含 [Approval Form Configuration] 區段。您僅可以為 [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）。

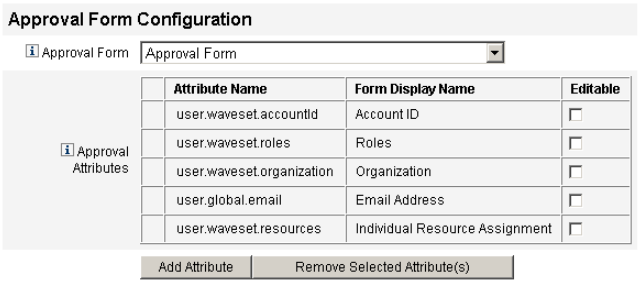


圖 24. 核准表單配置

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`

附註 預設核准表單配置為可以顯示核准屬性。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。

若要為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. 啟用 **[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，如果您啟用 `[user.waveset.accountId]` 核取方塊，則核准者可以變更使用者的帳號 ID。

附註 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` 屬性做為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，以指定要在核准表單中顯示的新使用者帳號資料的屬性。
   - 若要將屬性增加到表單，請參閱第 25 頁的「增加屬性」。
   - 若要從表單移除屬性，請參閱第 25 頁的「移除屬性」。

附註 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]** 功能表將變為可使用狀態，如下圖中所示：

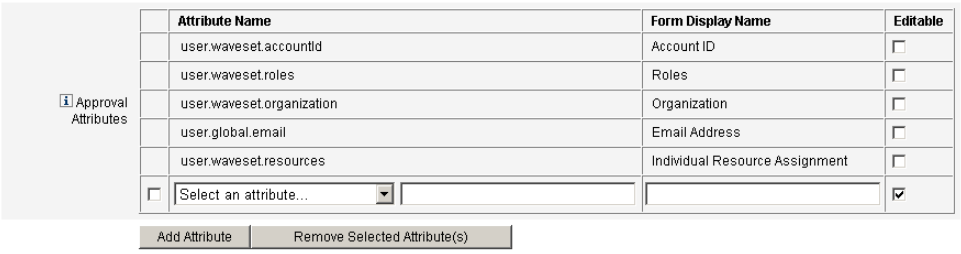


圖 25. 增加核准屬性

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，請啟用 **[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

附註　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. 啟用 [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。

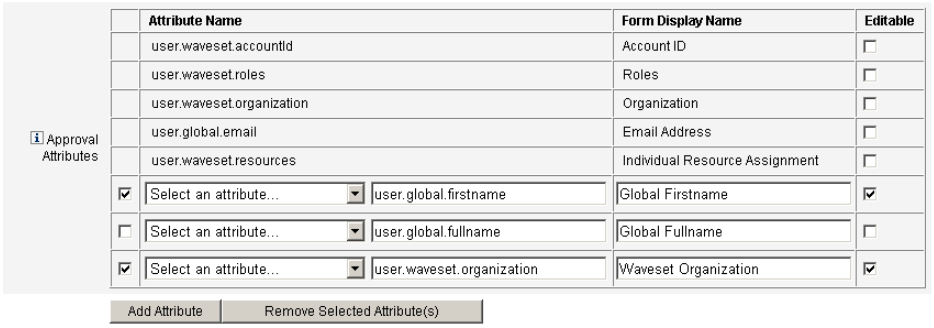


圖 26. 移除核准屬性

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。

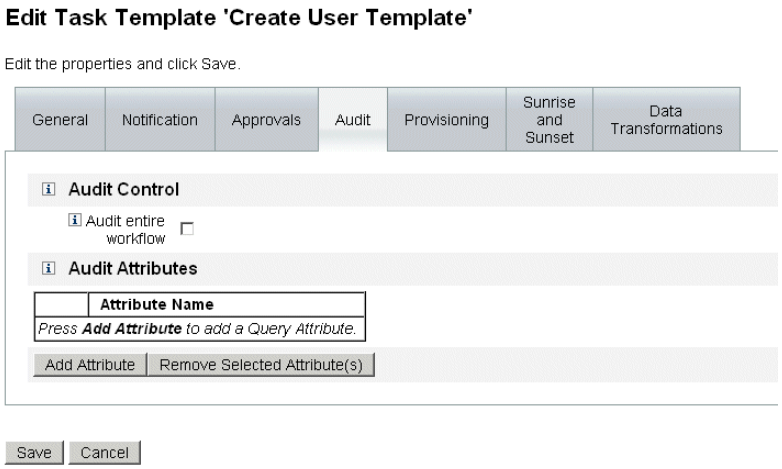


圖 27. 稽核建立使用者範本

若要從使用者範本的 [Audit] 標籤配置稽核，請：

1. 啟用 **[Audit entire workflow]** 核取方塊以啟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 28. 增加屬性

若要移除 [稽核屬性] 表格中的屬性：

1. 啟用您想移除之屬性旁的核取方塊。

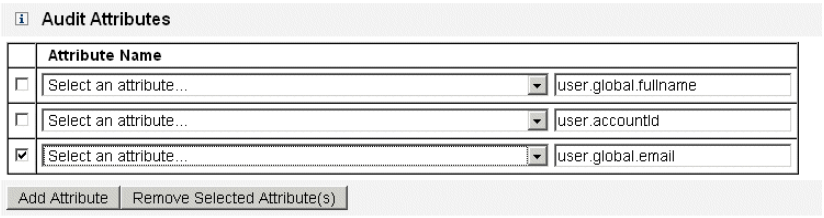


圖 29. 移除 user.global.email 屬性

2. 按一下 **[移除選取的屬性]** 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

附註 此標籤僅適用於 [Create User Template] 和 [Update User Template]。

您可以使用 [Provisioning] 標籤來配置與佈建相關的以下選項：

圖 30. [Provisioning] 標籤：Create User Template

- **Provision in the background** — 啟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** — 啟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

附註　此標籤僅對 [Create User Template] 可用。

您可以使用 [Sunrise and Sunset] 標籤，來選取確定以下時間和日期的方法

- 為新使用者進行佈建（**生效**）。
- 為新使用者取消佈建（**失效**）。
  例如，您可以為六個月後合同到期的臨時工指定失效日期。

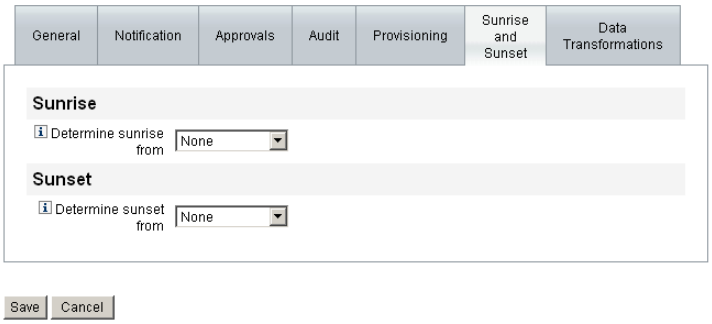


圖 31. [Sunrise and Sunset] 標籤：Create User Template

本節的剩餘部分提供了配置 [Sunrise and Sunset] 標籤的說明。資訊組織如下：

- 第 30 頁的「配置生效」
- 第 33 頁的「配置失效」

配置生效

本節提供確定對於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的說明。

若要配置生效，請：

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 31 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 31 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 32 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 32 頁，以取得說明。

附註 **[Determine sunrise from]** 功能表預設為 **[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。

附註 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時間，

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 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日曆時間，

1. 從 **[Determine sunrise from]** 功能表選取 **[Specified day]**。

   下列新功能表將顯示在 **[Determine sunrise from]** 功能表的右側。

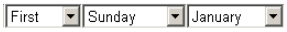


圖 33. 新功能表

2. 使用這些新功能表來指定在哪個月、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 34. 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，

1. 從 **[Determine sunrise from]** 功能表中選取 **[Attribute]** ，以下選項將變為可使用狀態：
   - **[Sunrise Attribute]** 功能表 — 提供目前為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)。

附註 若您未啟用 **[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，啟用 **[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：

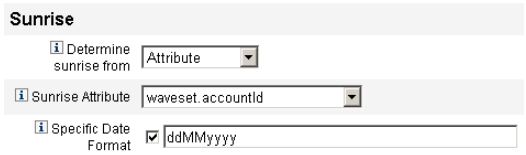


圖 35. 透過屬性佈建新使用者。

指定規則

若要透過評估指定規則來確定佈建日期和時間，

1. 從 **[Determine sunrise from]** 功能表中選取 **[Rule]** ，以下選項將變為可使用狀態：
   - **[Sunrise Rule]** 功能表 — 提供目前為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)。

附註 若您未啟用 **[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，啟用 **[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：

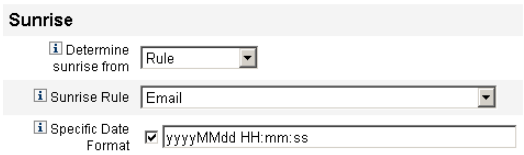


圖 36. 透過規則佈建新使用者。

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，因為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，

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：

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

   - **Specified time** — 將取消佈建延遲到未來的指定時間。請參閱第 31 頁的 「指定時間」，以取得說明。
   - **Specified date** — 將取消佈建延遲到未來的指定日曆日期。請參閱第 31 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 32 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 32 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

附註 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，如果您要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：

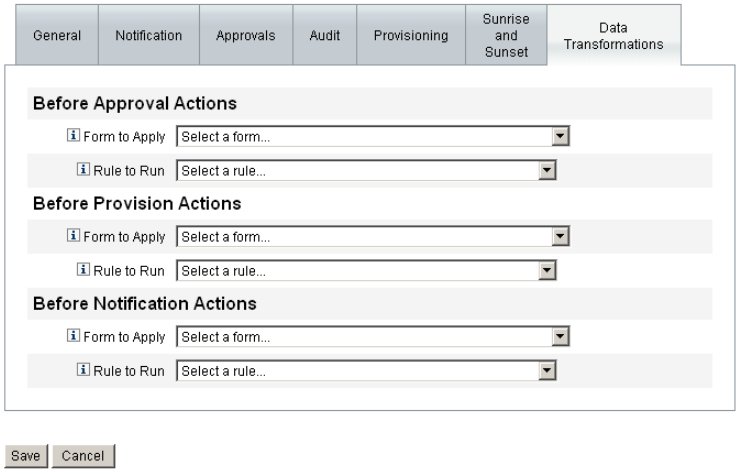


圖 37. [Data Transformations] 標籤：Create User Template

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 — 提供目前為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 — 提供目前為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。

10 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。

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 同步的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，該控制器將與做為 Java Messaging Service (JMS) 用戶端代理伺服器的 Servlet 進行通訊。而該 Servlet 與啟用 JMS 的訊息佇列進行通訊。JMS 偵聽程式資源配接卡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。

附註 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 PasswordSync 之前

只能在 Windows 2000、Windows 2003 和 Windows NT 網域控制器上設定 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。請參閱「Identity Manager 資源參照」中針對 JMS 偵聽程式資源配接卡的文件，以取得有關 JMS 系統需求的資訊。

此外，PasswordSync 還有以下需求

- 必須在每個網域控制器上安裝 Microsoft .NET 1.1 或更高版本
- 必須移除所有舊版 PasswordSync

以下各節將詳細討論這些需求。

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) 版本太低。
- 在 **[關鍵字]** 搜尋欄位中輸入 **`NET Framework 1.1 Redistributable`** 以快速查找架構工具組。
- 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 [Add/Remove Programs] 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。

Installing PasswordSync

以下程序說明了如何安裝 PasswordSync，並提供了安裝、配置和解除安裝 PasswordSync 配置應用程式的說明。

附註 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 [Welcome] 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 [Welcome] 螢幕上顯示的資訊，然後按一下 [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]** 以控制要安裝的套裝軟體部分。
4. 按一下 **[Install]** 以安裝產品。成功安裝 PasswordSync 後，螢幕上將顯示以下視窗。
5. 按一下 **[Finish]** 以完成安裝程序。確定已選取 **[Launch Configuration Application]**，以便可以開始配置 Password Sync。請參閱「配置 PasswordSync」，以取得有關該程序的詳細資訊。

附註 螢幕上將顯示對話方塊，表明您必須重新啟動系統才能使變更生效。完成配置 PasswordSync 之前不必重新啟動系統，但必須在實作 PasswordSync 之前重新啟動網域控制器。

下表可識別安裝在每個網域控制器上的檔案。

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

安裝的元件	說明
%$INSTALL_DIR$%\passwordsyncmsgs.dll	處理 PasswordSync 訊息的 DLL。
%SYSTEMROOT%\SYSTEM32\lhpwic.dll	密碼通知 DLL。此 DLL 可實作 Windows PasswordChangeNotify () 函數。

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為精靈。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。

使用以下步驟配置 PasswordSync。

1. 如果尚未執行 PasswordSync 配置應用程式，請將其啟動。依預設，此配置應用程式安裝在 [Program Files] —> [Sun Java System Identity Manager PasswordSync] —> [Configuration] 中。

   螢幕上將顯示以下對話方塊。

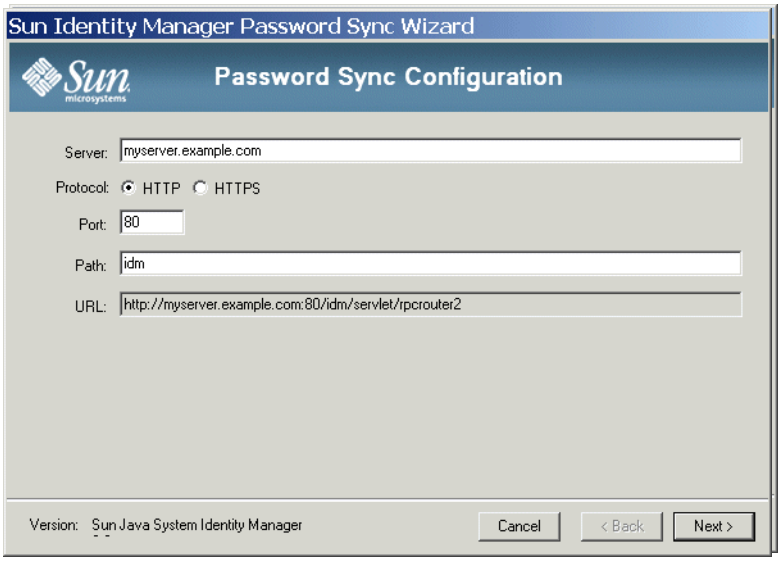


圖 1. 伺服器配置對話方塊

依需要編輯以下欄位。

- **[Server]** 必須用安裝 Identity Manager 應用程式伺服器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，則預設連接埠為 80。如果選取 HTTPS，則預設連接埠為 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. 按一下 **[Next]** 以顯示代理伺服器配置頁面。

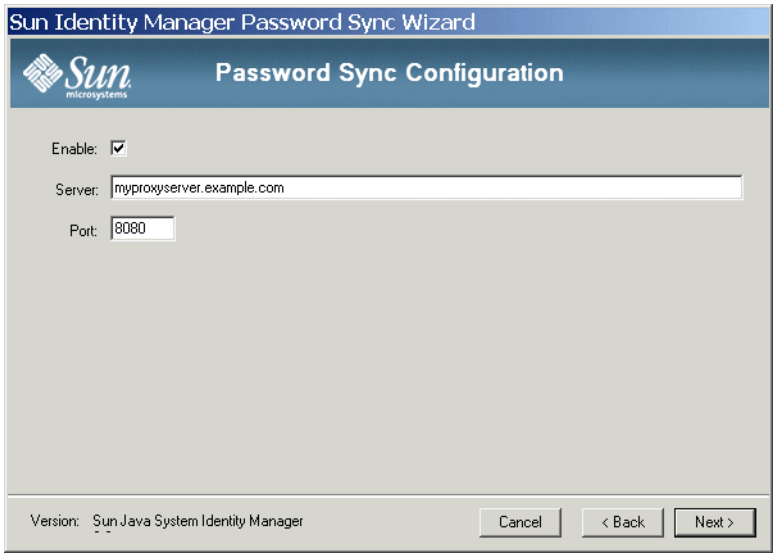


圖 2. 代理伺服器對話方塊

依需要編輯以下欄位。

- 如果需要代理伺服器，則按一下 **[Enable]**。
- **Server** 必須用代理伺服器的完全合格的主機名稱或 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為 8080，預設 HTTPS 連接埠為 443。)

3. 按一下 **[Next]** 以顯示 JMS 設定對話方塊。

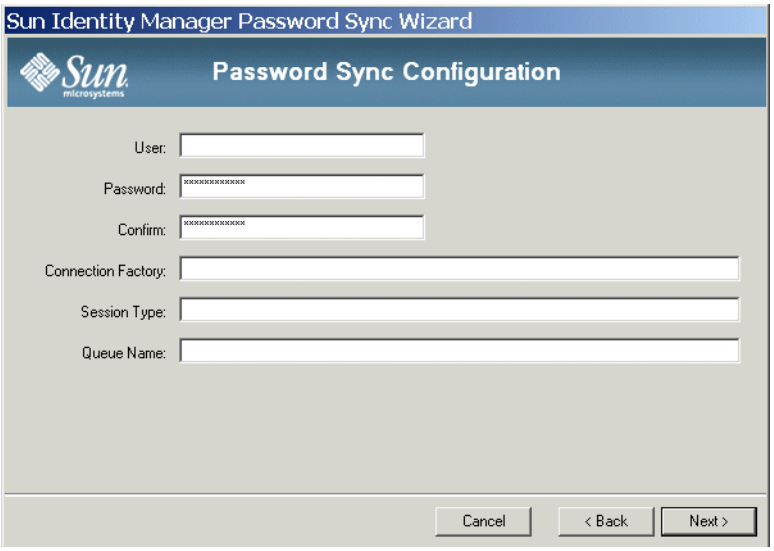


圖 3. JMS 設定對話方塊

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]** 指定應使用的 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]** 設定為 [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。

4. 按一下 **[Next]** 以顯示 JMS 特性對話方塊。

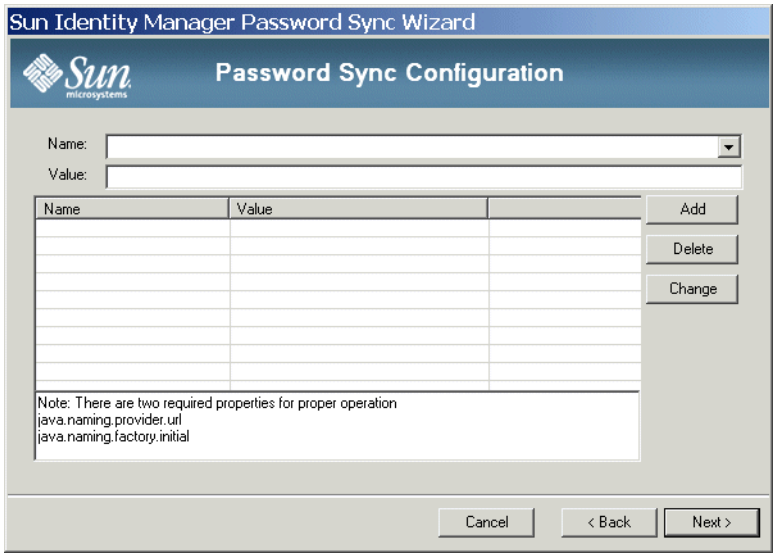


圖 4. JMS 特性對話方塊

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` — 必須將該值設定為執行 JNDI 服務之電腦的 URI。
- `java.naming.factory.initial` — 必須將該值設定為 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. 按一下 **[Next]** 以顯示電子郵件對話方塊。

透過電子郵件對話方塊，您可以配置在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。

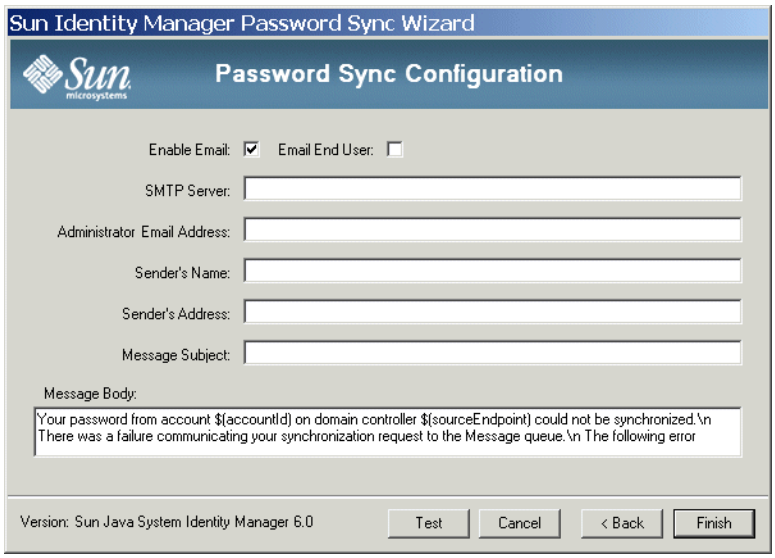


圖 5. 電子郵件對話方塊

依需要編輯以下欄位。

- 選取 **[Enable Email]** 以啟用該功能。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的 SMTP 伺服器的完全合格的名稱或 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位址。
- **[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。如果您要將應用程式顯示為精靈，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啟用追蹤的詳細資訊。還列出了對 PasswordSync 執行除錯或啟用配置工具無法實作的功能可能需要的登錄機碼。

錯誤記錄

PasswordSync 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，以後每次啟動該配置工具時都會顯示 **[Trace]** 標籤。

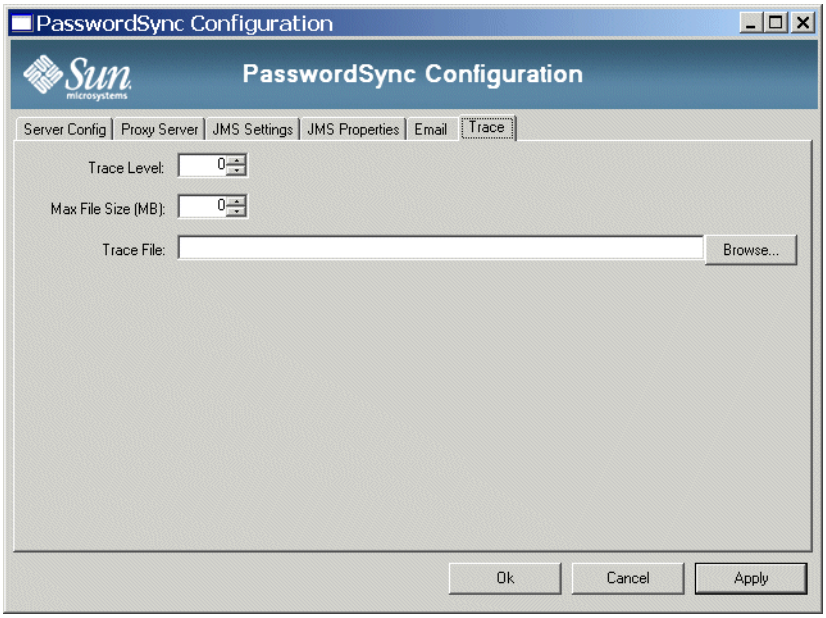


圖 6. 追蹤對話方塊

[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為 C:\logs\pwicsvc.log，並將追蹤層級設定為 100 MB，則當追蹤檔案超過 100 MB 時，PasswordSync 會將該檔案重新命名為 C:\logs\pwicsvc.log.bk，並將新資料寫入新的 C:\logs\pwicsvc.log 檔案中。

登錄機碼

可以使用 Windows 登錄編輯器編輯下表中列出的登錄機碼。這些機碼位於 HKEY_LOCAL_MACHINE\SOFTWARE\Waveset\Lighthouse\PasswordSync 的機碼中。此位置也會顯示其他機碼，但這些機碼可使用配置工具進行編輯。

機碼名稱	類型	說明
allowInvalidCerts	REG_DWORD	如果設定為 1，則在 .NET 用戶端上設定以下標幟： • 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 [Control Panel] 並選取 **[新增 / 移除程式]**。然後選取 [Sun Java System Identity Manager PasswordSync] 並按一下 **[Remove]**。

附註 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。

必須重新啟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 偵聽程式配接卡
- 實作同步化使用者密碼工作流程
- 設定通知

配置 JMS 偵聽程式配接卡

網域控制器間接將訊息置入佇列中後，必須將資源配接卡配置為接受這些訊息。您必須建立 JMS 偵聽程式資源配接卡並對其進行配置以與佇列通訊。請參閱「Identity Manager 資源參照」，以取得有關設定該配接卡的更多資訊。

必須配置以下資源參數：

Destination Type — 通常將該值設定為 [Queue]。因為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` — 必須將該值設定為執行 JNDI 服務之電腦的 URI。
- `java.naming.factory.initial` — 必須將該值設定為 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。

Reliable Messaging Support — 選取 [LOCAL] (本機作業事件)。其他選項不適用於密碼同步化。

Message Mapping — 輸入 `java:com.waveset.adapter.jms.PasswordSyncMessageMapper`。該類別可將來自 JMS 伺服器的郵件變換為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並簽出，然後返回 ChangeUserPassword 檢視器。完成簽入後，工作流程將反覆運算所有資源帳號並選取除資源來源以外的所有資源。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，請將其指定為 JMS 偵聽程式配接卡實例的程序規則。可以在配接卡的 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可能修改包括：

- 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「Identity Manager 工作流程、表單與視圖」。

設定通知

Identity Manager 提供了密碼同步化通知和密碼同步化故障通知電子郵件範本。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，為其提供有關下一步操作的公司特定資訊。請參閱名為「**配置**」一章中的「**瞭解電子郵件範本**」，以取得更多資訊。

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，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。

附註　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 檔案以外，PasswordSync Servlet 還需要 `spml.jar` 和 `idmcommon.jar` JAR 檔案。

PasswordSync 服務是否將密碼以明文傳送至 Ih 伺服器？

雖然我們建議透過 SSL 執行 PasswordSync，但是在將敏感資料傳送至 Identity Manager 伺服器之前，所有資料都是加密的。

密碼變更有時是否會導致 com.waveset.exception.ItemNotLocked？

如果啟用 PasswordSync，密碼變更 (即使從使用者介面啟動) 將導致資源的密碼變更，從而導致資源與 Identity Manager 接觸。

如果正確配置 thepasswordSyncThreshold 工作流程變數，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。

A lh 參照

用法

```
lh { $class | $command } [ $arg [$arg... ] ]
```

備註

- 若要顯示指令用法說明，請鍵入 `lh` (不使用任何引數)。
- 使用 `lh` 指令時，您應該將 `JAVA_HOME` 設定為包含內有 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` 設定為 `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` 設定為內嵌的 `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` 設定為 `D:\java\jdk1.3.1_02.jre`。

類別

必須是完全合格的類別名稱，如 `com.waveset.session.WavesetConsole`。

指令

必須為下列其中一個指令：

- `config` — 啟動業務程序編輯器。
- `console` — 啟動 Identity Manager 主控台。
- `js` — 呼叫 JavaScript 程式。
- `license [ 選項 ] {status | set { 參數 }}` — 設定 Identity Manager 授權金鑰。
- `setRepo` — 設定 Identity Manager 索引儲存庫。
- `setup` — 啟動 Identity Manager 設定程序，可讓您設定授權金鑰、定義 Identity Manager 索引儲存庫和匯入配置檔案。
- `syslog [ 選項 ]` — 從系統記錄中擷取記錄。
- `xpress [ 選項 ] *Filename*` — 計算表示式。有效選項為 `-trace` (啟用追蹤輸出)。

範例

- `lh com.waveset.session.WavesetConsole`
- `lh console`
- `lh console ñu$user ñp$password`
- `lh setup -U`*Administrator* `-P`*Password*
- `lh setRepo -c -A`*Administrator* `-C`*Password*
- `lh setRepo -t`*LocalFiles* `-f$WSHOME`

license 指令

用法

```
license [options] { status | set {parameters} }
```

選項

`-U` *username* (如果重新命名了 Configurator 帳號)

`-P` *password* (如果變更了 Configurator 密碼)

`set` 選項的參數必須為 `-f` *File* 形式。

範例

- `lh license status`
- `lh license set -f` *File*

syslog 指令

用法

```
syslog [ 選項 ]
```

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)

B 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。

附註　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。

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>。

附註 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為「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。

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。

運算子	說明	範例
<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。

索引

符號

英文

三畫

四畫

五畫

六畫

七畫

八畫

九畫

十二畫

十三畫

十四畫