Identity Console
管理指南

2022 年 9 月

法律聲明

關於本書和文件庫

*《管理指南》*提供關於 NetIQ Identity Console (Identity Console) 產品的概念性資訊。此指南定義了術語，並介紹了多個實作案例。

如需最新版的 *《NetIQ Identity Console 管理指南》*，請參閱 NetIQ Identity Console 線上文件網站的英文版文件。

適用對象

本指南適用於網路管理員。

文件庫其他資訊

文件庫提供下列資訊資源：

安裝指南

描述如何安裝 Identity Console。本書適用於網路管理員。

關於 NetIQ Corporation

我們是一家全球性企業軟體公司，著重於處理您環境中三個不斷出現的挑戰：變動、複雜性和風險，以及我們可以如何協助您進行控制。

我們的觀點

因應變動及管理複雜性和風險已不是新資訊

事實上，在您所面對的挑戰中，這些或許是最明顯的變數，可控制您是否可以安全地測量、監控及管理您的實體、虛擬和雲端運算環境。

更有效、更快速地啟用重要的業務服務

我們認為對 IT 組織提供最大控制權限，是提供及時服務交付並符合成本效益的唯一方式。隨著組織繼續推動革新，用來進行管理的技術也日益複雜，由變動及複雜性所帶來的壓力只會繼續提高。

經營理念

不只銷售軟體，而是銷售智慧型解決方案

為提供可靠的控制，我們會先確保已瞭解真實世界中與您類似的 IT 組織日常的操作方式。這是我們能夠開發出實際的智慧型 IT 解決方案的唯一方式，這些解決方案也已順利產生經過證明且可測量的成效。這比單純銷售軟體更有價值。

協助您成功是我們的目標

我們將您的成就視為我們的業務核心。從產品發想到部署，我們瞭解您需要能夠運作良好的 IT 解決方案，並與現有投資緊密結合；您需要持續的支援以及部署後訓練，並需要改與容易合作的對象往來。到了最後，您的成功就是我們的成就。

我們的解決方案

- 身分與存取治理
- 存取管理
- 安全性管理
- 系統與應用程式管理
- 工作量管理
- 服務管理

聯絡銷售支援

若有關於產品、價格及功能等方面的問題，請聯絡當地合作夥伴。如果您無法聯絡合作夥伴，請聯絡我們的銷售支援團隊。

全球：	www.netiq.com/about_netiq/officelocations.asp
美國和加拿大：	1-888-323-6768
電子郵件：	info@netiq.com
網站：	www.netiq.com

聯絡技術支援

若有關於特定產品的問題，請聯絡我們的技術支援團隊。

全球：	www.netiq.com/support/contactinfo.asp
北美與南美：	1-713-418-5555
歐洲、中東和非洲：	+353 (0) 91-782 677
電子郵件：	support@netiq.com
網站：	www.netiq.com/support

聯絡文件支援

我們的目標是提供符合您需求的文件。若您有任何改善建議，請按一下 HTML 文件版本任何頁面底部的 **「新增備註」**，HTML 文件版本的張貼網址是：www.netiq.com/documentation。您也可以將電子郵件寄至 Documentation-Feedback@netiq.com。我們重視您的意見並期待您提出建議。

聯絡線上使用者社群

Qmunity (NetIQ 線上社群) 是一個協同網路，將您與使用者和 NetIQ 專家連接起來。透過提供更多立即的資訊、有用資源的實用連結以及諮詢 NetIQ 專家的管道，Qmunity 協助確保您精通必要知識，以充分發揮您所仰賴之 IT 投資的全部潛力。如需詳細資訊，請造訪 http://community.netiq.com。

1 什麼是 Identity Console？

Identity Console 是最新技術的 Web 式管理主控台，可提供透過網際網路和 Web 瀏覽器從任何位置對網路管理公用程式進行虛擬、安全且自訂的存取。Identity Console 可讓系統管理任務的分權化更為容易。

Identity Console 的功能

Identity Console 提供下列功能：

- 管理 eDirectory 物件、使用者、綱要、分割區、複本、權限等
- 管理 Identity Manager 驅動程式和驅動程式集
- 管理和檢視驅動程式的效能統計資料
- 檢查物件、檢視驅動程式的資料流、管理授權、工作順序等等。
- 管理驅動程式的密碼同步狀態和設定
- 管理密碼規則和登入方法
- 管理證書
- 管理各種網路資源
- 改善保全措施以保護您的資料
- 改善延展性以管理較大型 eDirectory 物件
- 透過 One SSO Provider (OSP) 保護對 Identity Console 入口網站的登入
- 以產業中最新的 UI 技術為建立基礎
- 透過 Docker 容器易於安裝和設定

2 如何存取 Identity Console？

您可以從任何支援的網頁瀏覽器存取 Identity Console 及其提供的完整功能。或許您以可使用未列出的網頁瀏覽器存取 Identity Console，但我們不保證未獲得正式支援的任何瀏覽器可正常運作，或可支援全部功能。

重要：如需關於支援網頁瀏覽器的資訊，請參閱 *《Identity Console 安裝指南》*。

存取 Identity Console

若要存取以伺服器為基礎的 Identity Console，請執行下列步驟：

1. 在支援之網頁瀏覽器的網址 (URL) 欄位中輸入以下內容。

   安全登入：https://*<server-ip-address*/hostname>:<port>/identityconsole/

   在範例中，*<server-ip-address>* 中的 IP 位址應該是 IPv4。使用的預設連接埠為 9000。
2. 使用您的使用者 dn 和密碼登入。
3. 指定具有或不具有 ldap 安全埠的 eDirectory 樹狀結構 IP 或 DNS。

附註：

- 在 Identity Console 中重新整理任何索引標籤將會因為安全性因素，而將使用者登出。
- 在瀏覽器中開啟重複的 Identity Console 索引標籤將會因為安全性因素，而將使用者登出。
- dn 應以 cn=admin,ou=sa,o=system 格式指定。
- 當以非預設連接埠配置 eDirectory 時，您必須指定連接埠編號。

3 導覽 Identity Console 介面

本小節說明如何導覽 Identity Console Web 介面。

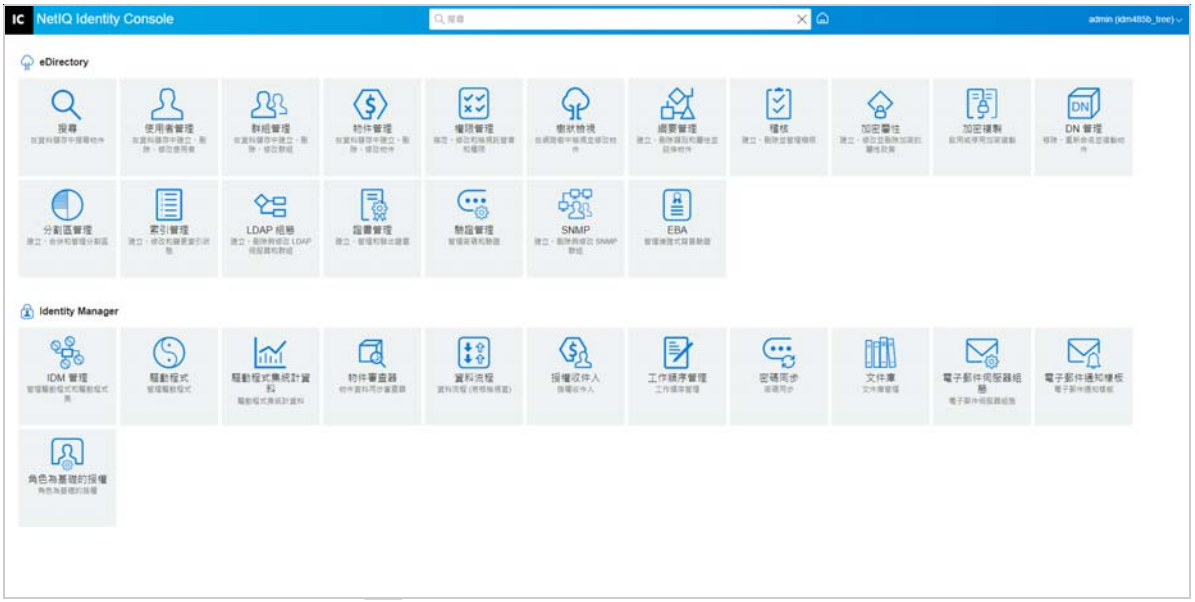
搜尋 (技術預覽)

搜尋 (技術預覽) 為您提供了搜尋功能的介紹性配置。在此預覽中，您可以指定關鍵字，搜尋欄位會確定要搜尋和顯示比對結果的資訊來源。使用此選項，您可以尋找資源，並在 Identity Console 應用程式的任何頁面上輕鬆存取該資源。

Identity Console 介面

Identity Console 介面由 eDirectory 和 Identity Manager 模組組成。

圖 3-1 *Identity Console 介面*



重要：本指南中使用的數個 GIF 動畫僅適用線上文件。如果您決定切換到 PDF，則只會顯示螢幕擷取畫面。

表格 3-1 Identity Console Web 入口網站各種模組的說明

模組名稱	描述
搜尋	搜尋資料儲存中的物件。如需詳細資訊，請參閱第 4 章 「執行搜尋」 (第 23 頁)。
使用者管理	在資料儲存中建立、刪除和修改使用者。如需詳細資訊，請參閱 第 5 章 「管理使用者」 (第 25 頁)。
群組管理	在資料儲存中建立、刪除和修改群組。如需詳細資訊，請參閱 第 6 章 「管理群組」 (第 35 頁)。
物件管理	在資料儲存中建立、刪除和修改物件。如需詳細資訊，請參閱第 7 章 「管理物件」 (第 41 頁)。
權限管理	指派、修改和檢視託管者和權限。如需詳細資訊，請參閱第 8 章 「管理權限」 (第 49 頁)。
樹狀檢視	檢視和修改樹狀中的物件。如需詳細資訊，請參閱 第 9 章 「樹狀檢視」 (第 53 頁)。
綱要管理	建立、刪除類別、輔助類別、屬性和延伸物件。如需詳細資訊，請參閱第 10 章 「管理綱要」 (第 57 頁)。
稽核	啟用、停用和管理 CEF 稽核。如需詳細資訊，請參閱 第 11 章 「管理稽核事件」 (第 65 頁)。
加密屬性	建立、修改、刪除和檢視已加密屬性的規則。如需詳細資訊，請參閱 第 12 章 「管理加密屬性」 (第 71 頁)。
加密複製	啟用、停用和檢視加密複製。如需詳細資訊，請參閱第 13 章 「管理加密複製」 (第 75 頁)。
DN 管理	移動、重新命名和複製物件。如需詳細資訊，請參閱 第 7 章 「管理物件」 (第 41 頁)。
分割區管理	建立、合併和移動分割區和複製本。如需詳細資訊，請參閱 第 14 章 「管理分割區與複製本」 (第 77 頁)。
索引管理	建立、修改和變更索引狀態。如需詳細資訊，請參閱 第 15 章 「管理索引」 (第 81 頁)。
LDAP 組態	建立、刪除和修改 LDAP 物件。如需詳細資訊，請參閱 第 16 章 「設定 LDAP 物件」 (第 85 頁)。
憑證管理	建立和管理伺服器和 CA 證書。如需更多資訊，請參閱 第 17 章 「管理證書」 (第 89 頁)。
驗證管理	建立和管理 login.post-login 方法和序列。您還可以使用此模組來管理密碼規則和安全集。如需詳細資訊，請參閱 第 18 章 「管理驗證框架」 (第 105 頁)。

模組名稱	描述
SNMP	建立、刪除和修改 SNMP 群組。如需詳細資訊，請參閱 第 19 章 「管理 SNMP 群組物件」(第 119 頁)。
EBA	管理增強的背景驗證。如需詳細資訊，請參閱 第 20 章 「管理增強性背景驗證」(第 123 頁)。
IDM 管理	管理 Identity Manager 驅動程式和驅動程式集。如需詳細資訊，請參閱第 21 章 「管理驅動程式和驅動程式集」(第 127 頁)。您還可以使用此模組管理驅動程式集內容。如需詳細資訊，請參閱 第 22 章 「管理驅動程式集內容」(第 133 頁)。
驅動程式內容	管理各種驅動程式的內容。如需詳細資訊，請參閱 第 23 章 「管理驅動程式內容」(第 145 頁)。
驅動程式集統計資料	管理和檢視驅動程式集統計資料。如需詳細資訊，請參閱第 24 章 「管理驅動程式集統計資料」(第 171 頁)。
物件檢查者	管理物件關聯和資料同步。如需詳細資訊，請參閱 第 25 章 「審查 Identity Manager 物件」(第 173 頁)。
資料流	管理和檢視驅動程式的資料流。如需詳細資訊，請參閱 第 26 章 「管理資料流程」(第 175 頁)。
授權收件者	管理授權收件者。如需詳細資訊，請參閱 第 27 章 「管理授權收件人」(第 177 頁)。
工作順序管理	管理工作順序。如需詳細資訊，請參閱 第 28 章 「管理工作順序」(第 179 頁)。
密碼同步化	管理密碼同步和狀態。如需詳細資訊，請參閱 第 29 章 「管理密碼狀態和同步」(第 183 頁)。
文件庫管理	管理文件庫。如需詳細資訊，請參閱 第 30 章 「管理程式庫」(第 187 頁)。
電子郵件伺服器組態	管理電子郵件伺服器選項。如需詳細資訊，請參閱 第 31 章 「管理電子郵件伺服器選項」(第 189 頁)
電子郵件通知範本	管理電子郵件範本。如需詳細資訊，請參閱 第 32 章 「管理電子郵件範本」(第 191 頁)

使用 Identity Console 管理 eDirectory

本節描述了您可以執行的各種任務，以使用 Identity Console 入口網站管理您的 eDirectory 伺服器。

4 執行搜尋

「搜尋」磚可讓您指定在目錄樹上執行的搜尋作業並顯示結果。此選項可讓您搜尋各種物件、使用者、群組和數個其他項目。若要對資料儲存中的各種物件執行搜尋操作，請遵循下列步驟：

1 指定搜尋的物件名稱。使用星號萬用字元以指定部分名稱。例如：ldap*、*cert、*server* 等等。如果您僅在此欄位中使用星號，Identity Console 將根據選取的「類型」和「網路位置」傳回所有搜尋結果。

附註：使用「內容瀏覽器」，您可以在搜尋欄位中指定星號 (*) 來瀏覽整個 eDirectory 樹狀結構。您也可以使用萬用字元搜尋來篩選「內容瀏覽器」中的物件。例如，admin*。Identity Console 的各種模組都支援「內容瀏覽器」的這個行為。

---

2 選取要在類型欄位中搜尋的物件類型。Identity Console 僅會顯示指定類型的物件。預設會在此欄位中選取「使用者」類型。

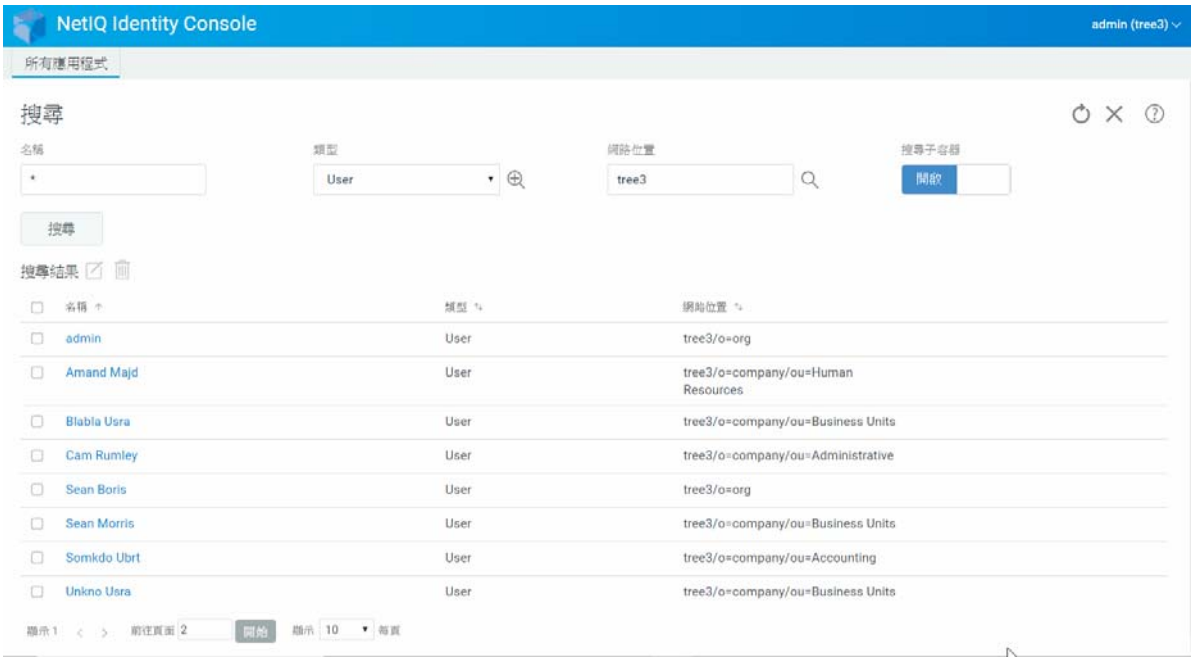
   按一下 圖示來定義其他的屬性層級搜尋設定。如需詳細資訊，請參閱 「設定進階搜尋」(第 24 頁)。

3 在「網路位置」欄位中指定用於搜尋操作的開始容器。

4 如果要搜尋併入從屬容器，請針對「搜尋子容器」選項選取「開啟」。

5 按一下 搜尋 按鈕。

圖 4-1 *執行搜尋操作*



設定進階搜尋

「進階選取」提供可設定的環境，以便在目錄中搜尋需要的物件。

物件類型：指定您要搜尋的物件基本類別。例如，「使用者」。

輔助類別：按一下 ＋ 圖示來指定要在搜尋中包含的輔助類別。

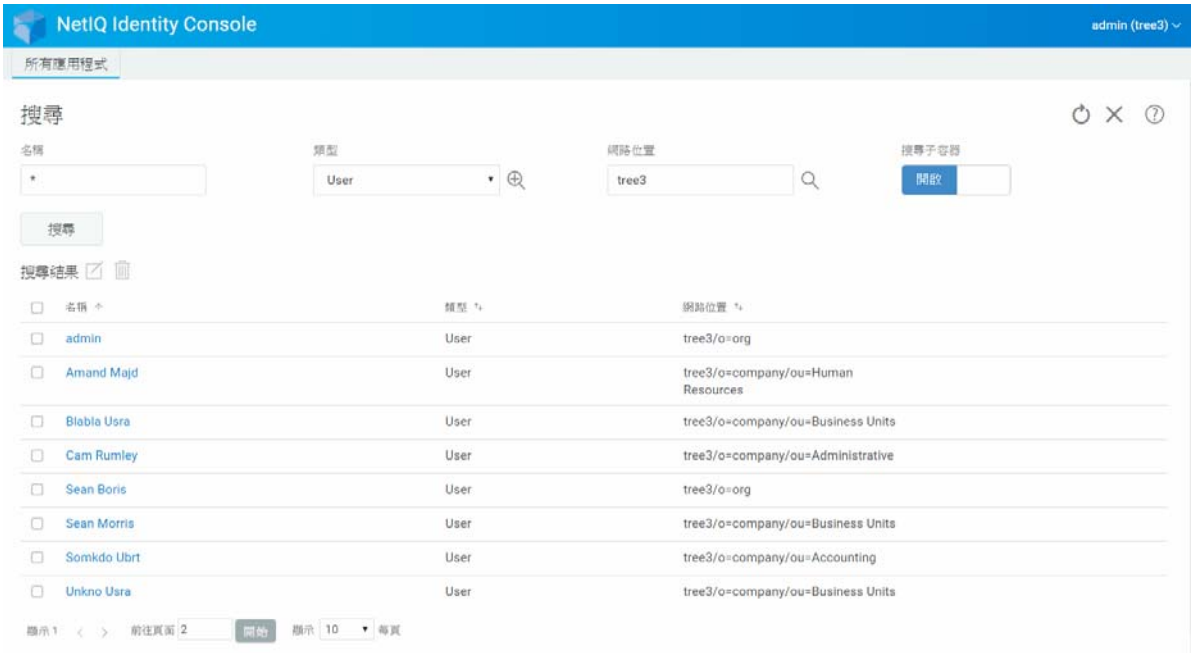
屬性：指定您要使用作為篩選器一部分的的屬性 (內容)。

運算子：指定要套用到篩選器的邏輯運算子。選項包括。

值：指定您作為篩選器的屬性值。您可以使用星號 (*) 作為萬用字元來指定部分名稱。例如，smi*、*th 和 *mit*。

此外，您可以使用 ＋ Rule 圖示將第二個屬性新增到清單，將多個屬性篩選器鏈結到篩選器群組中。使用多個屬性篩選器時，請使用邏輯 AND 或邏輯 OR 將他們連結起來。

圖 4-2 *設定進階搜尋*



5 管理使用者

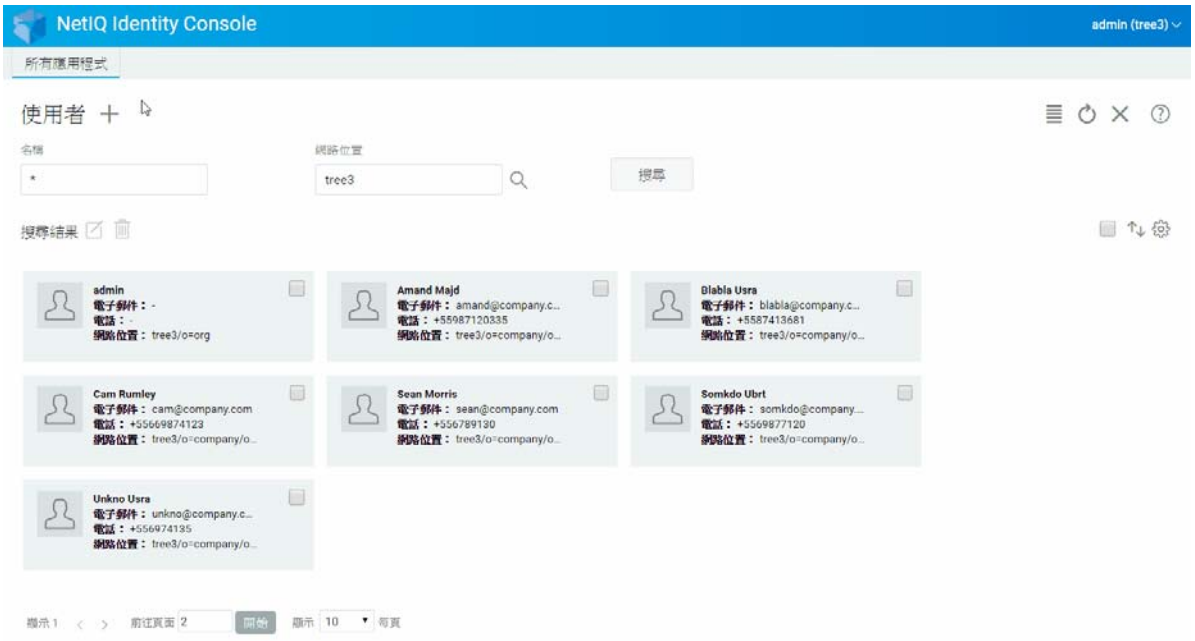
管理使用者及其網路存取是資料儲存的中心用途。您可以使用 Identity Console Web 入口網站，執行下列使用者相關的任務：

建立使用者

建立新的使用者物件：

1. 按一下位於 Identity Console 抵達頁面的 **「使用者管理」**選項。
2. 按一下 ＋ 圖示。
3. 在 「建立使用者」頁面中，請至少提供與使用者相關的必要資訊，然後按一下 **建立** 按鈕。
   - **使用者名稱**
   - **網路位置**
   - **姓**
   - **密碼**
4. 隨即顯示確認訊息，指出已建立使用者物件。

圖5-1 建立使用者



刪除使用者

刪除使用者物件：

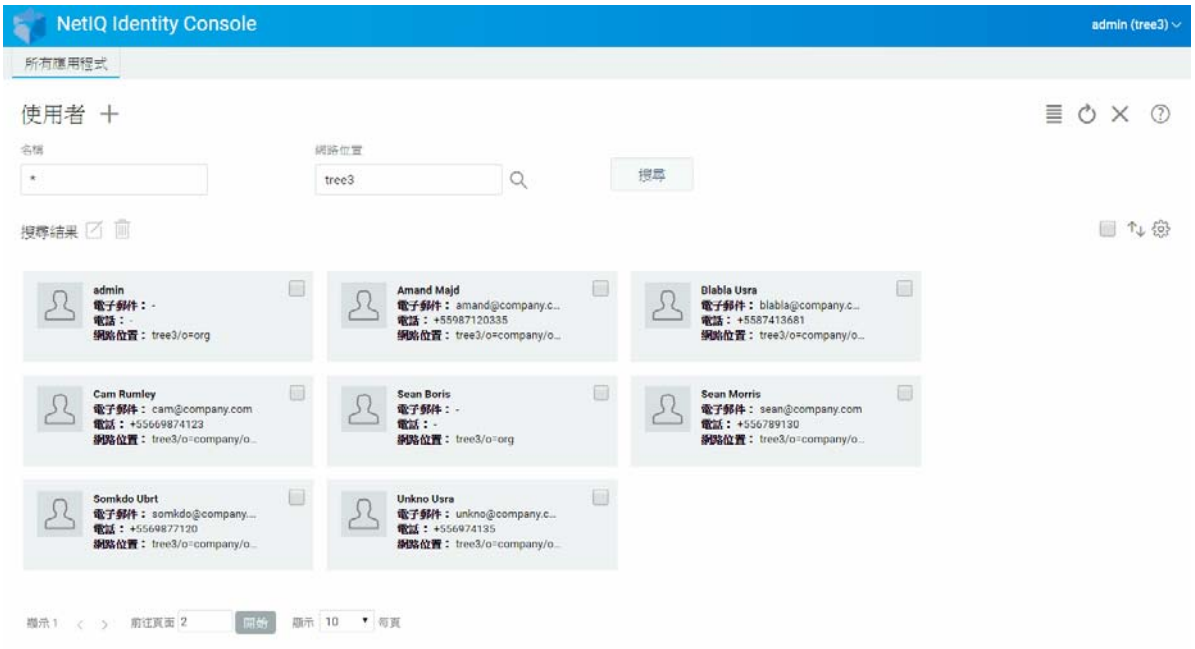
1 從 Identity Console 抵達頁面，按一下「使用者管理」選項。

2 輸入物件的名稱和網路位置，或使用搜尋功能進行尋找，然後按一下 搜尋 按鈕。

3 從使用者清單選取使用者物件，並按一下 圖示。

4 顯示確認訊息即代表使用者物件已成功刪除。

圖 5-2 刪除使用者



修改使用者

若要修改使用者物件：

1 從 Identity Console 抵達頁面，按一下「使用者管理」選項。

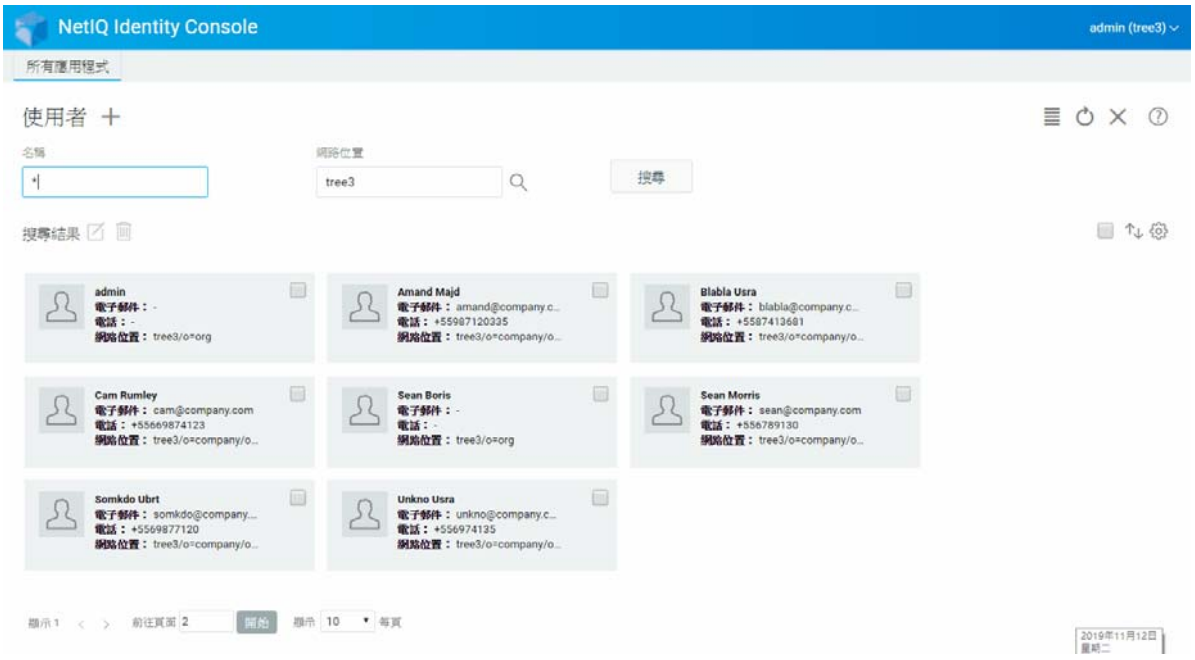
2 鍵入物件的名稱和網路位置，或使用搜尋功能進行尋找，然後按一下 搜尋 按鈕。

3 從使用者清單選取使用者物件，並按一下 圖示。

4 進行想要的變更，然後按一下 儲存 按鈕。

5 隨即顯示確認訊息，指出已修改使用者物件。

圖5-3 修改使用者



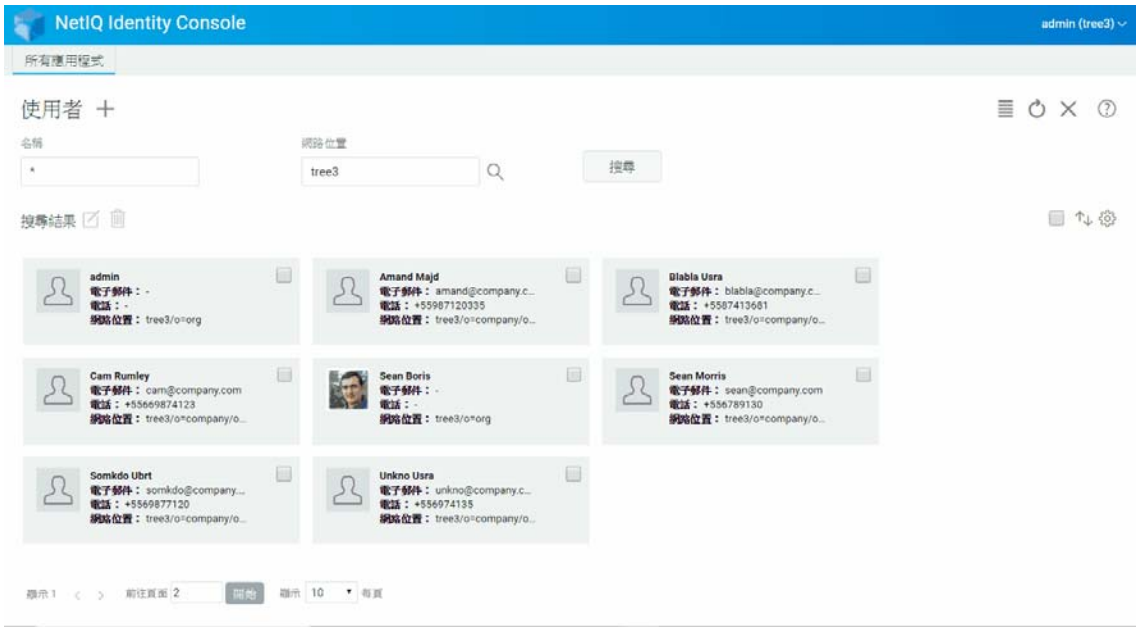
搜尋使用者

若要搜尋使用者物件：

1 從 Identity Console 抵達頁面，按一下 「使用者管理」選項。

2 您可以依名稱和同時名稱與網路位置搜尋使用者。指定需要的詳細資料之後，按一下 搜尋 圖示。

圖 5-4 搜尋使用者

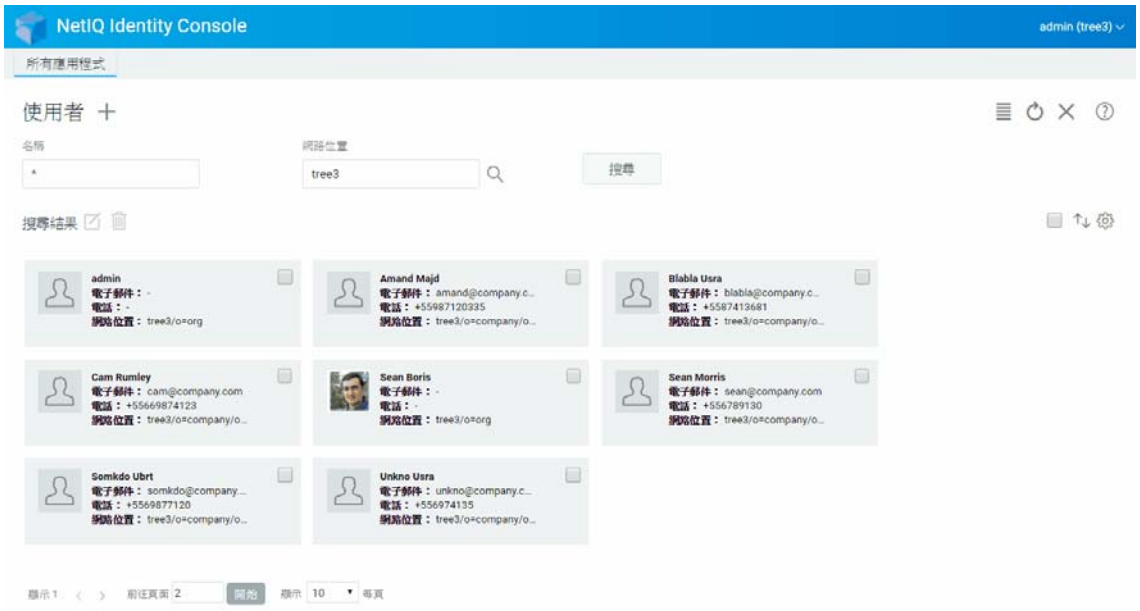


設定密碼限制

密碼限制允許您執行下列動作：

- 允許使用者變更其各自的密碼
- 強制將密碼用於登入
- 指定密碼強度
- 強制定期變更密碼
- 指定密碼過期日
- 強制建立唯一密碼
- 指定密碼已到期的情況下的寬限登入期間。

圖5-5 密碼限制

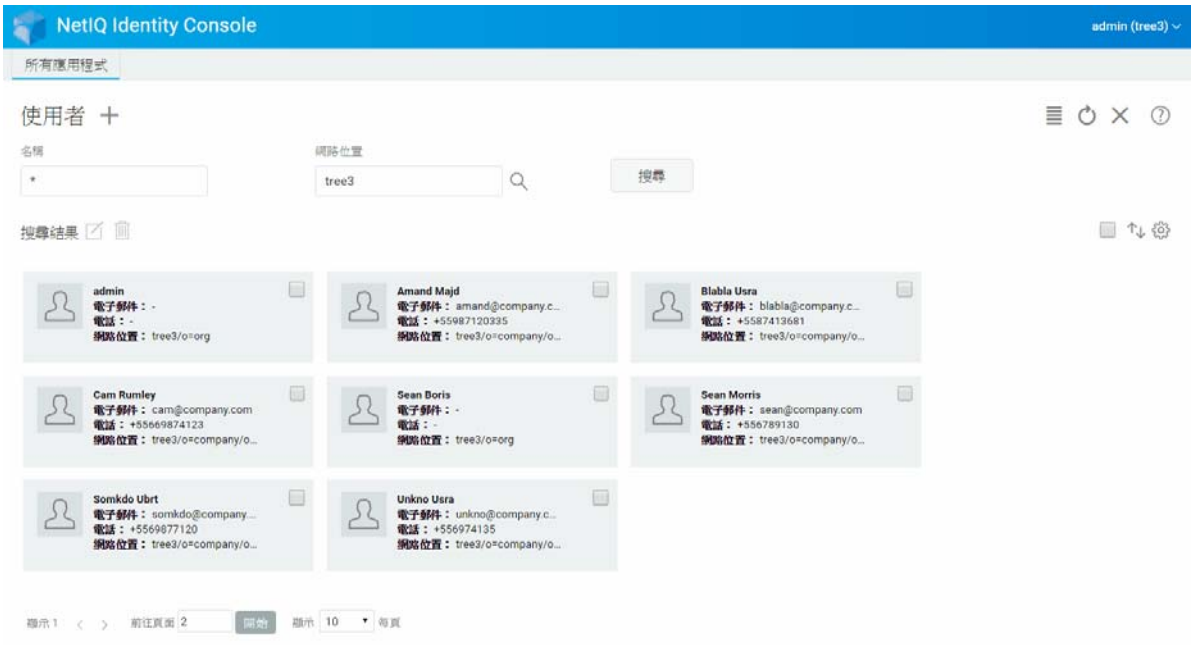


停用和啟用使用者帳戶

若要停用使用者帳戶，請執行下列步驟：

1. 選取需要停用其帳戶的使用者，並按一下 圖示。
2. 在 「修改使用者」頁面中，按一下 「限制」索引標籤。
3. 展開 「登入限制」索引標籤，並選取 「已停用帳戶」核取方塊。
4. 按一下 儲存 圖示。
5. 現在該使用者帳戶已停用。若要啟用任何停用的使用者帳戶，請取消選取 「已停用帳戶」核取方塊。

圖5-6 停用和啟用使用者帳戶

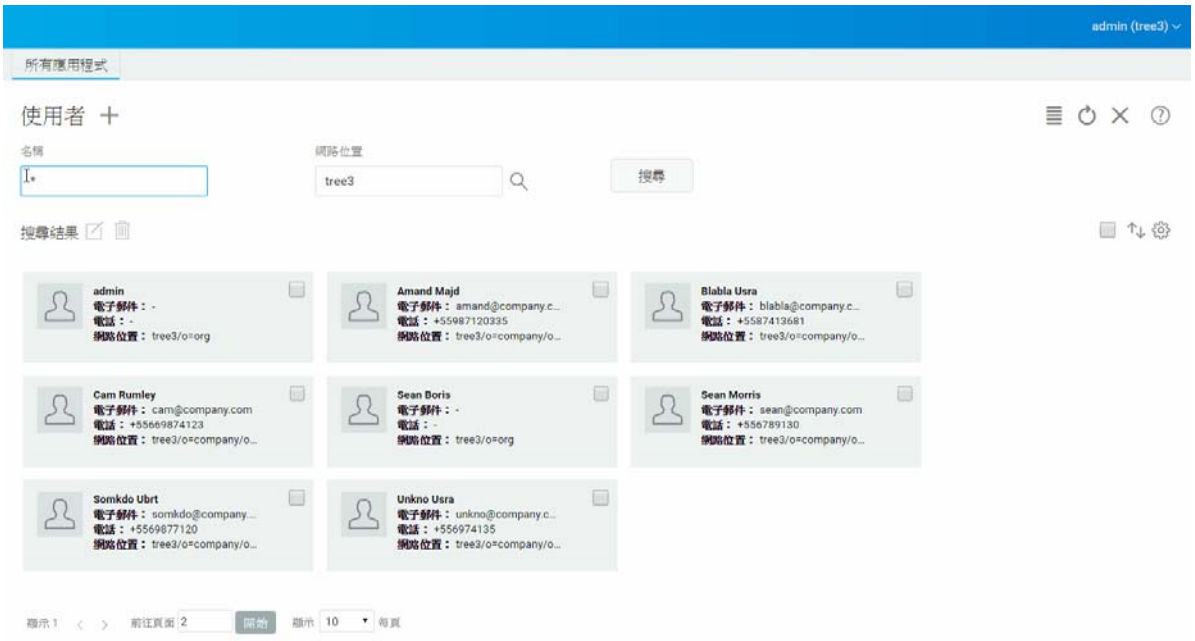


設定帳戶過期日

若要設定使用者的帳戶過期日，請執行下列步驟：

1. 選取需要設定其帳戶過期日的使用者，並按一下 圖示。
2. 在 「修改使用者」頁面中，按一下 「限制」索引標籤。
3. 展開 「登入限制」索引標籤，並選取 「帳戶有過期日」核取方塊，然後指定 「過期日」。
4. 按一下 儲存 圖示。

圖5-7 設定帳戶過期日

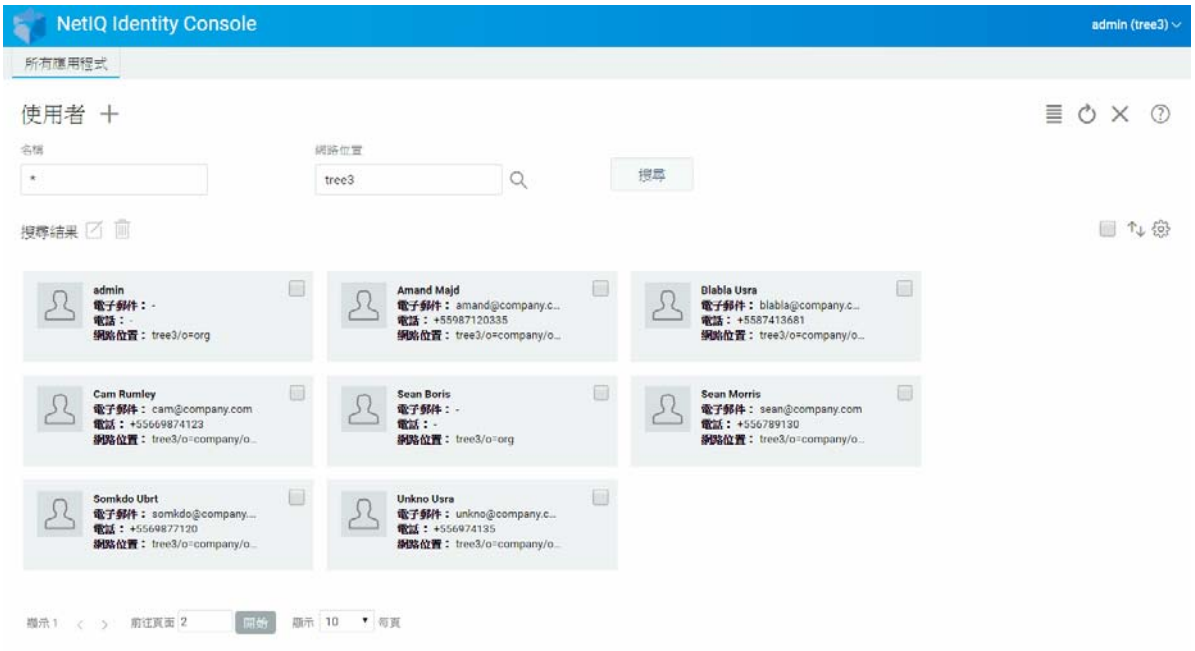


檢查和清除侵入者鎖定狀態

您可以使用 Identity Console Web 入口網站，來檢視任何使用者帳戶侵入者鎖定狀態的詳細資料。若要檢視侵入者鎖定狀態詳細資料：

1. 選取需要檢查其侵入者鎖定狀態詳細資料的使用者，並按一下 圖示。
2. 在 「修改使用者」頁面中，按一下 「限制」索引標籤。
3. 展開 「侵入者鎖定狀態」索引標籤，並檢視侵入者鎖定狀態的詳細資料。
4. 現在選取 「清除鎖定狀態」索引標籤，並按一下 清除鎖定 按鈕。
5. 按一下 儲存 按鈕。

圖 5-8 檢查和清除侵入者鎖定狀態



6 管理群組

群組通常會包含一些成員。任何建立群組的使用者都會自動成為該群組的擁有者。下列操作可以使用群組管理功能執行：

如需使用和設定群組物件的詳細資訊，請參閱 *《NetIQ eDirectory 9.2 管理指南》*(https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html)。

建立群組

若要建立群組：

1. 從 Identity Console 抵達頁面，按一下 **「群組管理」**選項。
2. 按一下 ＋ 圖示。
3. 在 「建立群組」頁面中，輸入下列詳細資料：
   - 指定群組名稱
   - 指定網路位置

   選取 **「動態群組」**將新群組建立為屬於 dynamicGroup 類別的動態群組。否則，會將群組建立為靜態群組。

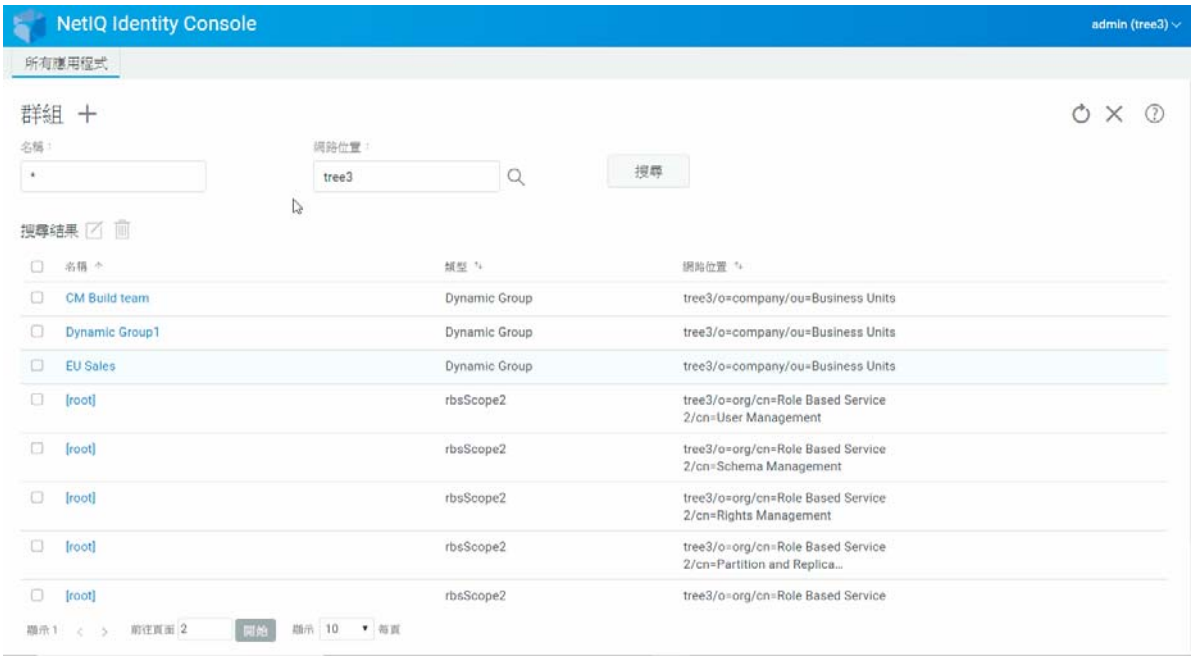
   選取 **「巢狀群組」**使得新群組成為巢狀群組，以便該群組可利用輔助類別 nestedGroupAux 建立。

   附註：您可以使用修改物件中提及的程序，將靜態群組轉換為動態群組或巢狀群組。這會將選取的群組物件延伸，以分別屬於 dynamicGroupAux 類別或 nestedGroupAux 類別。

   群組可以是巢狀或動態。您無法建立同時為巢狀與動態的群組。

   ---
4. 指定需要的詳細資料之後，按一下 建立 按鈕。
5. 隨即顯示確認訊息，指出已建立群組。

圖6-1 建立群組

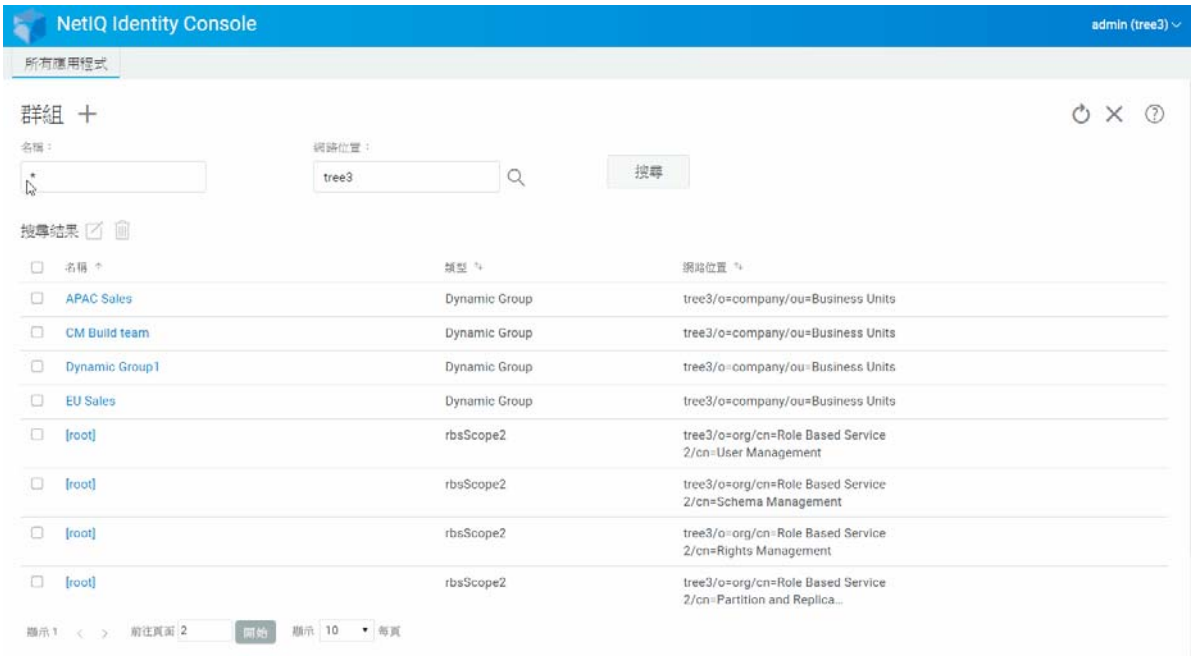


刪除群組

若要刪除群組：

1. 從 Identity Console 抵達頁面，按一下「**群組管理**」選項。
2. 指定群組的名稱和網路位置，或使用搜尋功能進行搜尋，然後按一下 搜尋 按鈕。
3. 選取需要刪除的群組，並按一下 圖示。
4. 隨即顯示確認訊息，指出已刪除群組。

圖 6-2 刪除群組



修改群組

若要修改群組：

1 從 Identity Console 抵達頁面，按一下「**群組管理**」選項。

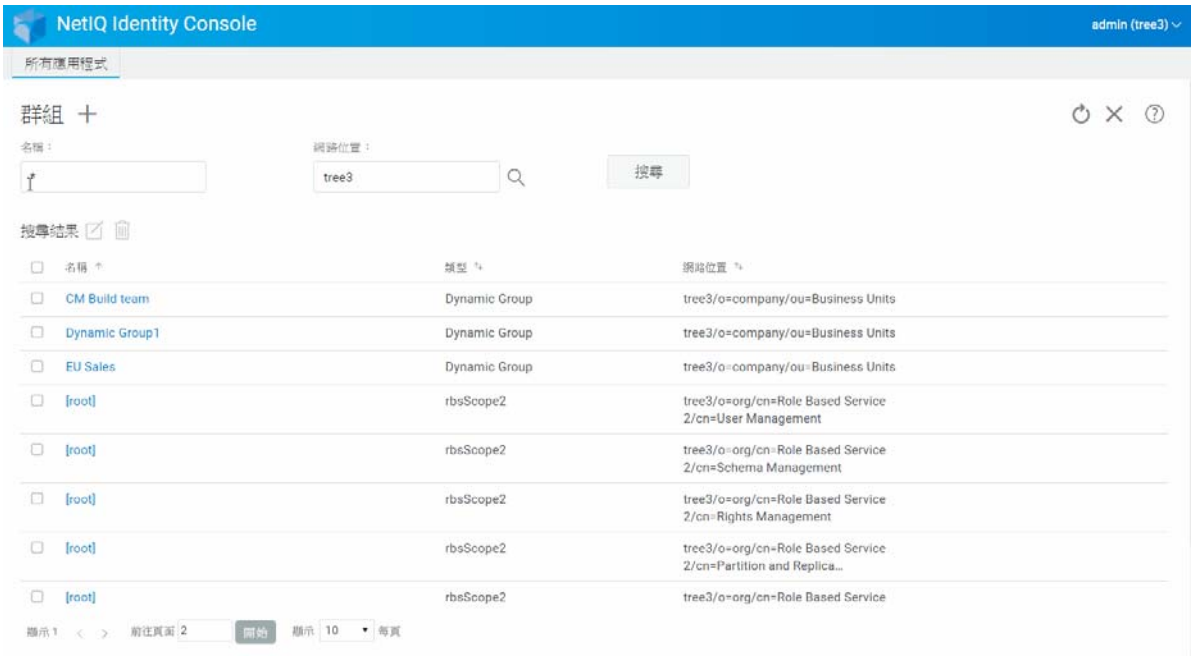
2 鍵入群組的名稱和網路位置，然後按一下 搜尋 按鈕。

3 選取需要修改的群組，並按一下 圖示。

4 進行想要的變更，然後按一下 儲存 按鈕。

5 隨即顯示確認訊息，指出已修改群組。

圖6-3 修改群組



新增或修改群組成員

若要新增或修改群組成員：

1 從 Identity Console 抵達頁面，按一下「**群組管理**」選項。

2 輸入群組的名稱和網路位置，然後按一下 搜尋 按鈕。

3 選取群組，並按一下 圖示。

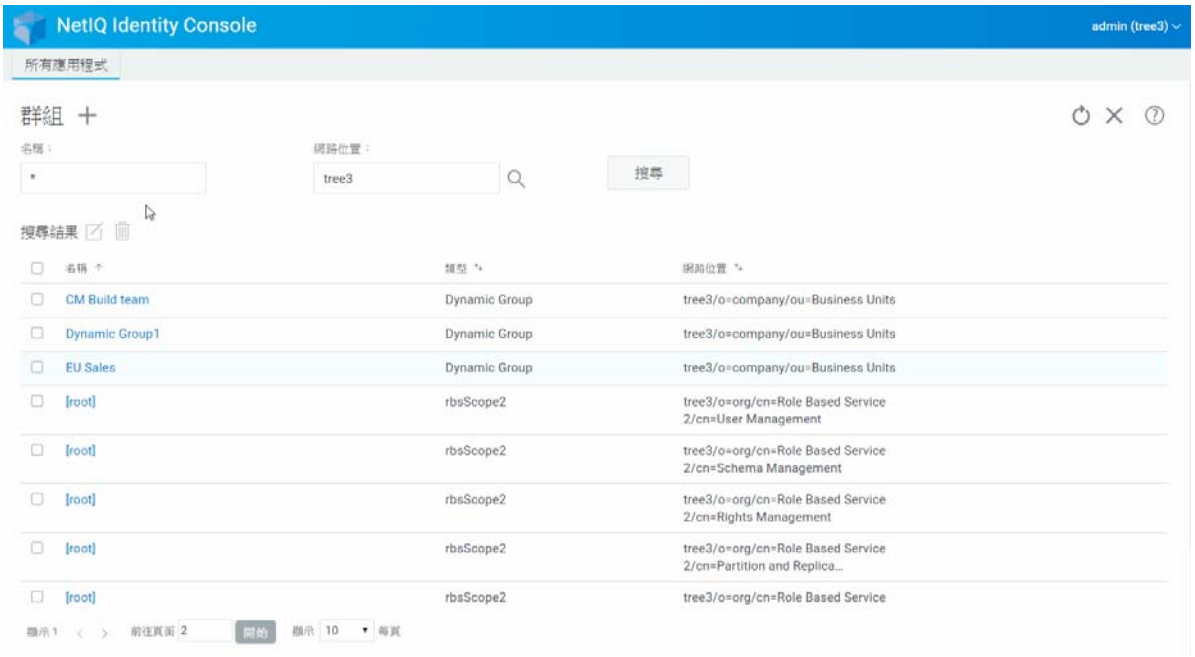
4 在「**修改群組**」頁面中，按一下「**成員**」索引標籤。

5 使用 + 圖示來將新成員新增至群組。如果您決定從群組移除成員，請按一下 圖示。

6 進行變更後，按一下 儲存 按鈕。

7 隨即顯示確認訊息，指出已修改群組。

圖 6-4 新增或修改群組成員

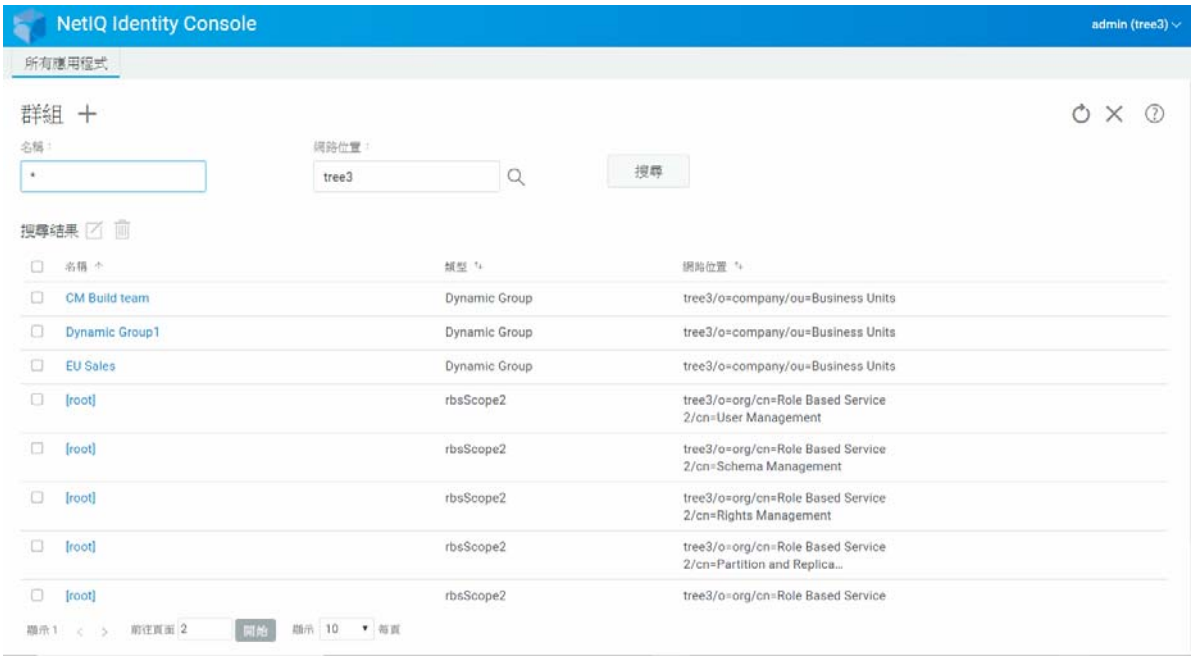


搜尋群組

若要搜尋群組：

1. 從 Identity Console 抵達頁面，按一下 **「群組管理」**選項。
2. 您可以依名稱和同時依名稱與網路位置搜尋群組。
3. 指定需要的詳細資料之後，按一下 搜尋 圖示。

圖6-5 搜尋群組


NetIQ Identity Console
admin (tree3)
所有應用程式
群組 +
名稱：
*
網路位置：
tree3
搜尋
搜尋結果
名稱
類型
網路位置
CM Build team
Dynamic Group
tree3/o=company/ou=Business Units
Dynamic Group1
Dynamic Group
tree3/o=company/ou=Business Units
EU Sales
Dynamic Group
tree3/o=company/ou=Business Units
[root]
rbsScope2
tree3/o=org/cn=Role Based Service 2/cn=User Management
[root]
rbsScope2
tree3/o=org/cn=Role Based Service 2/cn=Schema Management
[root]
rbsScope2
tree3/o=org/cn=Role Based Service 2/cn=Rights Management
[root]
rbsScope2
tree3/o=org/cn=Role Based Service 2/cn=Partition and Replica...
[root]
rbsScope2
tree3/o=org/cn=Role Based Service
顯示 1
前往頁面 2
開始
顯示 10
每頁

7 管理物件

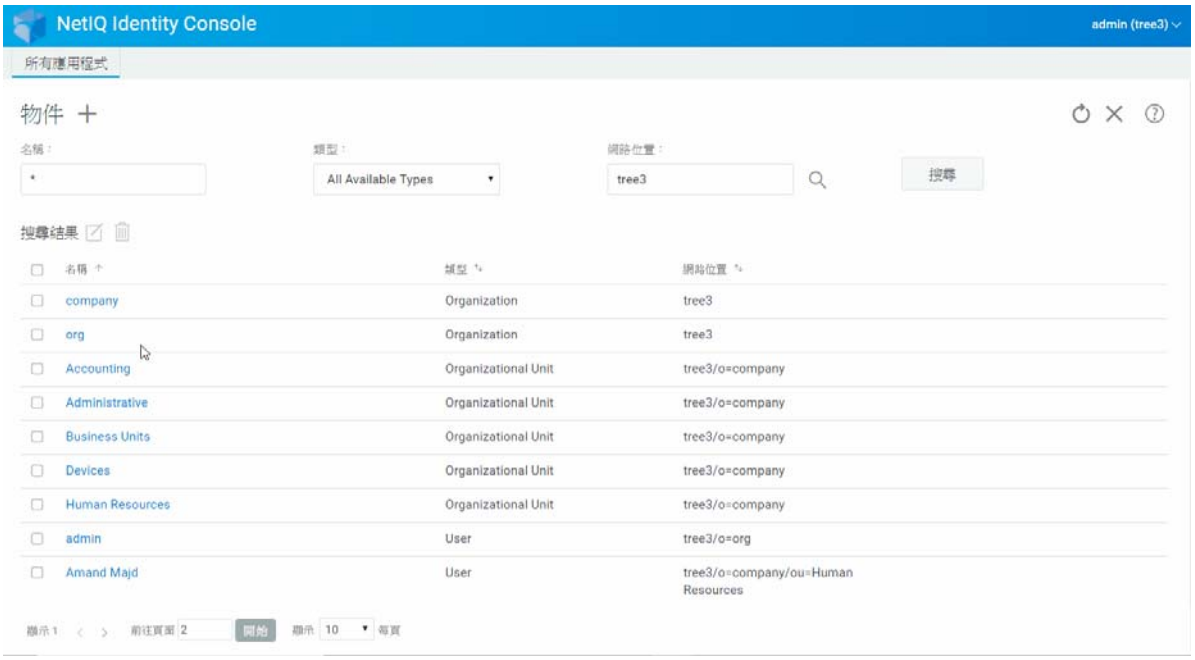
Identity Console 可讓您管理資料儲存中的各種物件。您可以使用此模組來建立、修改、刪除和搜尋物件。

建立物件

若要建立新的物件：

1. 從 Identity Console 抵達頁面，按一下 **「物件管理」**選項。
2. 按一下 ＋ 圖示。
3. 在 「建立物件」頁面中，輸入下列詳細資料：
   - 指定物件名稱
   - 指定類型
   - 指定網路位置
4. 輸入所有需要的詳細資料之後，按一下 **「下一步」** > **「建立」**。
5. 隨即顯示確認訊息，指出已建立物件。

圖 7-1 建立物件

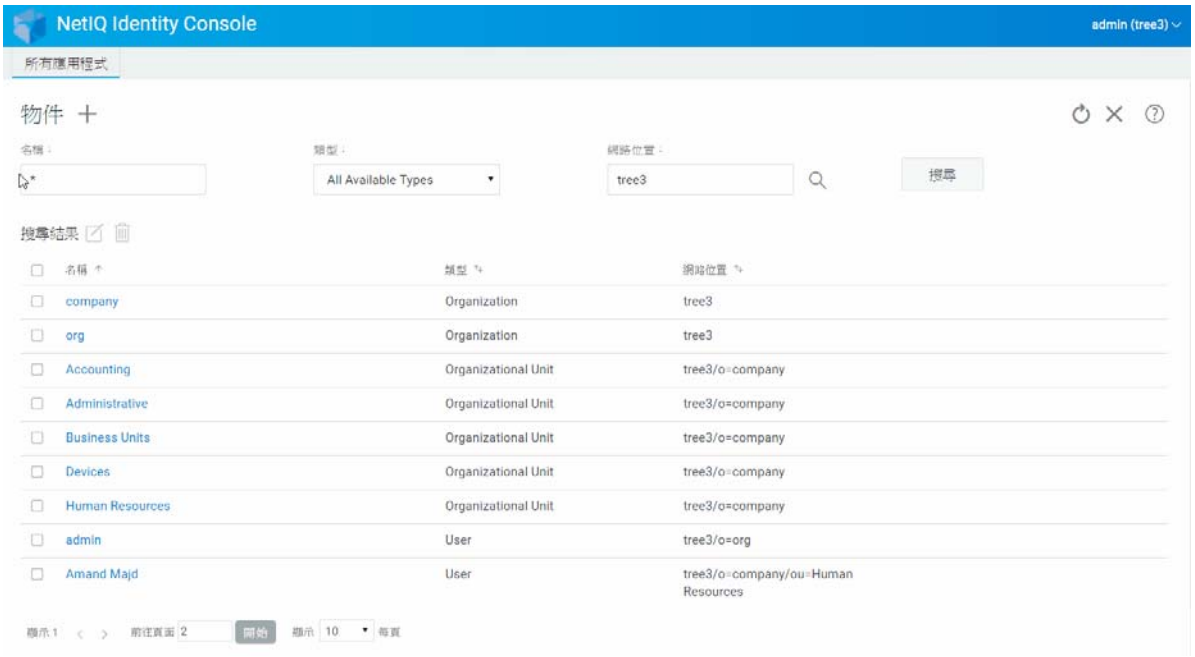


刪除物件

若要刪除物件：

1. 從 Identity Console 抵達頁面，按一下「**物件管理**」選項。
2. 指定物件的名稱、類型和網路位置，或使用搜尋功能進行尋找，然後按一下 搜尋 按鈕。
3. 從搜尋清單選取物件，然後按一下 圖示。
4. 隨即顯示確認訊息，指出已刪除物件。

圖 7-2 刪除物件



修改物件

若要修改物件：

1 從 Identity Console 抵達頁面，按一下「**物件管理**」選項。

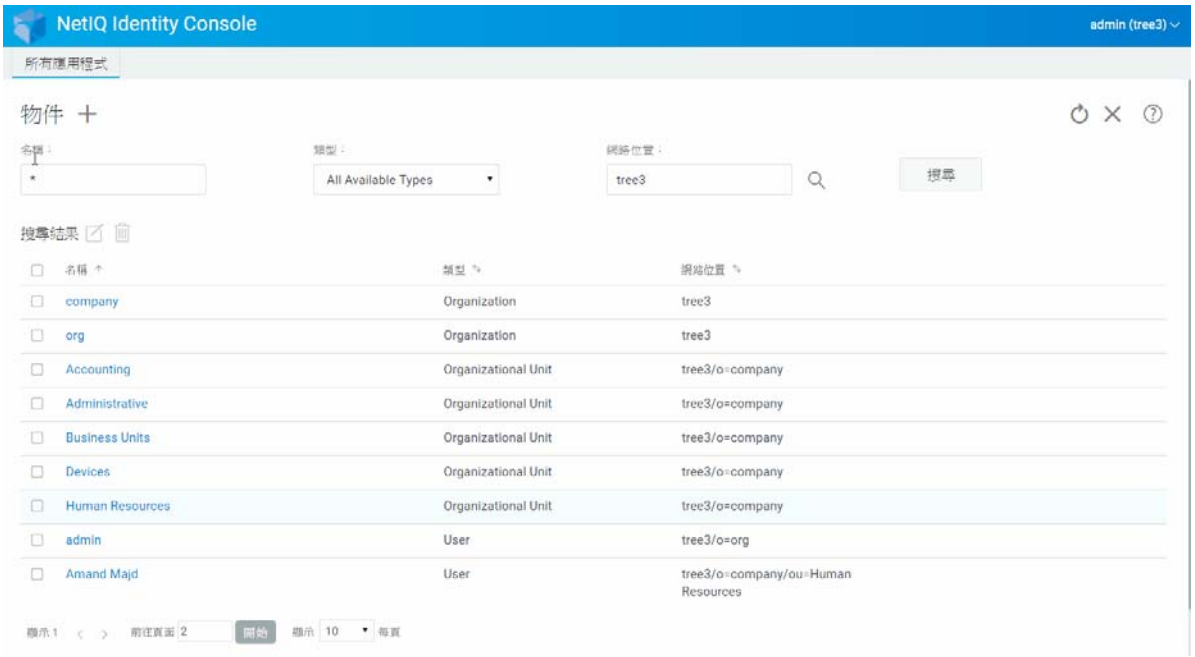
2 輸入物件的名稱、類型和網路位置，然後按一下 搜尋 按鈕。

3 從搜尋清單選取物件，並按一下 圖示。

4 進行想要的變更，然後按一下 儲存 按鈕。

5 隨即顯示確認訊息，指出已修改物件。

圖 7-3 修改物件

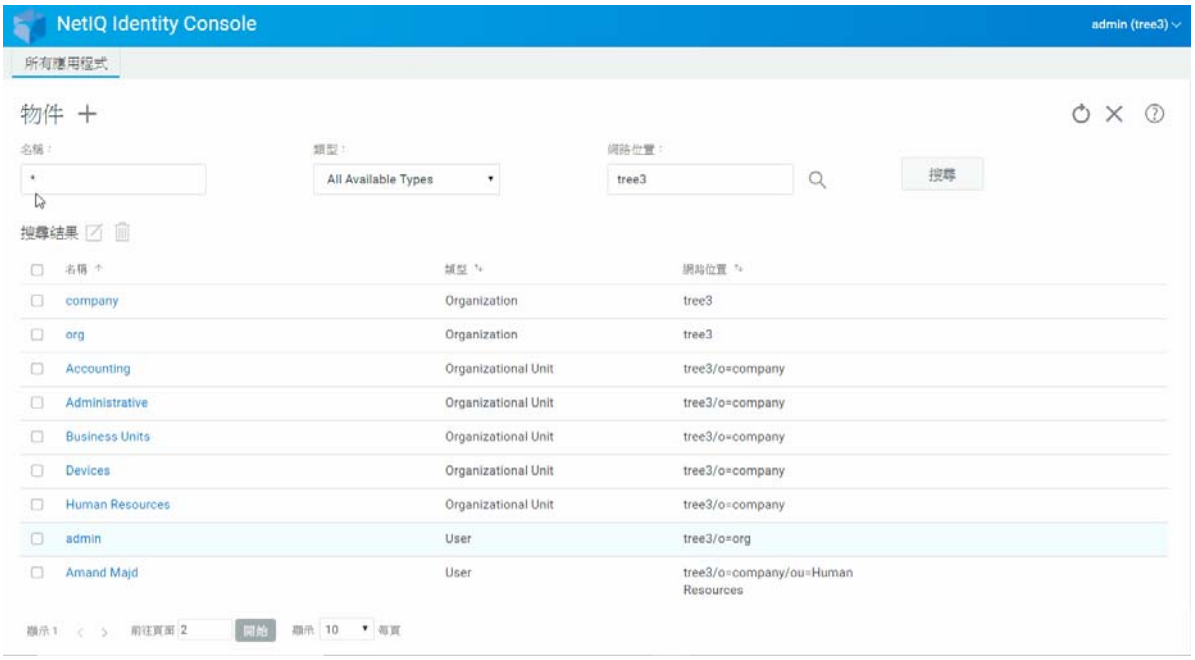


搜尋物件

若要搜尋物件：

1. 從 Identity Console 抵達頁面，按一下「**物件管理**」選項。
2. 您可以依名稱或同時依名稱與網路位置搜尋物件。
3. 指定需要的詳細資料之後，按一下 搜尋 按鈕。

圖 7-4 搜尋物件



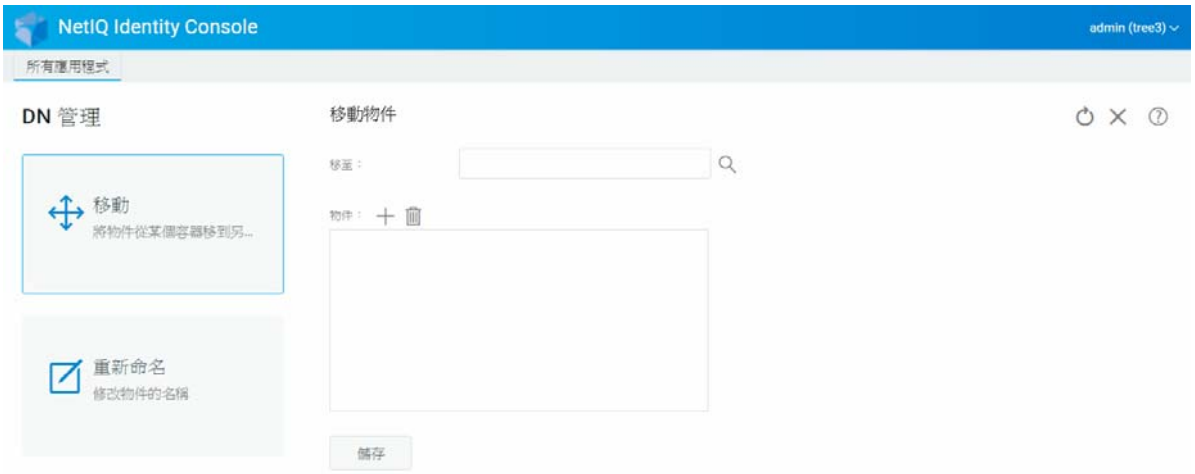
移動物件

若要移動物件：

1. 從 Identity Console 抵達頁面，按一下「**DN 管理**」選項。
2. 「**移動物件**」選項會預設選取。
3. 在「**移至**」欄位中，選取要移入此物件的容器。
4. 按一下 ＋ 圖示來新增您要移動到不同容器的物件。

   如果要移除選取的物件，請按一下 圖示。
5. 按一下 儲存 按鈕。
6. 顯示確認訊息即代表移動物件作業已成功完成。

圖 7-5 移動物件

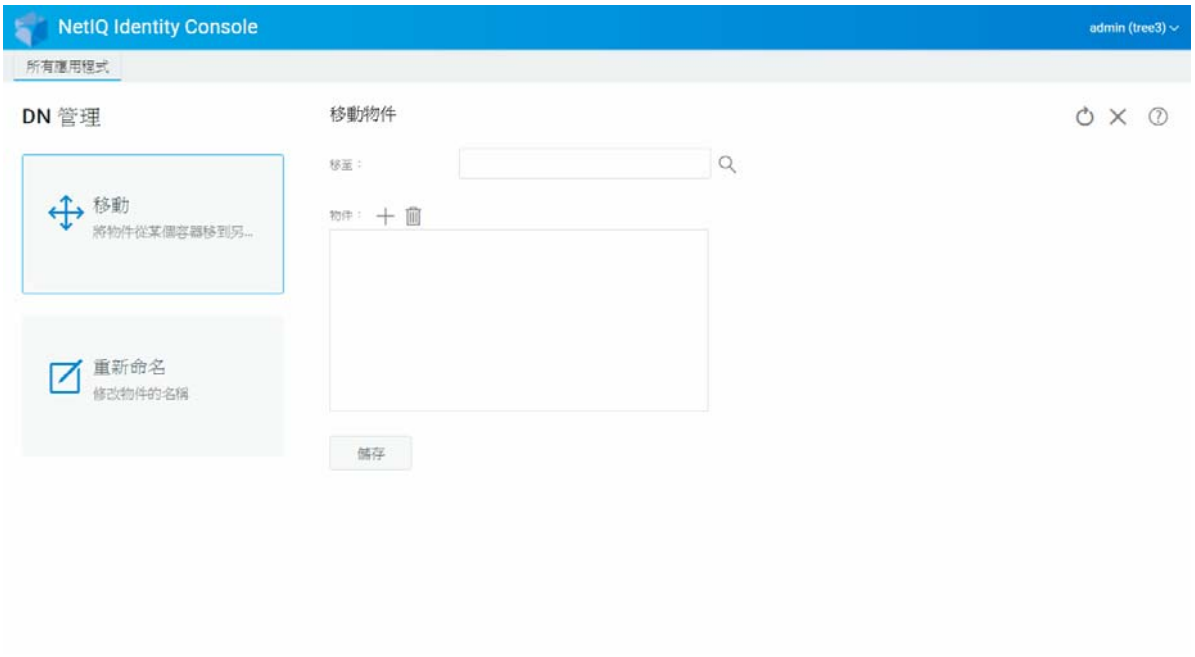


重新命名物件

若要重新命名物件：

1. 從 Identity Console 抵達頁面，按一下 「**DN 管理**」選項。
2. 選取 「**重新命名物件**」選項。
3. 使用搜尋功能來尋找需要在 「**物件名稱**」欄位中重新命名的物件。
4. 僅在 「**新名稱**」欄位中指定物件的新名稱。請勿指定網路位置。
5. 如果要儲存舊名稱，請選取以進行儲存。
6. 按一下 儲存 按鈕。
7. 隨即顯示確認訊息，指出已成功完成重新命名物件作業。

圖 7-6 重新命名物件


NetIQ Identity Console
admin (tree3)
所有應用程式
DN 管理
移動物件
移動
將物件從某個容器移到另...
重新命名
修改物件的名稱
移至：
物件：
儲存

8 管理權限

權限指的是 eDirectory 託管者權限和託管者。在您建立網路樹時，預設的權限任務會為您的網路提供通用的存取與保全性。Identity Console 可讓您執行下列與權限相關的任務：

- 「修改承襲的權限篩選」(第 49 頁)
- 「修改託管者權限」(第 50 頁)
- 「檢視有效權限」(第 51 頁)

如需 eDirectory 權限的詳細資訊，請參閱 *《NetIQ eDirectory 9.2 管理指南》*(https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html)。

修改承襲的權限篩選

eDirectory 提供承襲的權限篩選器 (IRF) 機制來封鎖個別從屬項目的權限承襲。

如需承襲權限篩選的詳細資訊，請參閱 *《NetIQ eDirectory 9.2 管理指南》*(https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html)。

1. 從 Identity Console 抵達頁面，按一下 **「權限管理」**選項
2. 選取 **「承襲的權限篩選器」**。

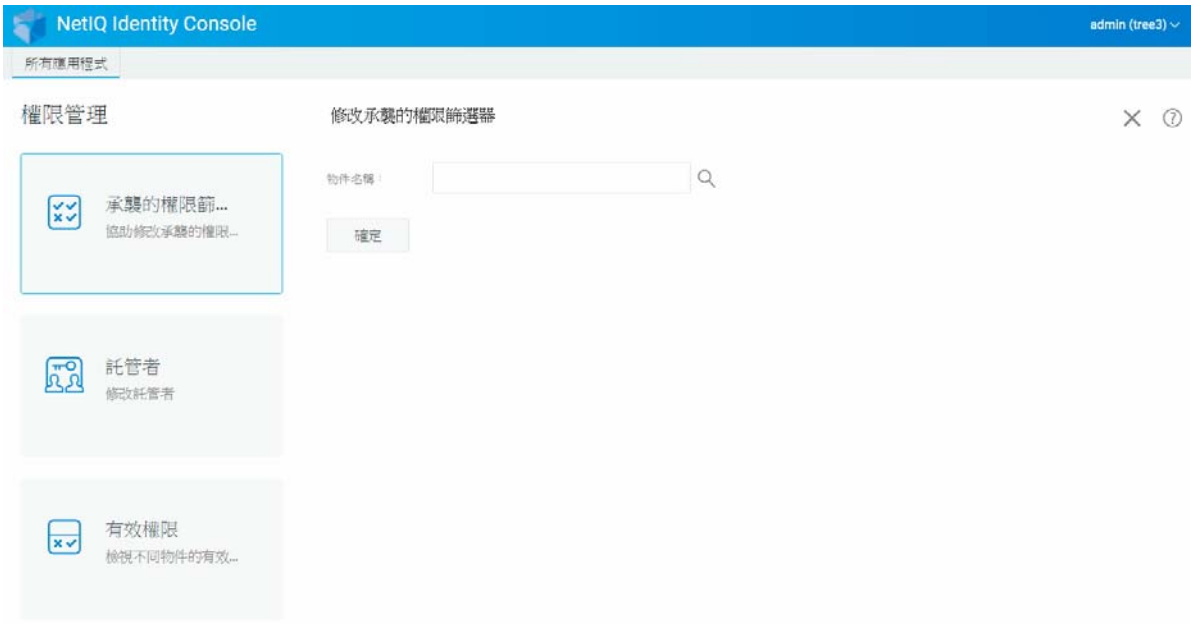
   附註：預設會選取 「承襲的權限篩選器」。

3. 指定您要修改其承襲權限篩選之物件的完整名稱，或使用 「物件選擇器」 圖示進行尋找，然後按一下 **「確定」**。

   這會顯示物件上已設定的承襲權限篩選清單。
4. 在 **「內容」**下，視需要編輯承襲的權限篩選器的清單，然後按一下 **「套用」**。

   若要編輯篩選器清單，必須擁有對物件 ACL 內容的 「監督者」或 「存取控制」權限。您可以針對整個物件、物件的所有內容及個別內容設定阻止承襲權限的篩選器。

圖 8-1 修改承襲的權限篩選



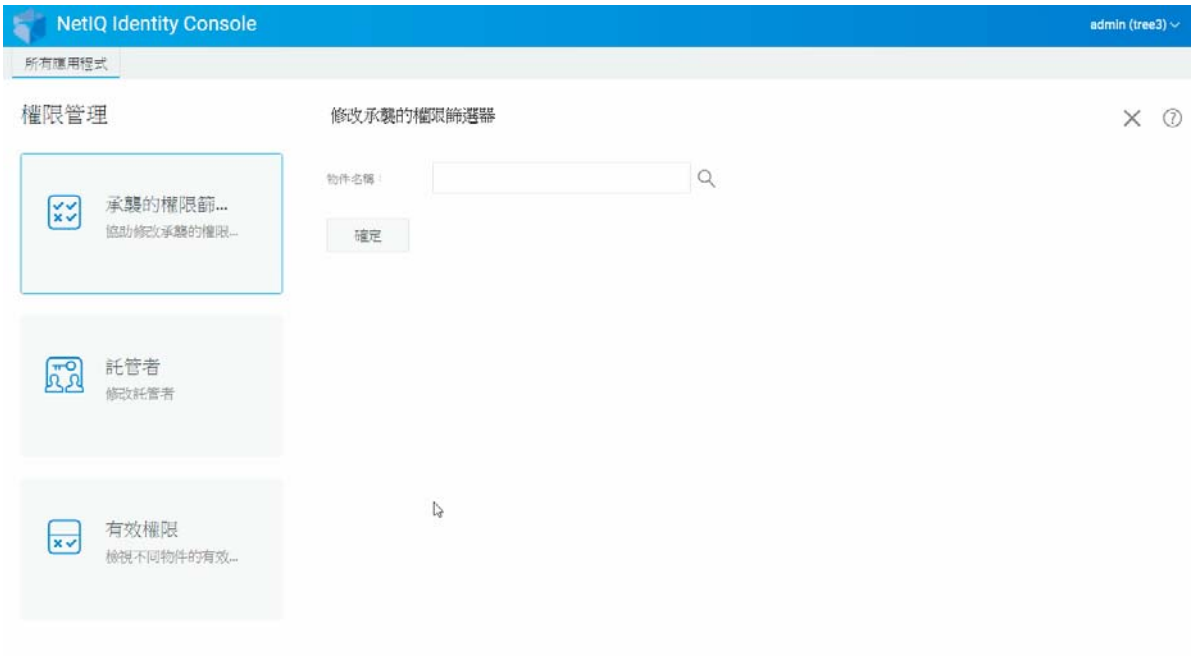
修改託管者權限

託管者是已具有您目錄樹中其他物件的明確權限的物件。若要修改指定物件的託管者清單：

1. 從 Identity Console 抵達頁面，按一下 **「權限管理」**選項
2. 選取 **「託管者」**。
3. 指定或使用「物件選擇器」圖示來尋找您要檢視其託管者清單的物件名稱，然後按一下 **「確定」**。

   這會開啟物件目前指定之託管者的清單。
4. 根據需要修改託管者清單，然後按一下 **「確定」**。
   - 按一下 ＋ 圖示來新增託管者。
   - 選取託管者的核取方塊並按一下 圖示以移除託管者。
   - 為託管者選取 **「指定的權限」**連結以修改託管者的權限指定。

圖 8-2 修改託管者權限



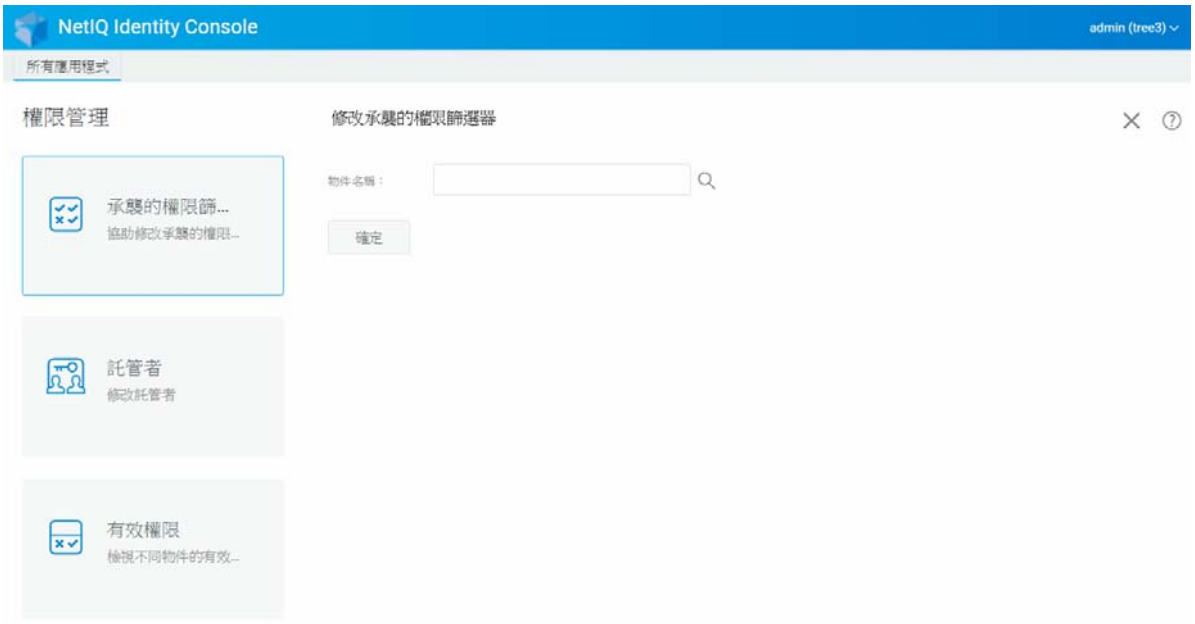
檢視有效權限

有效權限是明確和承襲權限的組合，物件在目錄樹中擁有任何點。檢視對另一個物件的物件有效權限：

1. 從 Identity Console 抵達頁面，按一下 **「權限」**管理選項
2. 選取 **「有效權限」**。
3. 指定或使用 「物件選擇器」 圖示來尋找您要檢視其權限的託管者名稱，然後按一下 **「確定」**。
4. 在 「物件名稱」欄位中，指定您要檢視託管者有效權限的物件名稱。

   eDirectory 會計算有效權限並在 **「有效權限」**欄位中顯示這些權限。

圖 8-3 檢視有效權限


NetIQ Identity Console
admin (tree3)
所有應用程式
權限管理
修改承襲的權限篩選器
物件名稱：
確定
承襲的權限篩...
協助修改承襲的權限...
託管者
修改託管者
有效權限
檢視不同物件的有效...

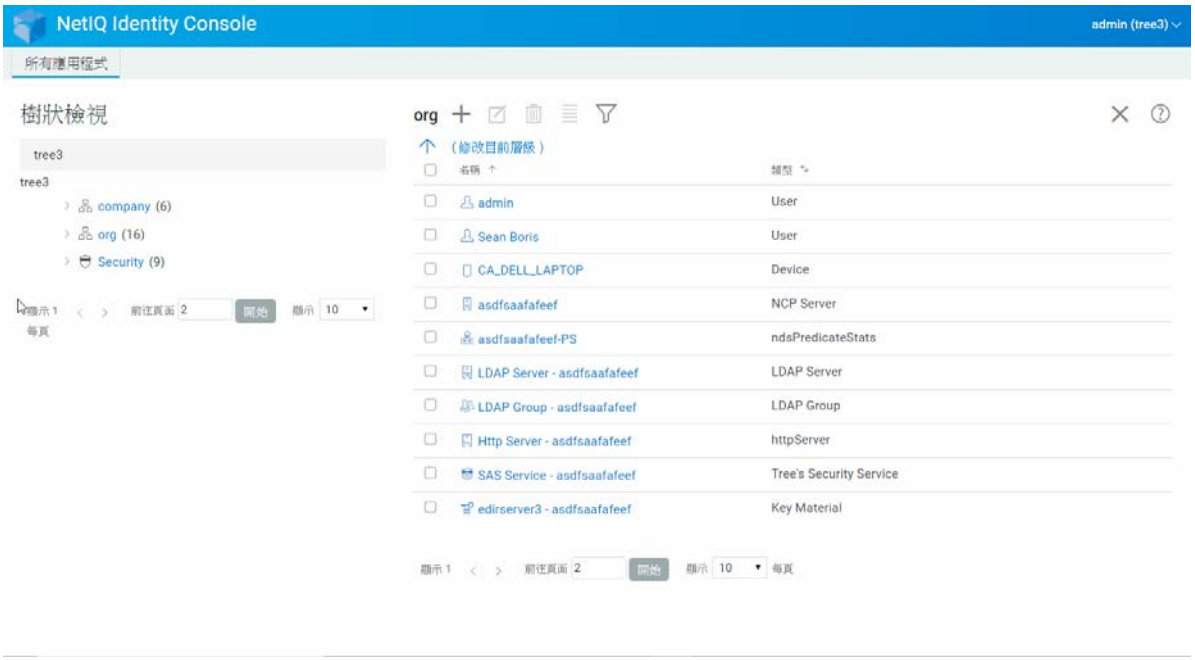
9 樹狀檢視

樹狀檢視可讓您瀏覽目錄樹狀，並建立、刪除或修改該樹狀中的各種物件。樹狀檢視具有導覽框架和內容框架。

網路樹檢視窗導覽框架

在樹狀檢視中，導覽框架會顯示目錄結構。瀏覽框架會顯示 「容器」，包括 「卷冊」 (檔案系統)、物件。導覽框架下顯示的所有選項是可點按的，以協助您瀏覽目錄結構。依預設，導覽框架會對每個容器顯示最多 10 個從屬物件，但您可以在樹狀檢視中的導覽框架面板中變更此設定。

圖 9-1 *網路樹中的導覽框架*



網路樹檢視窗內容框架

在 「導覽」框架中選取其中一個容器物件，會使 「內容」框架顯示該容器內的所有物件。「內容」框架是您實際檢視和修改目錄物件的地方。內容框架包含的標題具有數個可用動作：

標題列：「內容」框架的標題列顯示目前選取之容器物件的名稱。

物件清單標題：物件清單標題可供存取下列項目：

- 新增：按一下 ＋ 圖示可新增新的物件。

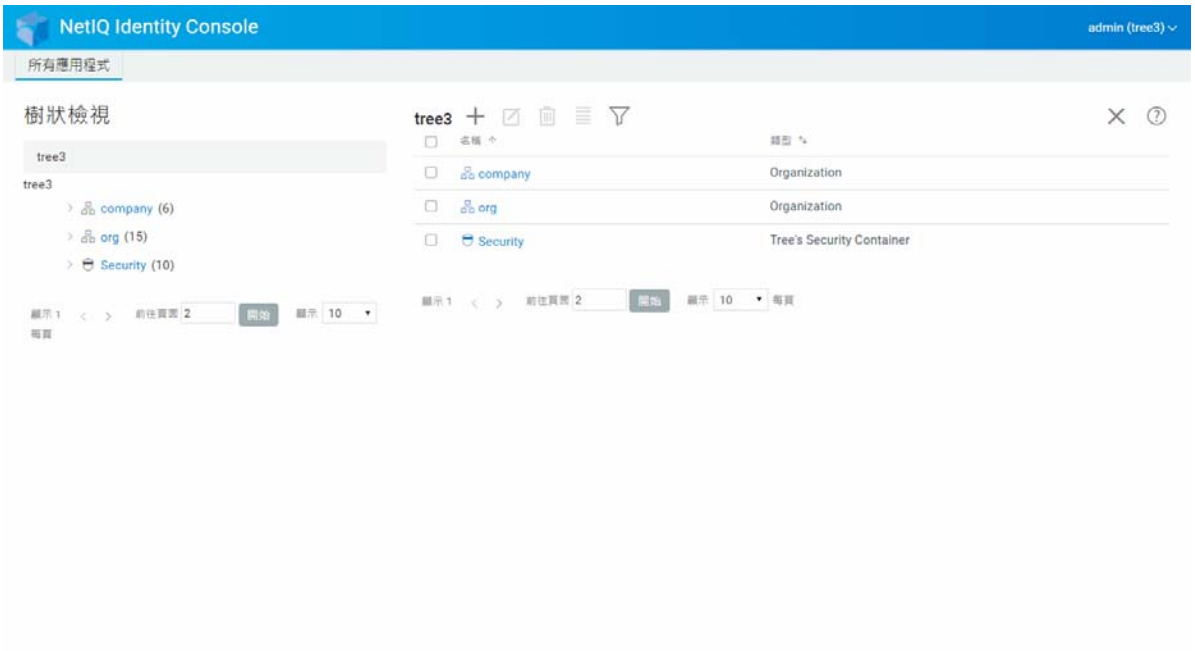
- **修改**：選取物件，並按一下  圖示來修改。這會開啟所選取物件的內容登記，使得您可以修改其屬性。不能一起修改多個物件。
- **刪除**：選取物件，並按一下  圖示來刪除選取的物件。可以一起刪除多個物件。不能刪除無葉物件。
- **動作**：選取物件並按一下  圖示，這會開啟所選取物件支援任務的下拉式功能表。若要執行任務，請從下拉式功能表中選取，並提供必要的資訊。
- **物件計數**：樹狀檢視會在頁面底端列出目前頁面中的物件數。依預設，內容框架會對每個容器顯示最多 20 個從屬物件，但您可以變更此設定。
- **全部選取**：標題中的核取方塊作用與物件目前頁面的「全選」核取方塊一樣。
- **排序**：**「名稱」**和**「類型」**欄皆可排序。按一下其中一個圖示可以在遞增和遞減字母順序之間切換物件排序。
- **搜尋篩選器**：按一下  。用來啟動篩選器快顯視窗的圖示。您可以使用此選項來建立篩選器，以限制顯示在物件清單中的物件。您可以視需要依物件類型和物件名稱來進行篩選。

  選取  選項以開啟「進階篩選器」對話方塊，讓您可使用幾乎任一個物件屬性來建立篩選器。如需詳細資訊，請參閱 「設定進階搜尋」(第 24 頁)。

若要對物件執行動作，請選取其核取方塊，然後從「物件清單」標題選取動作圖示  。選取 (目前層級) 物件以針對您目前所瀏覽的容器執行動作。下列動作可以使用此選項執行：

- 「修改承襲的權限篩選」(第 49 頁)
- 「修改託管者權限」(第 50 頁)
- 「延伸物件」(第 62 頁)
- 「重新命名物件」(第 46 頁)
- 設定密碼
- 「檢視有效權限」(第 51 頁)

圖 9-2 網路樹中的內容框架



10 管理綱要

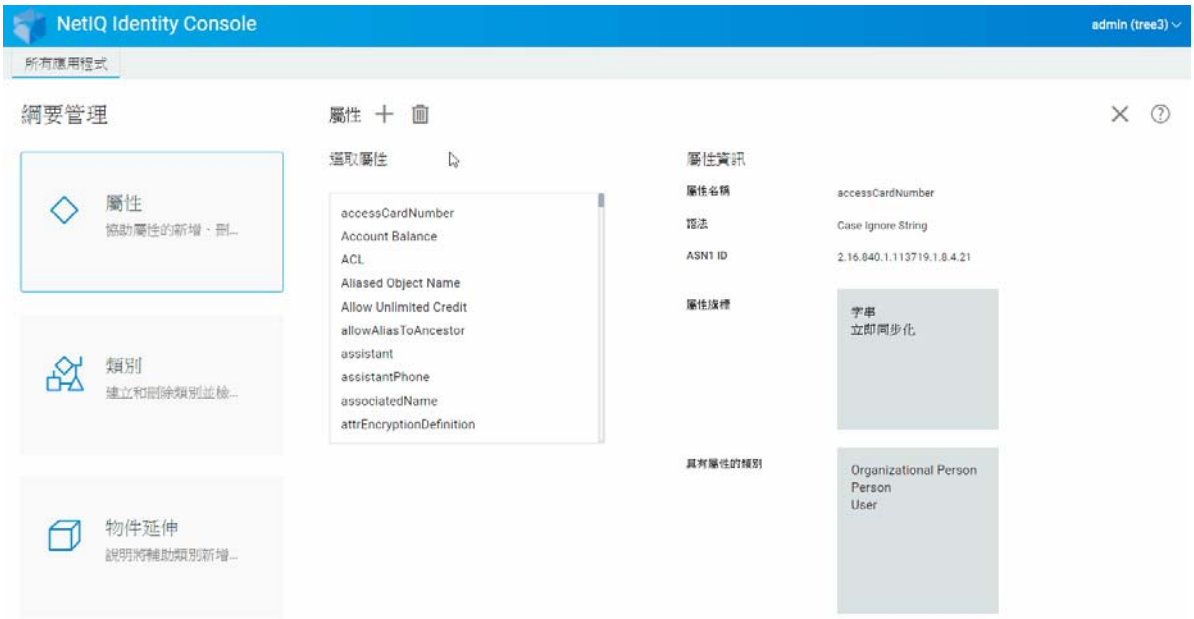
目錄綱要會定義可在您的樹狀中建立之物件的類型 (例如使用者、印表機、群組等)，以及建立物件時必要或選用的資訊。Identity Console 提供下列綱要相關的任務：

建立屬性

您可以定義自己的自訂屬性類型，然後將其新增為現有物件類別的選擇性屬性。但是，無法將強制屬性新增至現有類別。建立屬性：

1. 從 Identity Console 抵達頁面，按一下 **「物件管理」**選項。
2. 按一下 ＋ 圖示。
3. 在 「建立屬性」頁面中，輸入下列詳細資料：
   - 屬性名稱
   - ASN1 ID (選用)
   - 語法
   - 屬性旗標
4. 輸入所有需要的詳細資料後，按一下 建立 按鈕。
5. 隨即顯示確認訊息，指出已建立屬性。

圖 10-1 建立屬性



建立類別

您可以使用「綱要管理」選項來定義您自己的類別。然後使用在類別中定義的內容來延伸個別物件。建立類別：

1 從 Identity Console 抵達頁面，按一下「綱要管理」選項，並選取「類別」。

2 按一下 ＋ 圖示。

3 在「建立屬性」頁面中，輸入下列詳細資料：

- 類別名稱
- ASN1 ID (選用)
- 類別旗標：選取下列其中一個類別旗標：
  - **有效類別 :** 如果想建立有效類別，且此類別可用以建立物件，請設定這個旗標。
  - **無效類別 :** 用作一組屬性的佔位符。無效類別不能用於建立物件，但可以指定為能讓其他類別承襲其屬性的類別。例如，「個人」類別是無效類別，它具有「使用者」類別可承襲的屬性。
  - **輔助類別 :** 只能與個別物件而不是整個類別關聯的屬性集合。
  - **容器類別 :** 如果要建立為容器類別，請設定這個旗標。使用它建立物件時，所建立的物件成為容器物件 (如 OU)。請勿為葉物件類別設定這個旗標。

附註：如果選取「有效類別」和「無效類別」，則也必須指定「超級類別」的值。如果您選擇「輔助類別」，「超級類別」對您來說會是選用的。

4 輸入所有需要的詳細資料後，按一下「下一步」按鈕。

5 在下一個畫面中，選取選用、強制和命名屬性，並按一下「確定」。

6 隨即顯示確認訊息，指出已建立類別。

為類別指派屬性

當組織的資訊需求發生變更，或準備合併網路樹時，可以在現有的類別中新增選用的屬性。將屬性新增至現有的類別：

附註：只有在建立類別時才能定義強制屬性 強制性屬性是在建立物件時必須完成的屬性。

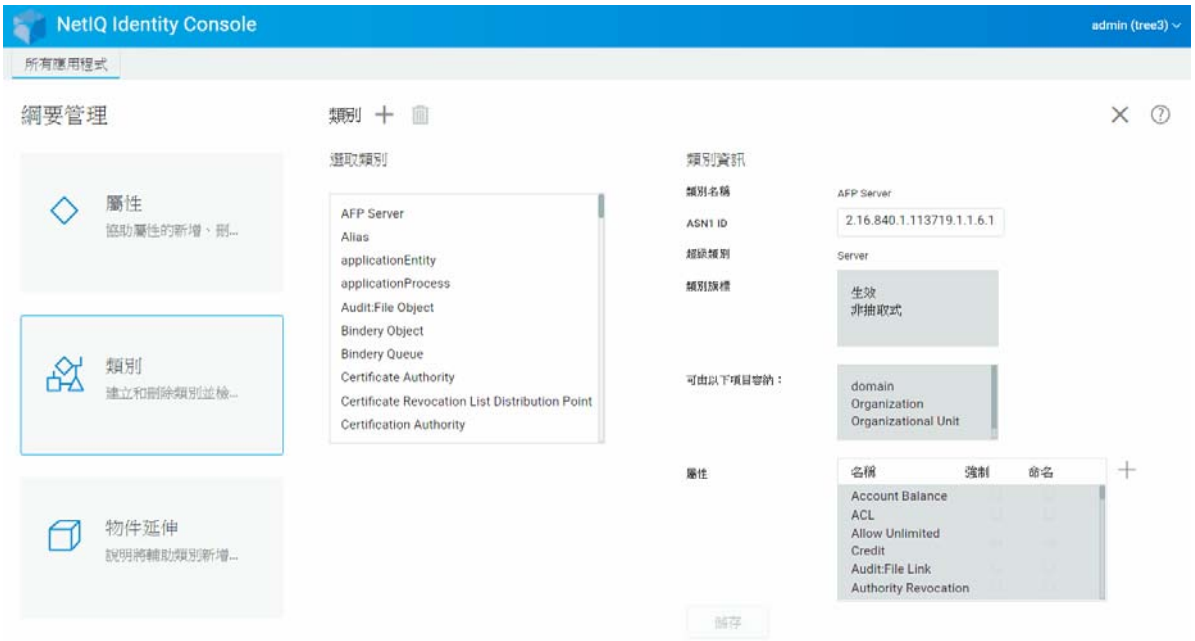
1 從 Identity Console 抵達頁面，按一下「綱要管理」選項，並選取「類別」。

2 按一下「選取類別」下列出的任何類別。

3 對應的類別資訊會顯示在畫面的右側。

4 按一下「屬性」選項旁的 ＋ 按鈕，選取您要新增的屬性，並按一下「新增」>「儲存」。

圖 10-2 為類別指派屬性



檢視屬性資訊

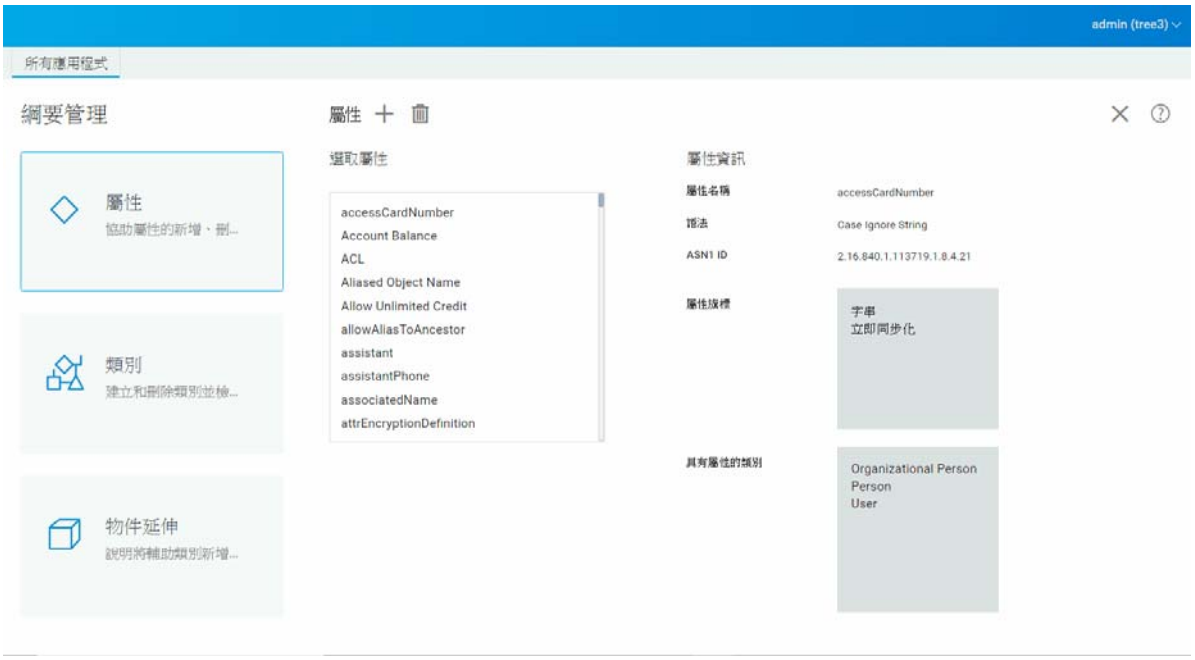
您可以檢視屬性的結構詳細資料，例如使用該屬性的語法、旗標和類別。檢視屬性的資訊：

1 從 Identity Console 抵達頁面，按一下「綱要管理」選項，並選取「屬性」。

2 按一下「選取屬性」下列出的任何屬性。

3 對應的屬性資訊會顯示在畫面的右側。

圖 10-3 檢視屬性資訊



刪除屬性

您可以刪除 eDirectory 網路樹中並非基礎綱要之一部份的未使用屬性。合併兩個目錄樹或當屬性隨時間經過而過時之後，這可能會很有用。如要刪除屬性：

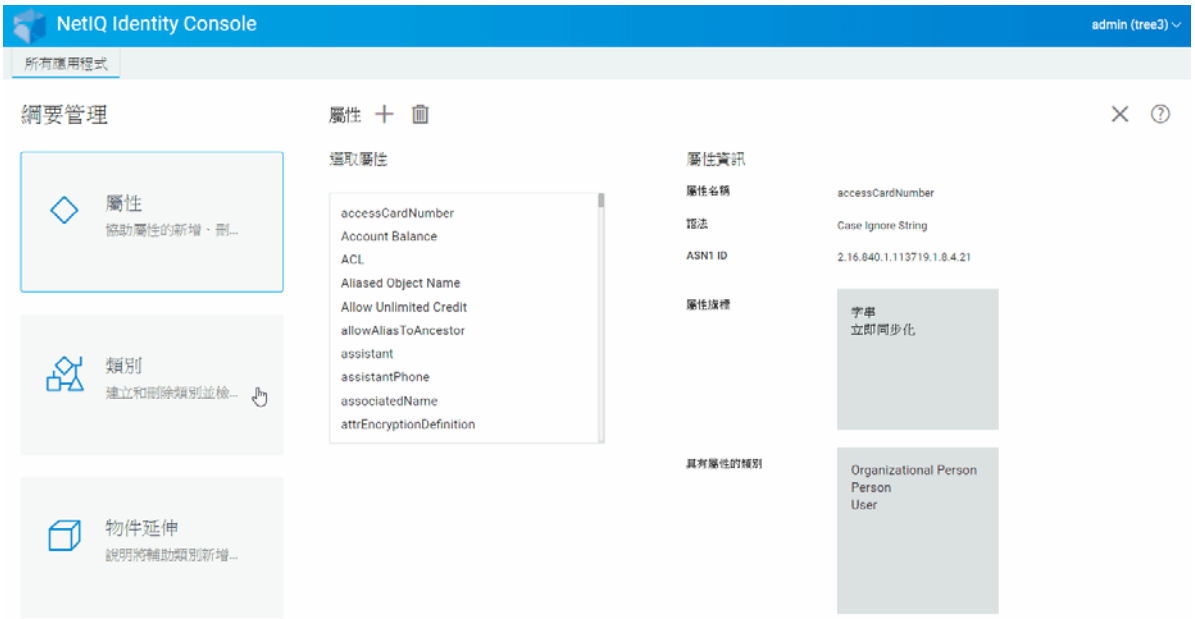
1 從 Identity Console 抵達頁面，按一下 **「綱要管理」**選項，並選取 **「屬性」**。

2 在 **「選取屬性」**清單下選取您要刪除的屬性，並按一下 圖示。

附註： 圖示只有在您選取可刪除的屬性時才會啟用。

3 按一下 **「確定」**以確認刪除。

圖 10-4 刪除屬性



刪除類別

您可以刪除 eDirectory 網路樹中並非基礎綱要之一部份的未使用類別。Identity Console 只能防止您刪除本地複製分割區中目前正在使用的類別。若要刪除類別：

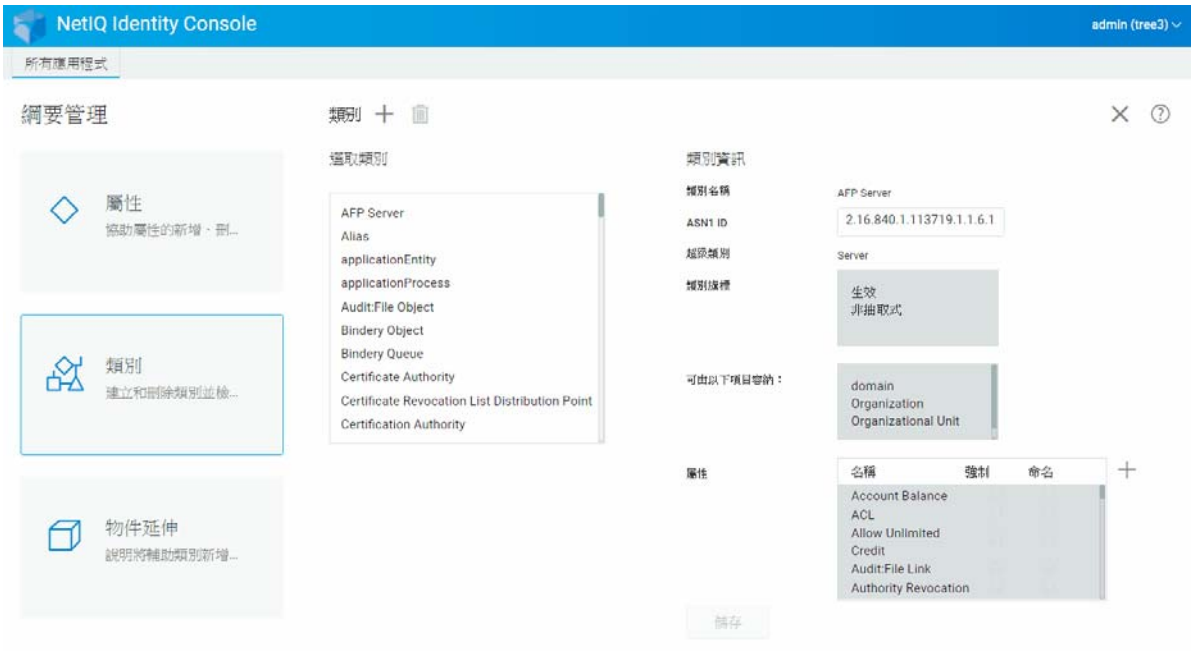
1 從 Identity Console 抵達頁面，按一下 **「綱要管理」**選項，並選取 **「類別」**。

2 在 **「選取類別」**清單下選取您要刪除的類別，並按一下 圖示。

附註： 圖示只有在您選取可刪除的類別時才會啟用。

3 按一下 **「確定」**以確認刪除。

圖 10-5 刪除類別



延伸物件

執行下列步驟來延伸物件：

1 從 Identity Console 抵達頁面，按一下 「綱要管理」選項，並選取 「物件延伸」。

2 指定物件名稱或使用物件選擇器來選取要延伸的物件，按一下 圖示。

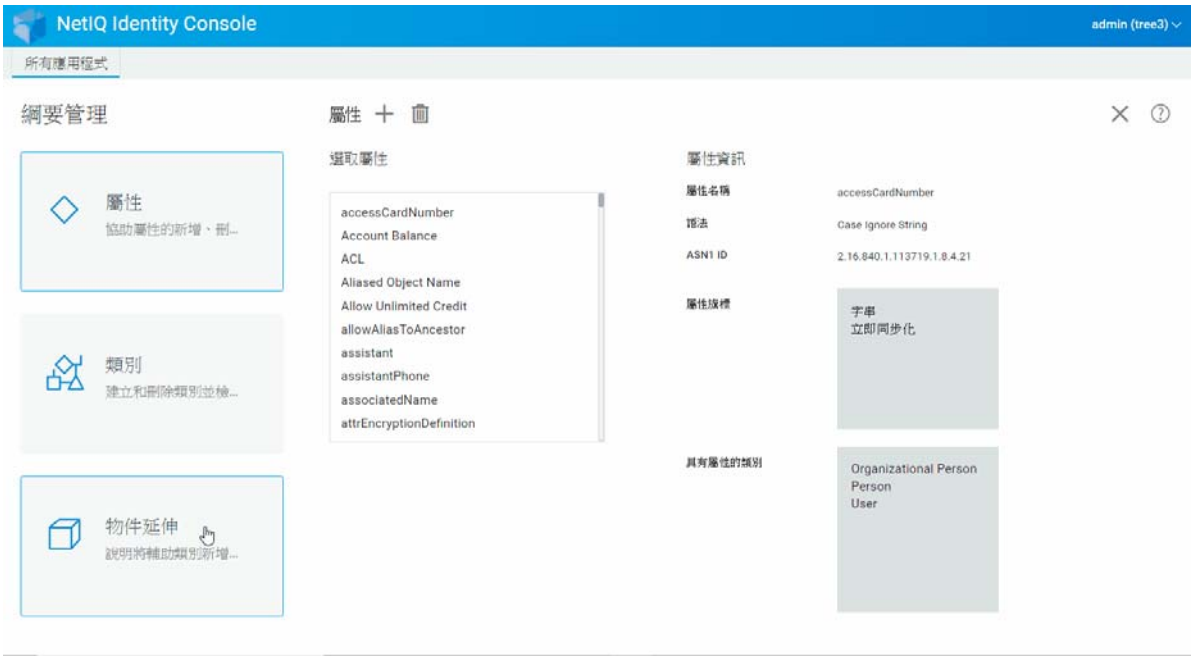
3 按一下 圖示並選取輔助類別，然後按一下 「確定」。

附註：如果對選取的輔助類別附加任何強制屬性，則會提示您在 「強制屬性」快顯視窗中輸入需要的值。

4 確認訊息隨即顯示，說明輔助類別已新增至物件。

5 若要從物件移除現有的輔助類別，請選取類別，並按一下 圖示。

圖 10-6 延伸物件


NetIQ Identity Console
admin (tree3)
所有應用程式
綱要管理
屬性
協助屬性的新增、刪...
類別
建立和刪除類別並檢...
物件延伸
說明將輔助類別新增...
屬性
選取屬性
accessCardNumber
Account Balance
ACL
Aliased Object Name
Allow Unlimited Credit
allowAliasToAncestor
assistant
assistantPhone
associatedName
attrEncryptionDefinition
屬性資訊
屬性名稱
accessCardNumber
語法
Case Ignore String
ASN1 ID
2.16.840.1.113719.1.8.4.21
屬性旗標
字串
立即同步化
具有屬性的類別
Organizational Person
Person
User

11 管理稽核事件

本章節說明如何使用 Identity Console 管理各種稽核事件。您可以使用此功能來為您的 NCP 伺服器啟用或停用稽核事件。

設定 CEF 稽核事件

1. 使用您的使用者名稱和密碼登入 Identity Console。
2. 選取 **「稽核」**。
3. 選取您要監控的 NCP 伺服器，然後按一下 **「確定」**。

   附註：第一次為任何 NCP 伺服器啟用 CEF 事件之後，預設會選取一些事件。

4. 設定 CEF 稽核事件：
   - **事件組態：**根據您的環境需要的稽核來啟用或停用下列事件：

附註：預設會收合事件組態區段下的個別事件類別。您可以展開每個類別以選取個別事件。

選項	描述
安全性事件	選取想要記錄事件的安全性事件。您可以記錄事件以便新增或刪除成員、偵測侵入者、變更密碼，以及驗證使用者等等。
物件事件	選取想要記錄事件的物件事件。您可以記錄事件以便建立刪除、重新命名、移動和搜尋物件。
屬性事件	選取想要記錄事件的屬性事件。您可以記錄事件以便讀取和刪除屬性，以及新增、刪除和比較屬性值。
LDAP 事件	選取想要記錄事件的 LDAP 事件。

- **Advanced Settings (進階設定)：**使用進階設定，您可以執行下列動作。
  - **全域 :** 您可以選取或清除重複項目的全域設定。
    - **不要傳送複製事件 :** 選取此選項可以停止接收因為從其他伺服器複製，所導致的重複事件。
  - **記錄事件值：**事件都已記錄在文字檔中。事件值大小超過 768 位元組，即會視為「大值」。您可記錄任何大小的事件。
    - **記錄大值 :** 選取此選項，以記錄大小超過 768 位元組的事件。
    - **記錄屬性值：**選取此選項會顯示屬性值。僅適用於 **「新增值」**和 **「刪除值」**事件。
    - **記錄加密屬性值 :** 選取此選項會顯示加密屬性值。僅適用於 **「新增值」**和 **「刪除值」**事件。

    附註：如果事件大小大於 768 個位元組，則會截斷事件值並儲存至記錄檔案。

了解 CEF 事件類型

您可以設定 CEF 以記錄下列類別中的事件：

- 安全性
- 物件
- 屬性
- LDAP

您可以稽核事件類型的下列預設集：

類別	事件類型
安全性	◆ 已變更 ACL ◆ 新增成員 ◆ 刪除成員 ◆ 偵測到侵入者 ◆ 已停用登入 ◆ 已啟用登入 ◆ 登入 ◆ 變更安全性等於 ◆ 稽核組態 ◆ 變更密碼 ◆ 帳戶解除鎖定 ◆ 登出 ◆ 連接 ◆ 模擬 ◆ 驗證 ◆ 驗證密碼 ◆ 變更登入組態 ◆ 查詢身分證明
物件	◆ 建立物件 ◆ 刪除物件 ◆ 重新命名物件 ◆ 移動物件 ◆ DSA 讀取 ◆ 搜尋
屬性	◆ 讀取屬性 ◆ 刪除屬性 ◆ 新增值 ◆ 刪除值 ◆ 比較屬性值

類別	事件類型
LDAP	• LDAP 結合 • LDAP 結合回應 • LDAP 取消結合 • LDAP 連接 • LDAP 搜尋 • LDAP 搜尋回應 • LDAP 搜尋項目回應 • LDAP 新增 • LDAP 新增回應 • LDAP 比較 • LDAP 比較回應 • LDAP 修改 • LDAP 修改回應 • LDAP 刪除 • LDAP 刪除回應 • LDAP 修改 DN • LDAP 修改 DN 回應 • LDAP 放棄 • LDAP 延伸作業 • LDAP 系統延伸作業 • LDAP 延伸作業回應 • 修改 LDAP 伺服器組態 • 未知的 LDAP 操作 • LDAP 密碼修改

設定 CEF 稽核篩選

使用篩選器和事件通知，CEF 可在特定事件類型發生時，或當事件不發生時加以報告。取決於事件類型而定，您也可以篩選一或多個特定物件類別或屬性的事件。CEF 會對 eDirectory 伺服器上設定的篩選器評估所有產生的事件，並僅記錄符合這些篩選器的事件。

本節提供設定系統篩選和通知所需的資訊。

- 「使用排除篩選器篩選 eDirectory 事件」(第 69 頁)
- 「篩選 CEF 物件事件」(第 69 頁)
- 「篩選 CEF 屬性事件」(第 70 頁)

使用排除篩選器篩選 eDirectory 事件

按一下 **「排除篩選器」**連結來針對您不要產生事件的這些物件類別和屬性設定篩選。您可以選取物件類別和屬性。

若要設定不需要的 eDirectory 事件的篩選：

1. 在 Identity Console 中，從首頁選取 **「稽核」**。
2. 選取您要監控的 NCP 伺服器，然後按一下 **「確定」**。
3. 現在前往 **「進階設定」**，並按一下 **「篩選器」**下的 **「排除篩選器」**。

   「CEF 排除篩選」視窗隨即顯示。
4. 在 **「可用的物件類別」**清單中，選取您不要收集事件的物件類別，然後按一下向右箭頭來移動至 **「選取的物件類別」**清單。
5. 在 **「可用的屬性」**清單中，選取任何數量的屬性。選取屬性並按一下向右箭號，將屬性新增至選取的屬性清單中。
6. 按一下 **「確定」**。

CEF 稽核模組會使用設定的篩選器，來停止對所有選取的物件類別和屬性產生事件。

篩選 CEF 物件事件

您可以設定物件的篩選，以僅尋找特定的一或多個事件。例如，如果想要在某人於 eDirectory 中建立使用者帳戶時收到通知，您可以建立篩選器，選取要針對建立新使用者物件記錄事件的使用者物件類別。

若要設定帳戶篩選，請按一下「物件事件」連結，選取類別，然後按一下 **「確定」**來結束應用程式。

若要設定帳戶管理事件的篩選：

1. 在 Identity Console 中，從首頁選取 **「稽核」**。
2. 選取您要監控的 NCP 伺服器，然後按一下 **「確定」**。
3. 現在前往 **「進階設定」**，並按一下 **「篩選器」**下的 **「物件事件」**。

   「CEF 物件篩選」視窗隨即顯示。
4. 在 **「可用的物件類別」**清單中，選取任何物件類別，然後按一下向右箭頭來將物件類別移動至 **「選取的物件類別」**清單，然後按一下 **「確定」**。

CEF 稽核模組會使用設定的篩選，來檢查選取的物件類別的所有產生事件，並記錄這些事件。

篩選 CEF 屬性事件

按一下 **「屬性事件」**連結來設定屬性事件的篩選。例如，如果想要在某人於 eDirectory 中新增屬性值時收到通知，您可以建立篩選器來針對新增新的值記錄事件。

若要設定屬性事件的篩選：

1. 在 Identity Console 中，從首頁選取 **「稽核」**。
2. 選取您要監控的 NCP 伺服器，然後按一下 **「確定」**。
3. 現在前往 **「進階設定」**，並按一下 **「篩選器」**下的 **「屬性事件」**。

   顯示**屬性設定篩選**視窗。
4. 在 **「可用的物件類別」**清單中，選取您想要收集事件的物件類別，然後按一下向右箭頭來移動至 **「選取的物件類別」**清單。
5. 在 **「可用的屬性」**清單中，針對選取的物件類別選取任何數量的屬性。選取屬性並按一下向右箭號，將屬性新增至選取的屬性清單中。

   附註：如果您選取某個物件類別，則會選取該物件類別上所有屬性的所有屬性事件。在此情況下，您會取得選取的物件類別上所有屬性的屬性事件。
6. 按一下 **「確定」**。

使用設定的篩選，CEF 稽核模組會檢查所有選取物件類別和屬性的產生事件，並記錄這些事件。

12 管理加密屬性

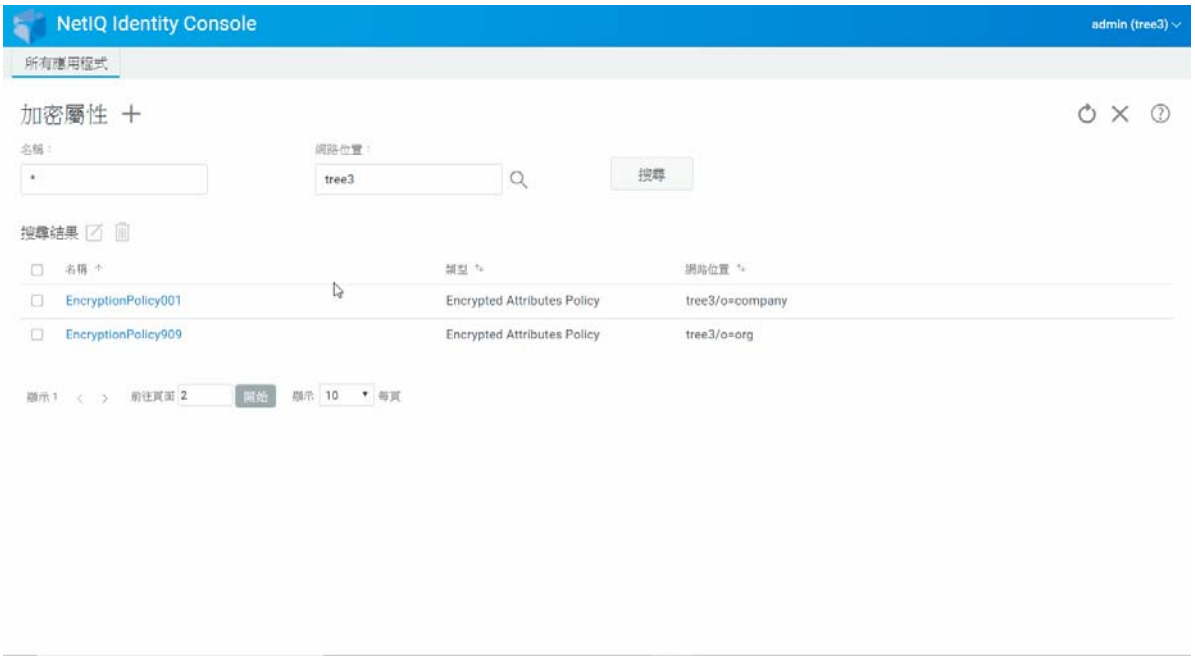
Identity Console 可以從您的 eDirectory 伺服器安全地讀取加密屬性。您可以使用 Identity Console 來建立、修改或刪除這些加密屬性的數個規則。

建立加密屬性的規則

若要建立新的屬性規則：

1. 從 Identity Console 抵達頁面，按一下「加密屬性」選項。
2. 按一下 ＋ 圖示。
3. 在「建立加密屬性規則」頁面中，輸入下列詳細資料：
   - 指定規則名稱
   - 輸入或選取網路位置
   - 選取 NCP 伺服器
   - 選取屬性
4. 指定所有需要的詳細資料之後，按一下「完成」。
5. 隨即顯示確認訊息，指出已建立規則。

圖 12-1 建立加密屬性規則

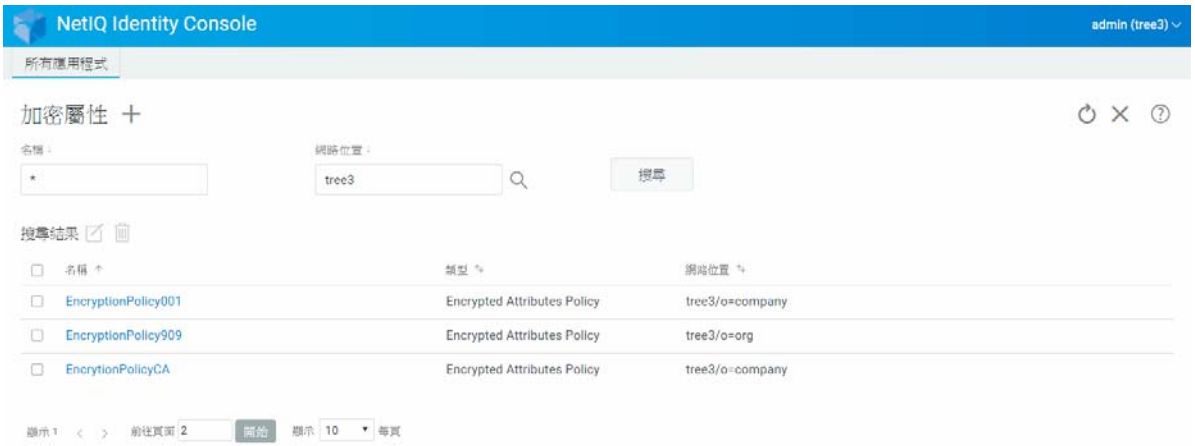


刪除加密屬性規則

若要刪除加密屬性規則：

1. 從 Identity Console 抵達頁面，按一下「加密屬性」選項。
2. 指定屬性的名稱和網路位置，或使用搜尋功能進行搜尋，然後按一下 搜尋 按鈕。
3. 從清單選取屬性，並按一下 圖示。
4. 隨即顯示確認訊息，指出已刪除規則。

圖 12-2 刪除加密屬性規則

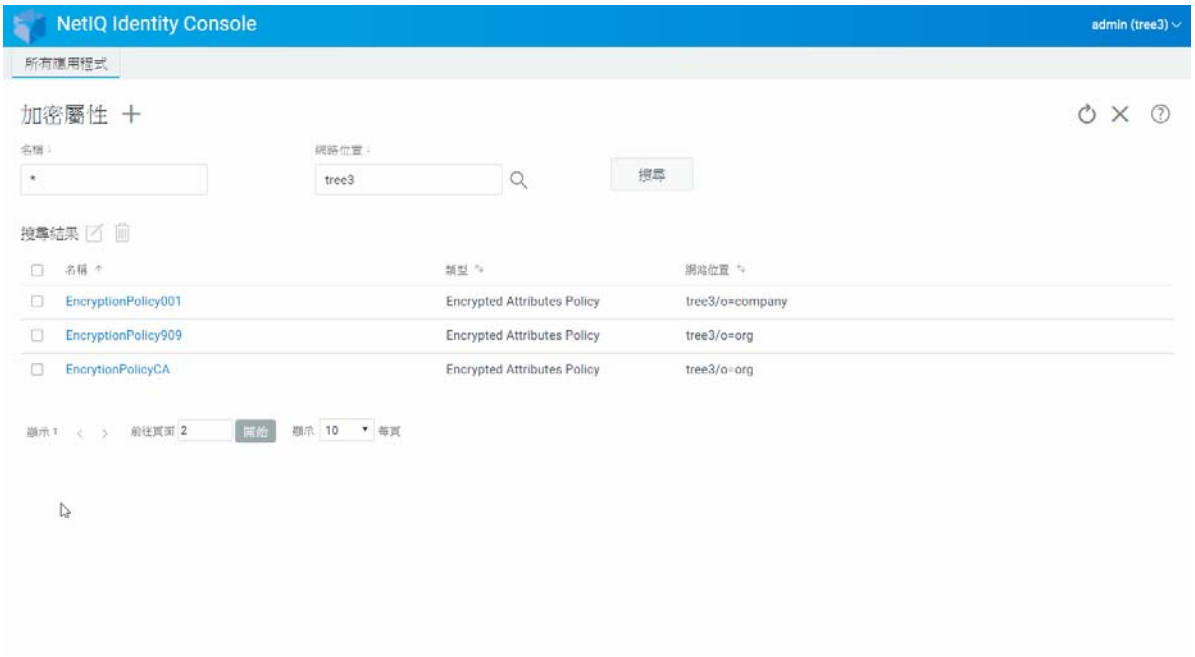


修改加密屬性規則

若要修改加密屬性規則：

1. 從 Identity Console 抵達頁面，按一下「加密屬性」選項。
2. 輸入物件的名稱和網路位置，然後按一下 搜尋 按鈕。
3. 從物件清單選取屬性，並按一下 圖示。
4. 進行想要的變更，然後按一下 儲存 按鈕。
5. 隨即顯示確認訊息，指出已修改規則。

圖 12-3 修改加密屬性規則



13 管理加密複製

若要啟用加密複製，您必須為加密複製設定分割區。組態設定會儲存在分割區根物件中。您僅能在分割區層級選擇啟用加密複製。在分割區層級啟用加密複製時，託管分割區的所有複本之間的複製都會加密。例如，假設分割區 P1 有複本 R1、R2、R3 和 R4。您可以在所有複本之間加密複製。

- 「為分割區啟用加密複製」(第 75 頁)

為分割區啟用加密複製

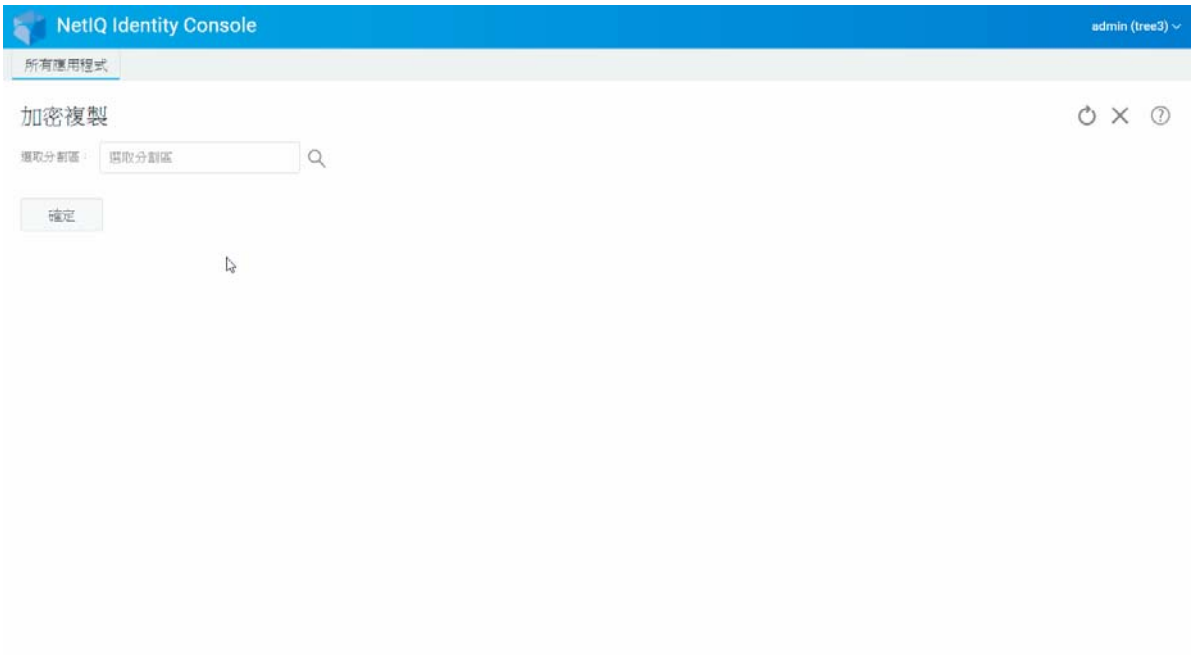
若要為分割區啟用加密複製：

附註：若要為加密複製啟用分割區，主控分割區的所有伺服器必須為 eDirectory 9.2 或更新版本伺服器。

---

1. 從 Identity Console 抵達頁面，按一下 **「加密複製」**選項。
2. 指定或瀏覽您要啟用加密複製的分割區。
3. 確保選取 **「啟用加密複製」**選項。停用分割區的加密複製時，請取消選取此選項。
4. 按一下**完成**。
5. 隨即顯示確認訊息，指出已啟用加密複製。

圖 13-1 *為分割區啟用加密複製*



14 管理分割區與複製本

分割區和複製本作業可讓您管理整個目錄伺服器中的 eDirectory 實體設計和配送。

分割區建立 eDirectory 網路樹的邏輯區塊。例如，如果您選擇 「組織單位」並將其建立為新分割區，您可以將 「組織單位」與所有次物件從其父分割區中分離。您選擇的 「組織單位」將成為新分割區的根部。新分割區的複製本位於父分割區之複製本所在的伺服器上，而新分割區中的物件則屬於新分割區的根部物件。

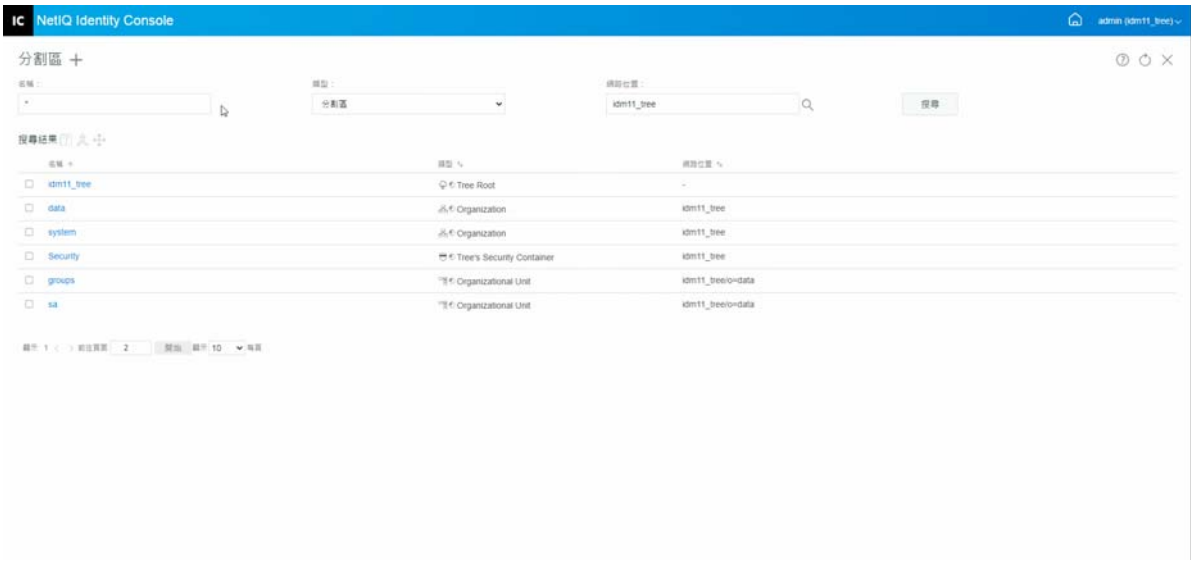
可以使用分割區模組執行以下任務：

建立分割區

若要建立新的分割區：

1. 從 Identity Console 抵達頁面，按一下 「**分割區管理**」選項。
2. 按一下 ＋ 圖示。
3. 在 「建立分割區」頁面中，指定要用作新分割區根部的容器，或使用 「物件選擇器」  圖示來搜尋，然後按一下 「**建立**」。
4. 隨即顯示確認訊息，指出已建立分割區。

圖 14-1 建立新分割區



合併分割區

若要將分割區與其父分割區合併：

1 從 Identity Console 抵達頁面，按一下「**分割區管理**」選項。

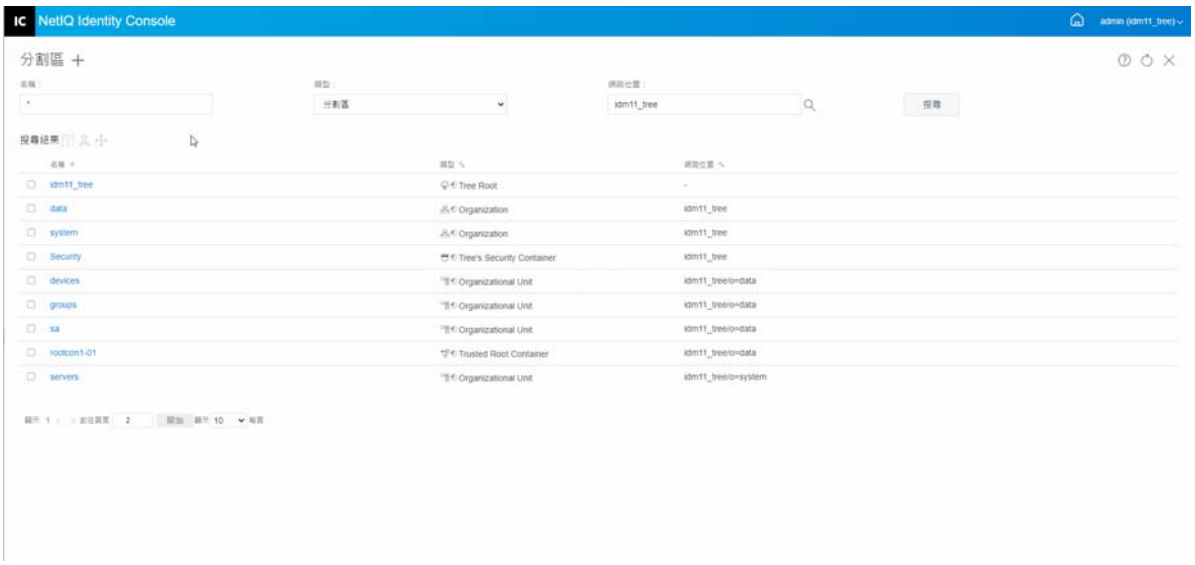
2 指定分割區的名稱、類型和網路位置，或使用搜尋功能進行尋找，然後按一下

按鈕。

3 從搜尋清單中選擇分割區，依次按一下 圖示然後按一下「**確定**」。

4 隨即顯示確認訊息，指出已合併分割區。

圖 14-2 合併分割區



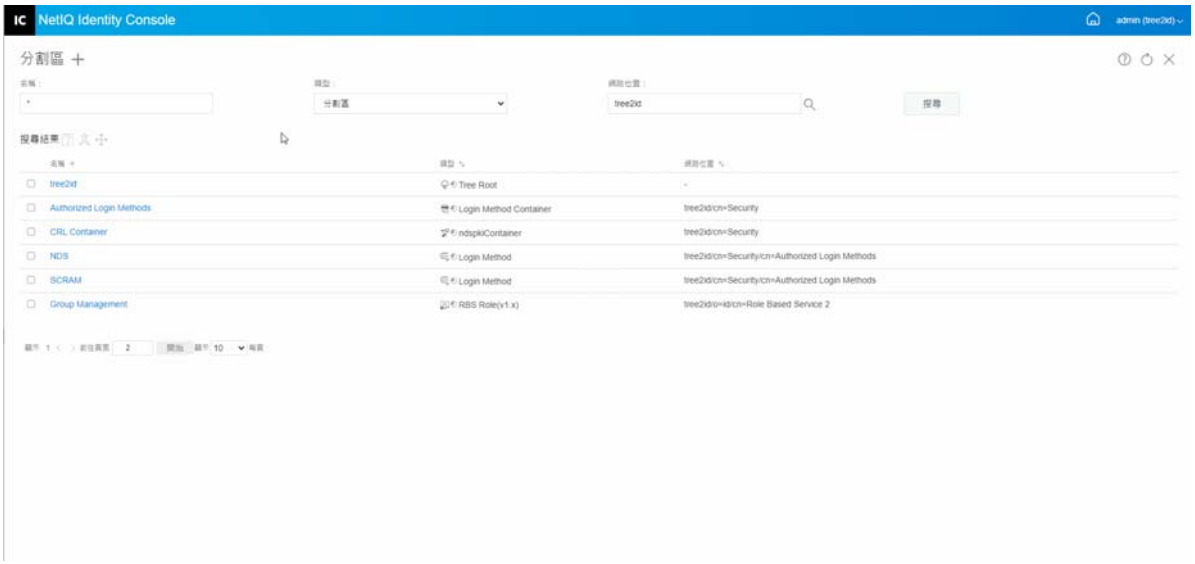
修改分割區

若要修改分割區：

1. 從 Identity Console 抵達頁面，按一下「**分割區管理**」選項。
2. 輸入分割區的名稱、類型和網路位置，然後按一下 搜尋 按鈕。
3. 從搜尋清單選取分割區，然後按一下 圖示。
4. 按一下「**篩選**」底下的「**編輯**」選項，以變更「複本」篩選器以及其對應的「類別」和「屬性」，然後按一下「**確定**」。

   如果您在「**類型**」欄位中選取「**伺服器**」，您會看到所有伺服器的清單。按一下每個伺服器將會顯示伺服器中所有分割區的清單。
5. 隨即顯示確認訊息，指出已修改分割區。

圖 14-3 *修改分割區*



移動分割區

移動分割區可讓您在目錄樹中移動子網路樹。這也就是所謂的剪除和接合作業。您僅可以移動未包含附屬分割區的分割區。如果附屬分割區已存在，您必須先合併那些分割區，然後才可以執行移動作業。

移動分割區時，edirectory 會變更分割區根部物件的所有參考。雖然物件的公用名稱仍未改變，但容器 (及所有附屬物件) 的完整名稱會改變。

附註：移動分割區時，必須遵照 eDirectory 包含規則。例如，不可以移動目錄樹的根部所直屬的「組織單位」，因為根部的包含規則允許「地域性」、「國家」或「組織」物件，但不允許「組織單位」物件。

若要移動分割區：

1 從 Identity Console 抵達頁面，按一下「**分割區管理**」選項。

2 輸入分割區的名稱、類型和網路位置，然後按一下 搜尋 按鈕。

3 從搜尋清單選取分割區，然後按一下 ✣ 圖示。

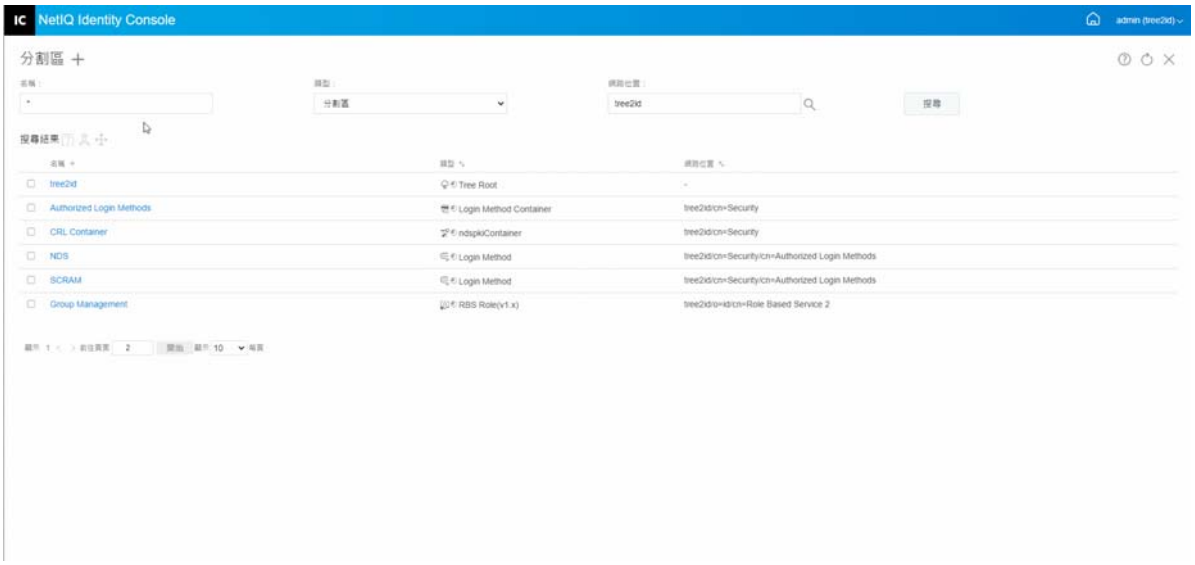
4 選擇要將目的地容器物件移至其中的指定分割區，然後按一下「**確定**」。

附註：「**在移動分割區的位置建立別名**」會建立分割區新位置的指標。這可讓您繼續進行原來位置的作業，直到您可以更新那些作業以反應新的位置為止。使用者可以繼續登入到網路，並找到原始目錄位置中的物件。

---

5 將顯示代表移動分割區作業已成功完成的確認訊息。

圖 14-4 *移動分割區*



15 管理索引

「索引管理員」是讓您管理資料庫索引的伺服器物件屬性。eDirectory 會使用這些索引，此可大幅改善查詢的效能。

NetIQ eDirectory 隨附於一組可提供基本查詢功能的索引。這些預設索引用於以下屬性。

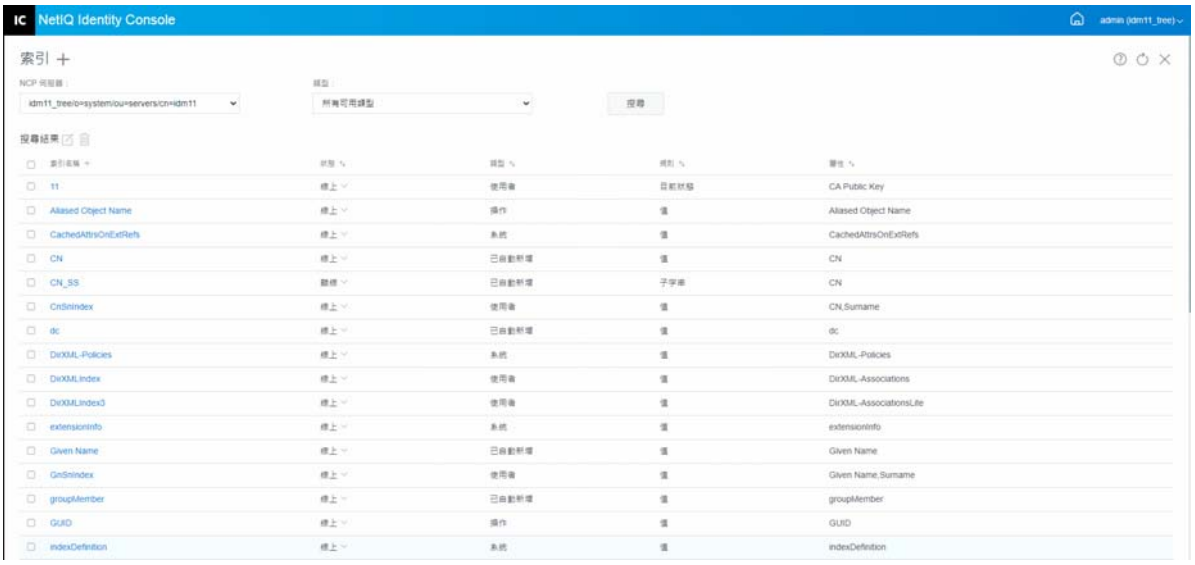
可以使用索引模組執行以下任務：

建立索引

若要建立新的索引：

1. 從 Identity Console 抵達頁面，按一下「**索引管理**」選項。
2. 按一下 ＋ 圖示。
3. 輸入索引名稱。
4. 從可用的 NCP 伺服器清單中選取伺服器。
5. 選取所需的屬性。
6. 選取索引規則：
   - 6a **子字串：**此與屬性值字串中的某個子集相符。例如，尋找所有具有「der」之 LastName 的查詢會傳回 Derington、Anderson 和 Lauder 的相符項目。建立和維護子字串索引是最耗費資源的索引。
   - 6b **目前狀態：**僅需要屬性的目前狀態，而不需要特定屬性值。尋找所有具有「登入程序檔」屬性之項目的查詢會使用目前狀態索引。
   - 6c **值：** 與整個值或屬性值的第一個部分相符。例如，值相符可用於尋找 LastName 等於「Jensen」的項目，以及 LastName 開頭為「Jen」的項目。
7. 按一下 建立 按鈕。
8. 隨即顯示確認訊息，指出已建立索引。

圖 15-1 建立新索引



刪除索引

若要刪除索引：

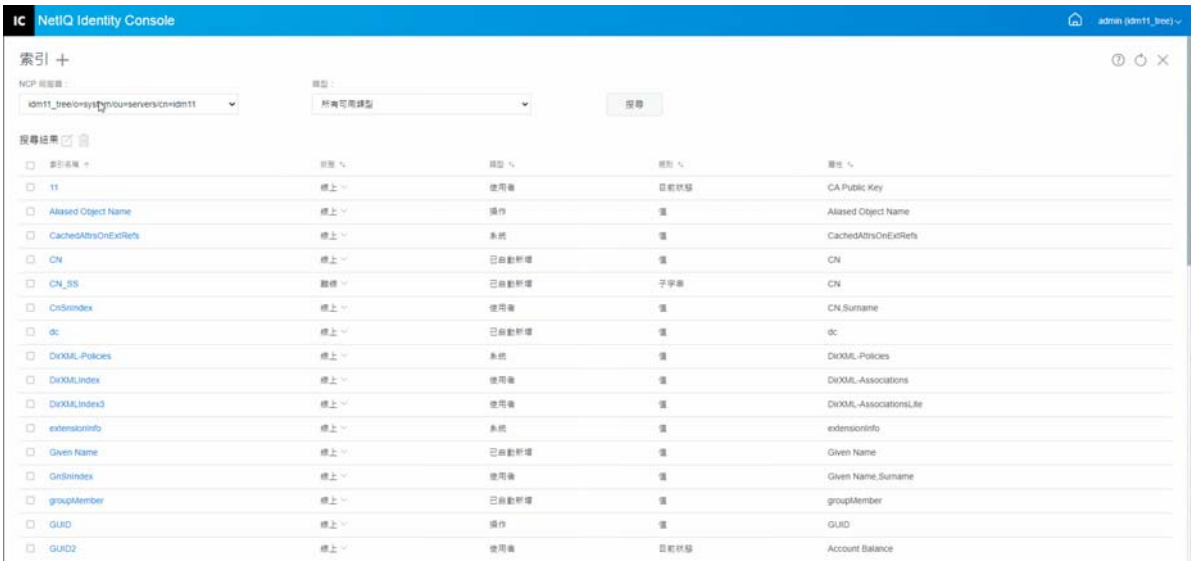
1 從 Identity Console 抵達頁面，按一下「索引管理」選項。

2 選取 NCP 伺服器和索引的類型，然後按一下 搜尋 按鈕。

3 從搜尋清單選取索引，然後按一下 圖示。

4 隨即顯示確認訊息，指出已刪除索引。

圖 15-2 刪除索引



複製索引

如果您發現特定索引在一部伺服器上很有用，並且在另一部伺服器上看到此索引的必要性，則可以將索引定義從一部伺服器複製到另一部伺服器。在檢閱述詞資料時，您可能還會發現相反的情況：滿足多部伺服器需求的索引在其中一部伺服器上不再有用。在這種情況下，您可以在未從索引獲益的單一伺服器中刪除索引。

若要複製索引：

1 從 Identity Console 抵達頁面，按一下「索引管理」選項。

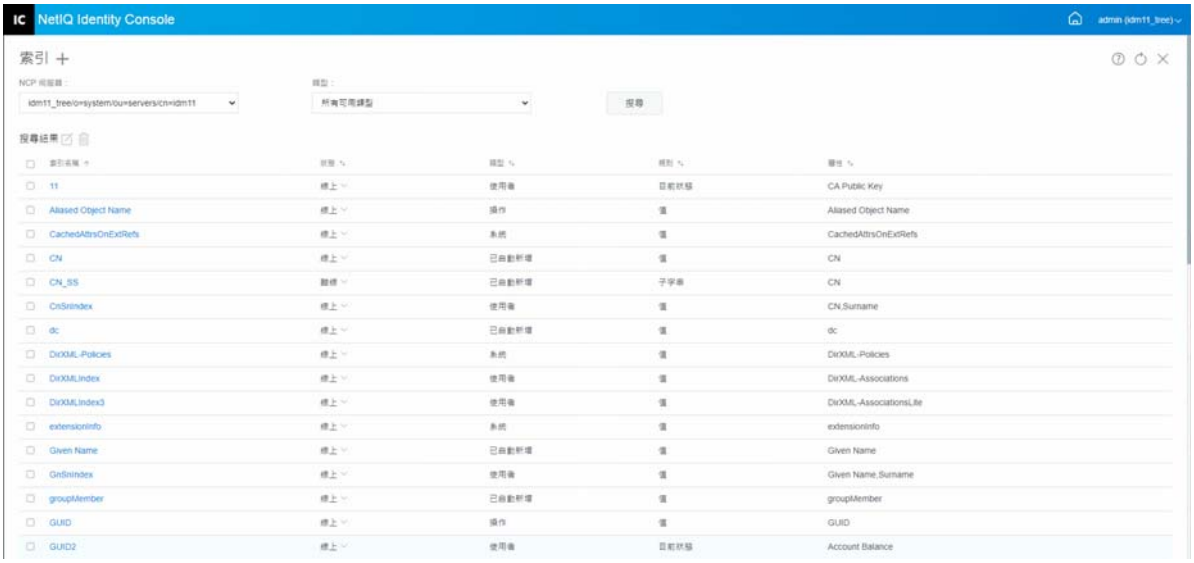
2 選取 NCP 伺服器和索引的類型，然後按一下 搜尋 按鈕。

3 從搜尋清單選取索引，然後按一下 圖示。

4 選取您要將索引複製到其中的所需 NCP 伺服器，然後按一下 儲存 按鈕。

5 隨即顯示確認訊息，指出已修改索引。

圖 15-3 複製索引



變更索引狀態

在尖峰時段，您可能需要藉由暫時讓索引離線來調整效能。例如，若要實現額外的大量載入速度，您可能需要暫停所有使用者定義的索引。因為每個物件的增加或修改都需要更新定義的索引，所以讓所有索引都處於作用中狀態可能會減慢資料的大量載入速度。大量載入完成之後，可以讓索引重新成為線上狀態。

若要讓索引離線：

1 從 Identity Console 抵達頁面，按一下「索引管理」選項。

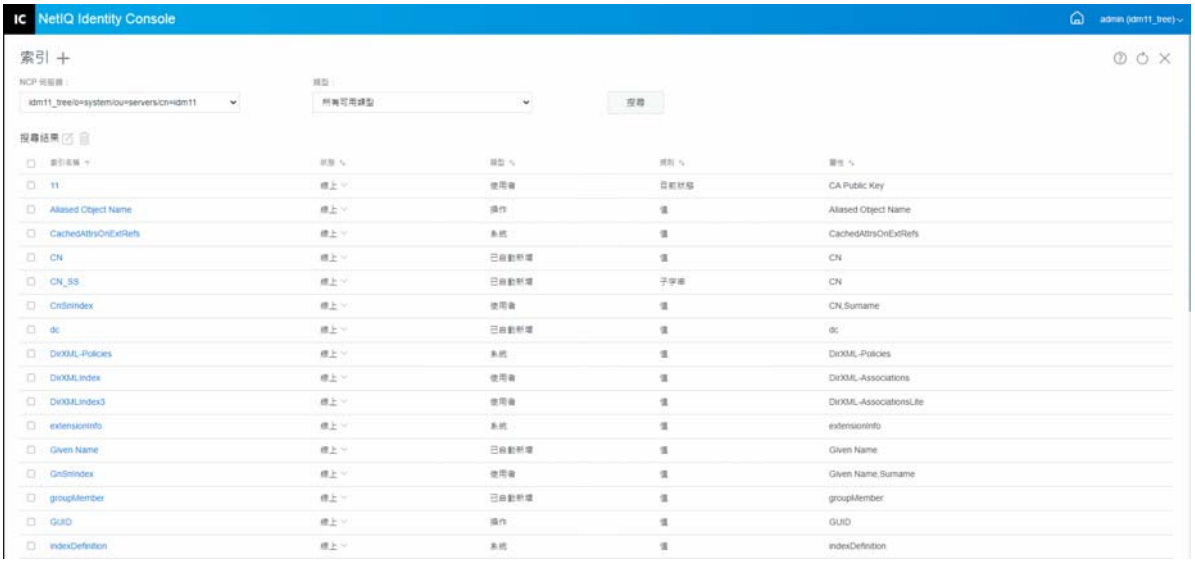
2 選取 NCP 伺服器和索引的類型，然後按一下 搜尋 按鈕。

3 按一下索引清單的「狀態」下拉式清單。索引可以具有以下狀態：

- **線上：**正在執行中
- **離線：**暫停。索引可以重新啟動。

附註：系統和作業類型索引的狀態無法變更。此類索引也不能刪除。

圖 15-4 讓索引離線



16 設定 LDAP 物件

eDirectory 安裝會建立 LDAP 伺服器物件和 LDAP 群組物件。LDAP 服務的預設組態位於這兩個物件的目錄中。您可以使用 Identity Console 中的 LDAP 管理任務來修改預設組態。

LDAP 伺服器物件表示伺服器特定的組態資料。但是，LDAP 群組物件包含可在多個 LDAP 伺服器之間方便共用的組態資訊。此物件提供常用組態資料，並代表一組 LDAP 伺服器。伺服器具有常用資料。

您可以將多個 LDAP 伺服器物件與一個 LDAP 群組物件產生關聯。然後，所有相關聯的 LDAP 伺服器都會從其 LDAP 伺服器物件取得其伺服器特定組態，但是從 LDAP 群組物件取得常用或共用資訊。

可以使用 LDAP 模組執行以下任務：

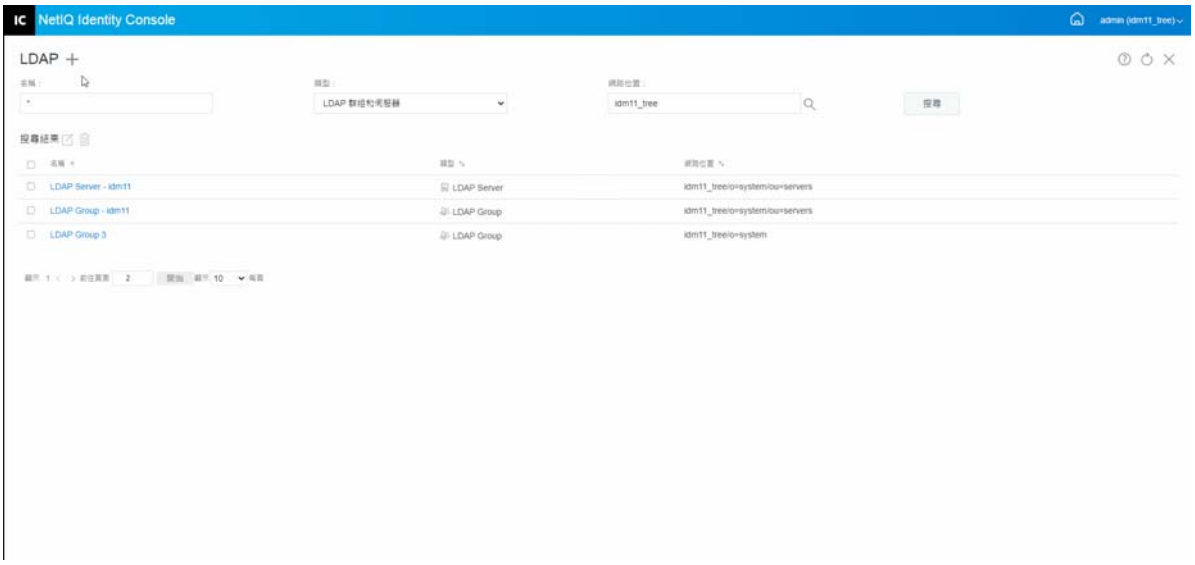
- 「建立 LDAP 物件」(第 85 頁)
- 「刪除 LDAP 物件」(第 86 頁)
- 「修改 LDAP 物件」(第 87 頁)

建立 LDAP 物件

若要建立新的 LDAP 物件：

1. 從 Identity Console 抵達頁面，按一下 **「LDAP 組態」**選項。
2. 按一下 ＋ 圖示。
3. 在 「建立 LDAP 物件」頁面中，指定名稱、類型和網路位置，或使用搜尋網路位置 圖示來尋找，然後按一下 **「建立」**。
4. 隨即顯示確認訊息，指出已建立 LDAP 物件。

圖 16-1 建立新的 LDAP 物件



刪除 LDAP 物件

若要刪除 LDAP 物件：

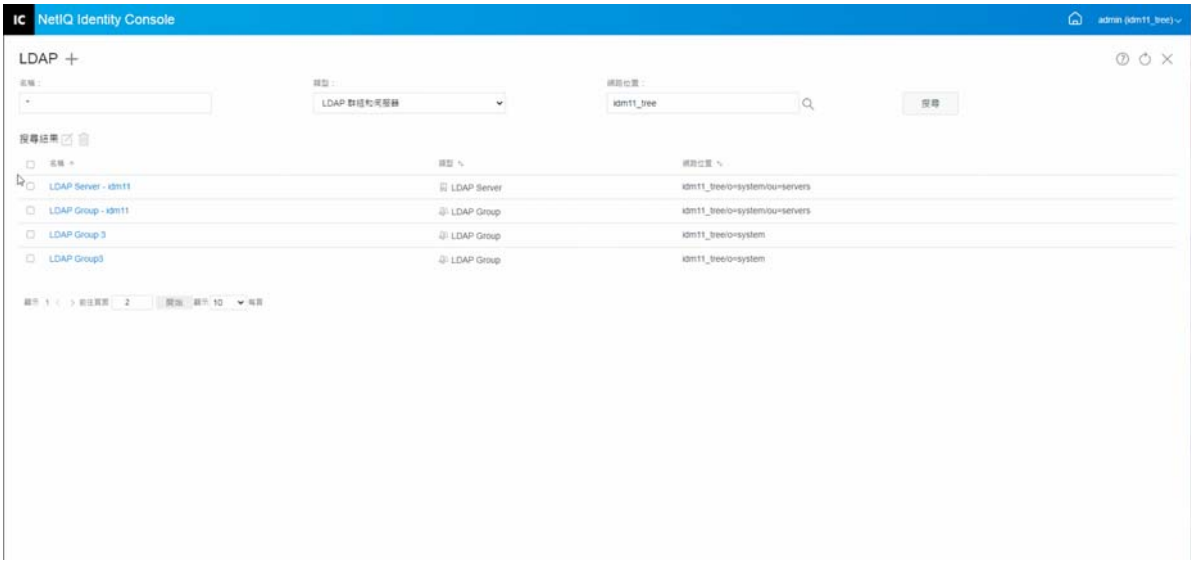
1 從 Identity Console 抵達頁面，按一下「**LDAP 組態**」選項。

2 指定 LDAP 物件的名稱、類型和網路位置，然後按一下 搜尋 按鈕。

3 從搜尋清單選取 LDAP 物件，然後按一下 圖示。

4 隨即顯示確認訊息，指出已刪除 LDAP 物件。

圖 16-2 刪除 LDAP 物件

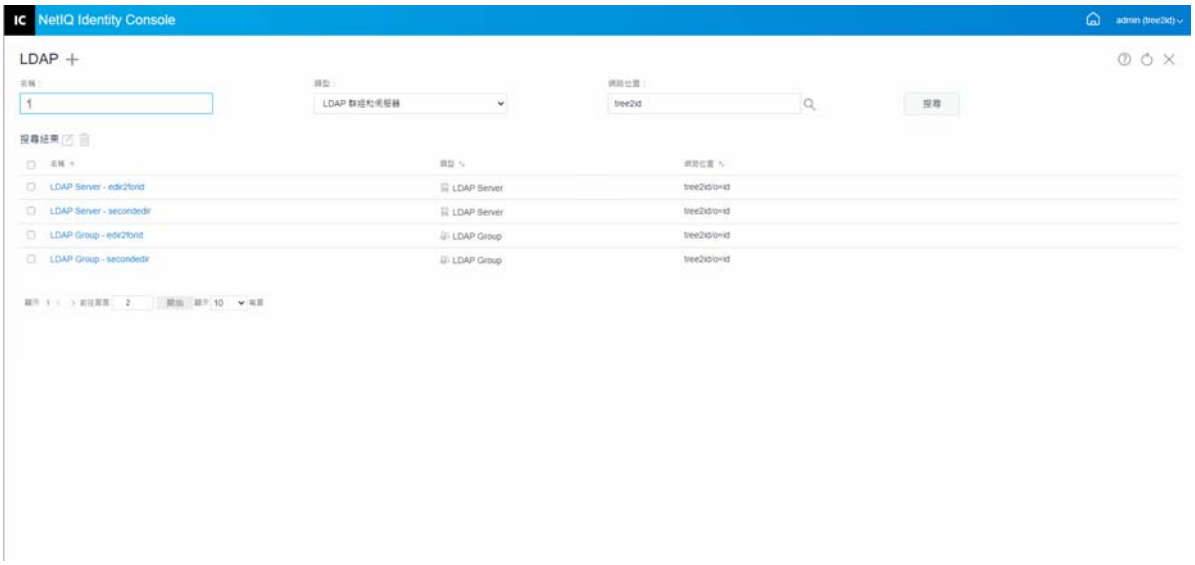


修改 LDAP 物件

若要修改 LDAP 物件：

1. 從 Identity Console 抵達頁面，按一下「**LDAP 組態**」選項。
2. 輸入 LDAP 物件的名稱、類型和網路位置，然後按一下 搜尋 按鈕。
3. 從搜尋清單選取 LDAP 物件，然後按一下 圖示。
4. 根據需要修改特定 LDAP 物件的屬性和資訊，然後按一下 儲存 按鈕。如需有關 LDAP 物件之屬性的詳細資訊，請參閱 *《NetIQ eDirectory 系統管理指南》*上的設定 Linux 上的 LDAP 伺服器和 LDAP 群組物件。
5. 隨即顯示確認訊息，指出已修改 LDAP 物件。

圖 16-3 *修改 LDAP 物件*



17 管理證書

當您安裝 eDirectory 時，會自動安裝 NetIQ 證書伺服器。「證書伺服器」提供公用金鑰密碼服務，此服務原本就整合在 eDirectory 並容許您創造、發送和管理使用者和伺服器證書。這些服務可讓您保護透過公用通訊通道 (如網際網路) 傳輸的機密資料。

附註：如果您想要 「證書管理」模組與 Identity Console 搭配使用，則必須將您的 eDirectory 伺服器升級至 9.2.4 HF2。

Identity Console 提供下列證書管理任務 :

管理證書管理中心

根據預設，NetIQ 證書伺服器安裝程序會為您建立組織證書管理中心 (CA)。系統會提示您指定組織 CA 名稱。當您按一下 「完成」時，即會建立組織 CA，其具有預設參數並放置在安全性容器中。如果您希望對於建立 CA 有更多控制權，則可以藉由使用 Identity Console 入口網站來手動建立組織 CA。此外，如果您刪除組織 CA，則需要重新建立。

使用證書管理中心模組，您可以執行以下任務 :

建立組織 CA 物件

若要建立組織 CA 物件，請執行以下步驟：

1 按一下 Identity Console 抵達頁面上的「**證書管理**」>「**CA 管理**」選項。

2 如果不存在任何組織證書管理中心物件，這將會開啟「建立組織證書管理中心物件」對話方塊，以及建立物件的對應精靈。遵循提示建立物件。

附註：確保此處指定的 CRL 檔案路徑與 eDirectory 安裝路徑相關。

---

3 在您完成建立證書管理中心之後，我們建議您備份 CA 的公用 / 私密金鑰組，並將此金鑰組儲存在安全的地方。如需詳細資訊，請參閱 「備份組織 CA 證書」(第 90 頁)。

備份組織 CA 證書

我們建議您備份組織 CA 的私密金鑰和證書，以防組織 CA 的主機伺服器出現無法恢復的故障。如果出現故障，您可以使用備份檔案將「組織 CA」還原到樹狀結構中的任何伺服器。

附註：備份組織 CA 的能力僅適用於至少使用證書伺服器 9.0 版建立的組織 CA。在先前版本的證書伺服器中，組織 CA 的私密金鑰是以不可能輸出的方式建立。

備份檔案包含 CA 的私密金鑰、自行簽署的證書、公用金鑰證書以及操作所需的其他幾個證書。此資訊以 PKCS #12 格式 (也稱為 PFX) 進行儲存。

組織 CA 應該在正常運作時進行備份。

若要備份組織 CA，請執行以下步驟：

1 按一下 Identity Console 抵達頁面上的「**證書管理**」>「**CA 管理**」選項。

2 按一下「**證書**」索引標籤。

3 選取「**自行簽署的證書**」或「**公用金鑰證書**」。在備份操作期間，這兩個證書都會寫入檔案。我們建議您個別針對 RSA 和 ECDSA 證書選取「自行簽署的證書」。

4 按一下 圖示。

5 選擇輸出私密金鑰，指定具有 6 個以上英數字元的密碼，用於加密 PFX 檔案，並且選取 PKCS12 作為輸出格式，然後按一下「**確定**」。

6 加密備份檔案已寫入指定位置。現已準備好儲存在安全位置，以供緊急使用。

還原組織 CA

如果組織 CA 物件已被刪除或損毀，或者組織 CA 的主機伺服器出現無法恢復的故障，則組織 CA 可以透過使用如 「備份組織 CA 證書」 (第 90 頁) 中所述建立的備份檔案，還原為完整操作。

若要還原組織 CA，請執行以下步驟：

1. 按一下 Identity Console 抵達頁面上的「**證書管理**」>「**CA 管理**」選項。
2. 按一下螢幕上方的 ↑↓ (「**證書管理中心管理**」旁邊) 以刪除現有的組織 CA。
3. 系統現在會提示您設定新的組織 CA。這樣會開啟「建立組織證書管理中心物件」對話方塊，以及建立物件的對應精靈。
4. 在建立對話方塊中，指定應代管組織 CA 的伺服器和組織 CA 物件的名稱。
5. 選取「**輸入**」。
6. 同時選取 RSA 和 ECDSA 證書。證書伺服器要求兩個證書的標題名稱相同。但是，證書伺服器不支援輸入外部自行簽署的 CA 證書。但是，其允許您輸入從屬 CA 證書。
7. 在隨後顯示的螢幕上，瀏覽並選取 RSA 和 ECDSA 的檔案名稱。
8. 在進行備份時輸入用於加密檔案的密碼，然後按一下「**確定**」。
9. 組織 CA 的私密金鑰和證書現已還原，CA 已完全正常運作。該檔案現在可以再次儲存以供未來使用。

驗證組織 CA 證書

如果您懷疑證書有問題或認為證書可能不再有效，您可以使用 Identity Console 輕鬆驗證證書。eDirectory 中的任何證書都可以驗證，包括外部 CA 簽發的證書。

證書驗證程序包括對證書中資料以及證書鏈中資料的多次檢查。證書鏈由根 CA 證書和選擇性的一或多個中介 CA 證書組成。

若要驗證證書：

1. 按一下 Identity Console 抵達頁面上的「**證書管理**」>「**CA 管理**」選項。
2. 按一下「**證書**」索引標籤。
3. 選取「**自行簽署的證書**」或「**公用金鑰證書**」。
4. 按一下 ✓ 以驗證選取的 CA 證書。

取代組織 CA 的證書

如果證書因為某種原因而損毀或無效，或者您只是想取代現有證書，請執行以下步驟：

1. 按一下 Identity Console 抵達頁面上的「**證書管理**」>「**CA 管理**」選項。
2. 按一下「**證書**」索引標籤。
3. 選取「**自行簽署的證書**」或「**公用金鑰證書**」。

4 按一下 ↑↓ 以取代選取的 CA 證書。

5 以 .pfx 或 .p12 格式輸入 CA 證書，並且指定密碼以加密私密金鑰。

6 按一下 「確定」。

撤銷組織 CA 證書

若要撤銷證書：

1 按一下 Identity Console 抵達頁面上的 「證書管理」 > 「CA 管理」選項。

2 按一下 「證書」索引標籤。

3 選取 「自行簽署的證書」或 「公用金鑰證書」。

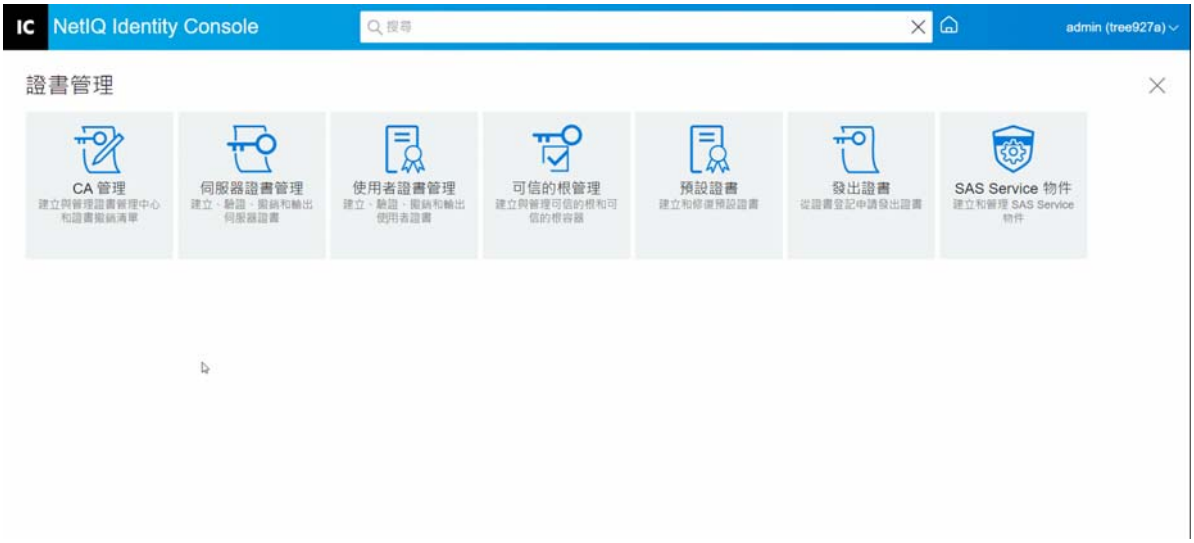
4 按一下 ⊘ 圖示。

5 閱讀並瞭解撤銷伺服器證書所涉及的風險。

6 從下拉式清單中選取撤銷的有效理由，選取無效日期並指定任何其他備註。

7 按一下 「確定」以完成撤銷。

圖 17-1 管理證書管理中心



管理伺服器證書

使用伺服器證書管理模組，管理員可以執行以下任務：

- 「建立伺服器證書物件」 (第 93 頁)
- 「輸出伺服器證書物件」 (第 93 頁)
- 「驗證伺服器證書物件」 (第 93 頁)
- 「取代伺服器證書物件」 (第 94 頁)

- 「撤銷伺服器證書物件」(第 94 頁)
- 「刪除伺服器證書物件」(第 94 頁)

建立伺服器證書物件

若要建立伺服器證書物件，請執行以下步驟：

1 按一下 Identity Console 抵達頁面上的「**證書管理**」>「**伺服器證書管理**」選項。

2 按一下 ＋ 圖示。

3 在「**建立伺服器證書**」頁面中，指定「**暱稱**」伺服器，並且選取下列任何一個選項：

- **標準 (預設參數):** 允許您建立 RSA 或 ECDSA 類型的預設伺服器證書物件。
- **自定 (使用者指定的參數):** 允許您指定伺服器證書物件的自定參數。
- **輸入 (允許輸入 PKCS12 檔案):** 允許您輸入 .pfx 或 .p12 格式的 PKCS12 檔案。

4 指定參數之後，按「**下一步**」以檢閱證書的摘要。

5 在「**摘要**」畫面中，按一下「**確定**」以建立伺服器證書物件。

輸出伺服器證書物件

若要輸出伺服器證書物件，請執行以下步驟：

1 按一下 Identity Console 抵達頁面上的「**證書管理**」>「**伺服器證書管理**」選項。

2 從下拉式清單中選取適當的伺服器。

3 從清單選取適當的伺服器證書，然後按一下 圖示。

4 在下一個畫面上，選取「**輸出私密金鑰**」的核取方塊，並且指定密碼以保護私密金鑰。確認密碼並選取輸出格式。

附註：只能以 PKCS12 格式輸出伺服器證書。

---

5 按一下「**確定**」以輸出伺服器證書物件。

驗證伺服器證書物件

若要驗證伺服器證書物件，請執行以下步驟：

1 按一下 Identity Console 抵達頁面上的「**證書管理**」>「**伺服器證書管理**」選項。

2 從下拉式清單中選取適當的伺服器。

3 從清單選取適當的伺服器證書，然後按一下 圖示。

4 隨即顯示確認，指出成功驗證伺服器證書物件。

取代伺服器證書物件

如果伺服器證書因為某種原因而損毀或無效，或者您只是想取代現有預設證書，請執行以下步驟：

1. 按一下 Identity Console 抵達頁面上的「證書管理」>「伺服器證書管理」選項。
2. 從下拉式清單中選取適當的伺服器。
3. 從清單選取適當的伺服器證書，然後按一下 ↑↓ 圖示。
4. 閱讀及瞭解取代伺服器證書所涉及的風險，然後按一下「確定」。
5. 在下一個畫面上，瀏覽並選取 .pfx 或 .p12 格式的新伺服器證書，並且指定密碼。
6. 按一下「確定」以取代伺服器證書。

撤銷伺服器證書物件

若要撤銷伺服器證書物件，請執行以下步驟：

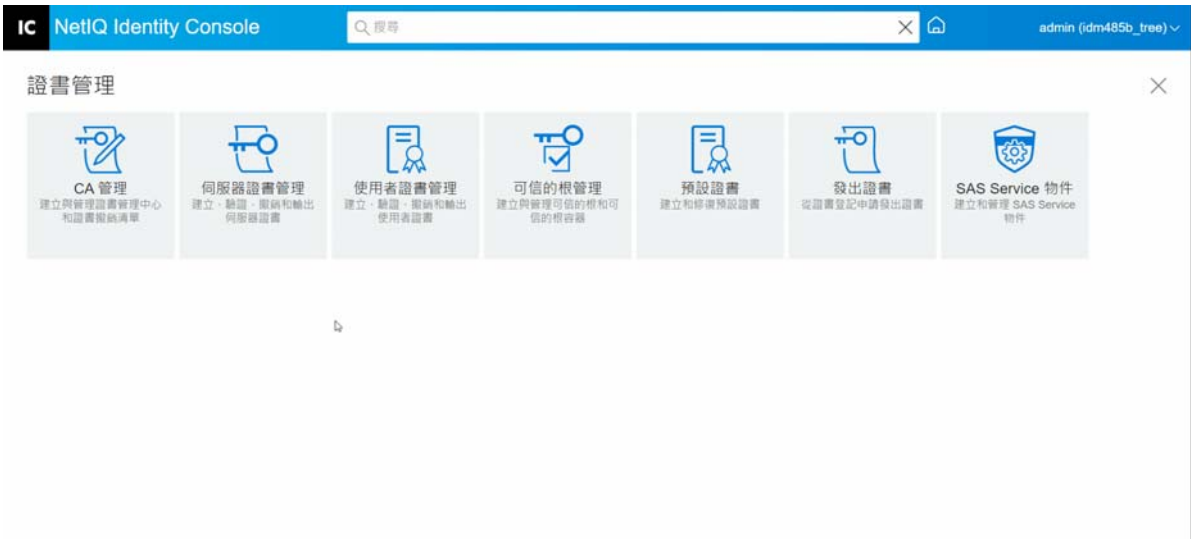
1. 按一下 Identity Console 抵達頁面上的「證書管理」>「伺服器證書管理」選項。
2. 從下拉式清單中選取適當的伺服器。
3. 從清單選取適當的伺服器證書，然後按一下 ⊘ 圖示。
4. 閱讀及瞭解撤銷伺服器證書所涉及的風險，然後按一下「確定」。
5. 在下一個畫面中，從下拉式清單中選取撤銷的有效理由，選取無效日期並指定任何其他備註。
6. 按一下「確定」以完成撤銷。

刪除伺服器證書物件

若要移除伺服器證書物件，請執行以下步驟：

1. 按一下 Identity Console 抵達頁面上的「證書管理」>「伺服器證書管理」選項。
2. 從下拉式清單中選取適當的伺服器。
3. 從清單選取適當的伺服器證書，然後按一下 🗑 圖示。
4. 在接下來的畫面上，按一下「確定」。
5. 隨即顯示確認，指出成功刪除伺服器證書物件。

圖 17-2 管理伺服器證書



管理使用者證書

使用使用者證書管理模組，您可以執行以下任務：

- 「建立使用者證書物件」(第 95 頁)
- 「匯出使用者證書物件」(第 96 頁)
- 「驗證使用者證書物件」(第 96 頁)
- 「撤銷使用者證書物件」(第 96 頁)
- 「刪除使用者證書物件」(第 96 頁)

建立使用者證書物件

若要建立伺服器證書物件，請執行以下步驟：

1. 按一下 Identity Console 抵達頁面上的 「**證書管理**」 > 「**使用者證書管理**」選項。
2. 按一下 ＋ 圖示。
3. 在 「**建立使用者證書**」頁面中，指定 「**暱稱**」伺服器，並且選取下列任何一個選項：
   - **標準 (預設參數):** 允許您建立 RSA 或 ECDSA 類型的預設使用者證書物件。
   - **自定 (使用者指定的參數):** 允許您指定使用者證書物件的自定參數。
   - **輸入**： 允許您以 CERT 或 PKCS12 格式輸入證書檔案。
4. 指定參數之後，按 「**下一步**」以檢閱證書的摘要。
5. 在 「**摘要**」畫面中，按一下 「**確定**」以建立使用者證書物件。

匯出使用者證書物件

若要輸出使用者證書物件，請執行以下步驟：

1 按一下 Identity Console 抵達頁面上的「**證書管理**」>「**使用者證書管理**」選項。

2 從下拉式清單中選取適當的伺服器。

3 從清單選取適當的使用者證書，然後按一下 圖示。

4 在下一個畫面上，選取「**輸出私密金鑰**」的核取方塊，並且指定密碼以保護私密金鑰。確認密碼並選取輸出格式。

附註：只能以 PKCS12 格式輸出使用者證書。

5 按一下「**確定**」以輸出使用者證書物件。

驗證使用者證書物件

若要驗證使用者證書物件，請執行以下步驟：

1 按一下 Identity Console 抵達頁面上的「**證書管理**」>「**使用者證書管理**」選項。

2 從下拉式清單中選取適當的伺服器。

3 從清單選取適當的使用者證書，然後按一下 圖示。

4 隨即顯示確認，指出成功驗證使用者證書物件。

撤銷使用者證書物件

若要撤銷使用者證書物件，請執行以下步驟：

1 按一下 Identity Console 抵達頁面上的「**證書管理**」>「**使用者證書管理**」選項。

2 從下拉式清單中選取適當的伺服器。

3 從清單選取適當的使用者證書，然後按一下 圖示。

4 閱讀並瞭解撤銷使用者證書所涉及的風險。

5 從下拉式清單中選取撤銷的有效理由，選取無效日期並指定任何其他備註。

6 按一下「**確定**」以完成撤銷。

刪除使用者證書物件

若要移除使用者證書物件，請執行以下步驟：

1 按一下 Identity Console 抵達頁面上的「**證書管理**」>「**使用者證書管理**」選項。

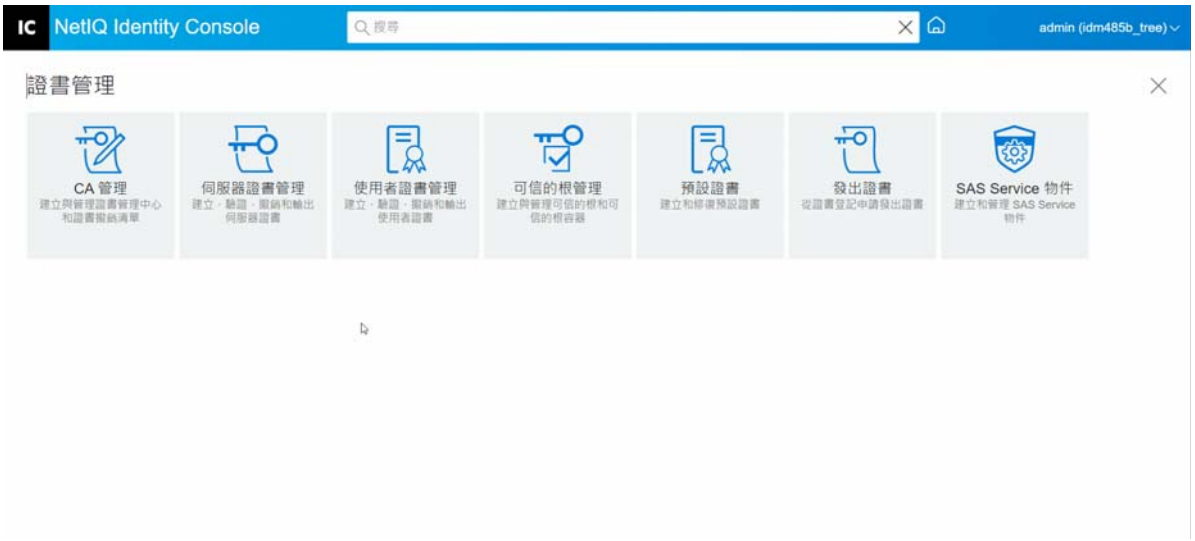
2 從下拉式清單中選取適當的伺服器。

3 從清單選取適當的使用者證書，然後按一下 圖示。

4 在接下來的畫面上，按一下「**確定**」。

5 隨即顯示確認，指出成功刪除使用者證書物件。

圖 17-3 管理使用者證書



管理可信的根和容器

可信的根提供在公用金鑰加密法中信任的基礎。可信的根用於驗證由其他 CA 簽署的證書。可信的根可實現 SSL、安全電子郵件和證書型驗證等安全性。

使用可信的根管理模組，您可以執行以下任務：

- 「建立可信的根容器」(第 97 頁)
- 「建立可信的根證書物件」(第 98 頁)
- 「輸出可信的根證書物件」(第 98 頁)
- 「驗證可信的根證書物件」(第 98 頁)
- 「刪除可信的根證書物件」(第 99 頁)
- 「刪除可信的根容器」(第 99 頁)

建立可信的根容器

若要建立可信的根容器，請執行以下任務：

1. 按一下 Identity Console 抵達頁面上的 **「證書管理」** > **「可信的根管理」**選項。預設會選取 **「可信的根容器」**核取方塊。
2. 按一下 ＋ 圖示以建立新的可信的根容器。
3. 指定可信的根容器的名稱。
4. 使用物件選擇器以瀏覽適當的容器。
5. 按一下 **「儲存」**按鈕。
6. 隨即顯示確認，指出已成功建立可信的根容器。

建立可信的根證書物件

若要建立可信的根物件，請執行以下步驟：

1 按一下 Identity Console 抵達頁面上的「證書管理」>「可信的根管理」選項。預設會選取「可信的根容器」核取方塊。選取「可信的根」核取方塊。

2 按一下 ＋ 圖示以建立新的可信的根物件。

3 指定可信的根物件的名稱。

4 從下拉式清單中選取適當可信的根容器。

5 瀏覽並選取 .der 或 .b64 格式的適當證書檔案。

附註：任何類型的證書都可以儲存在可信的根物件 (CA 證書、中介 CA 證書或使用者證書)。

6 按一下「確定」按鈕。

7 隨即顯示確認，指出已成功建立可信的根物件。

輸出可信的根證書物件

若要輸出可信的根證書物件，請執行以下步驟：

1 按一下 Identity Console 抵達頁面上的「證書管理」>「可信的根管理」選項。預設會選取「可信的根容器」核取方塊。選取「可信的根」核取方塊。

2 從清單選取適當可信的根證書，然後按一下 圖示。

3 在下一個畫面上，選取「輸出私密金鑰」的核取方塊，並且指定密碼以保護私密金鑰。確認密碼並選取輸出格式。

附註：可信的根證書只能以 DER 或 BASE64 格式輸出。

4 按一下「確定」以輸出可信的根證書物件。

驗證可信的根證書物件

若要驗證可信的根證書物件，請執行以下步驟：

1 按一下 Identity Console 抵達頁面上的「證書管理」>「可信的根管理」選項。預設會選取「可信的根容器」核取方塊。選取「可信的根」核取方塊。

2 從清單選取適當可信的根證書，然後按一下 圖示。

3 隨即顯示確認，指出成功驗證可信的根證書物件。

刪除可信的根證書物件

若要移除可信的根證書物件，請執行以下步驟：

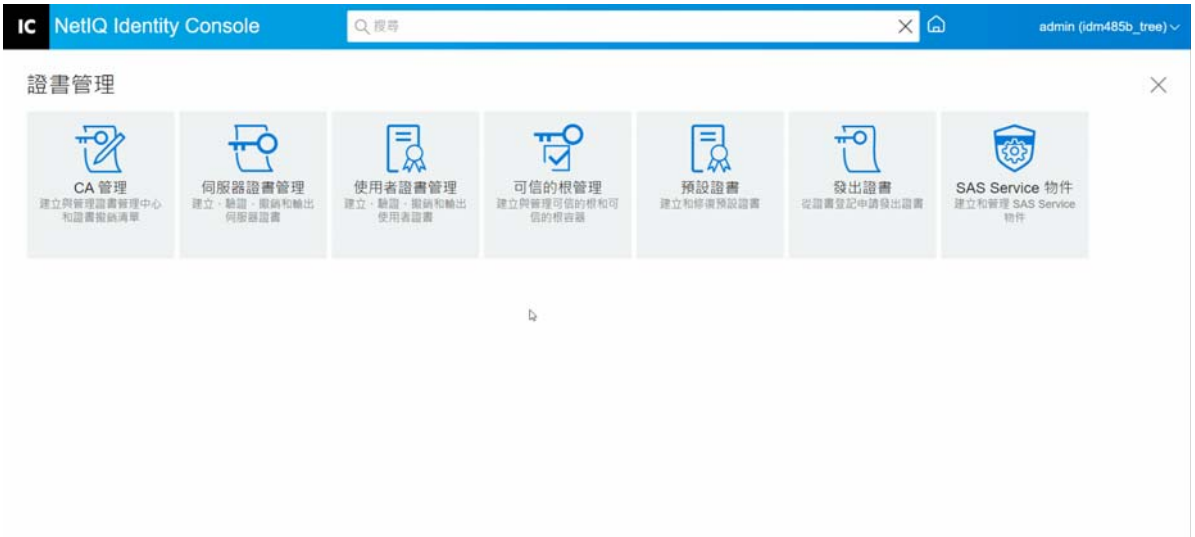
1. 按一下 Identity Console 抵達頁面上的「證書管理」>「可信的根管理」選項。預設會選取「可信的根容器」核取方塊。選取「可信的根」核取方塊。
2. 從清單選取適當可信的根證書，然後按一下 圖示。
3. 按一下警告畫面上的「確定」。
4. 隨即顯示確認，指出成功移除可信的根證書物件。

刪除可信的根容器

若要移除可信的根物件，請執行以下步驟：

1. 按一下 Identity Console 抵達頁面上的「證書管理」>「可信的根管理」選項。預設會選取「可信的根容器」核取方塊。
2. 從清單選取適當可信的根容器，然後按一下 圖示。
3. 按一下警告畫面上的「確定」。
4. 隨即顯示確認，指出成功移除可信的根容器。

圖 17-4 *管理可信的根容器*



建立預設伺服器證書物件

證書伺服器安裝會建立預設伺服器證書物件。

- SSL CertificateDNS - *server_name*
- 伺服器上針對每個 IP 位址設定的證書 (IPAG*xxx.xxx.xxx.xxx - server_name*)
- 伺服器上針對每個 DNS 名稱設定的證書 (DNSAG*www.example.com - server_name*)

附註：eDirectory 不會自動建立 SSL CertificateIP。SSL 證書 DNS 包含標題替代名稱中列出的所有 IP。當您嘗試使用 Identity Console 建立或修復預設證書時，預設不會建立或修復 SSL CertificateIP 證書。但是，外掛程式介面提供了一個核取方塊，您可以選取該核取方塊以覆寫預設行為並強制建立 / 修復 SSL CertificateIP 證書。

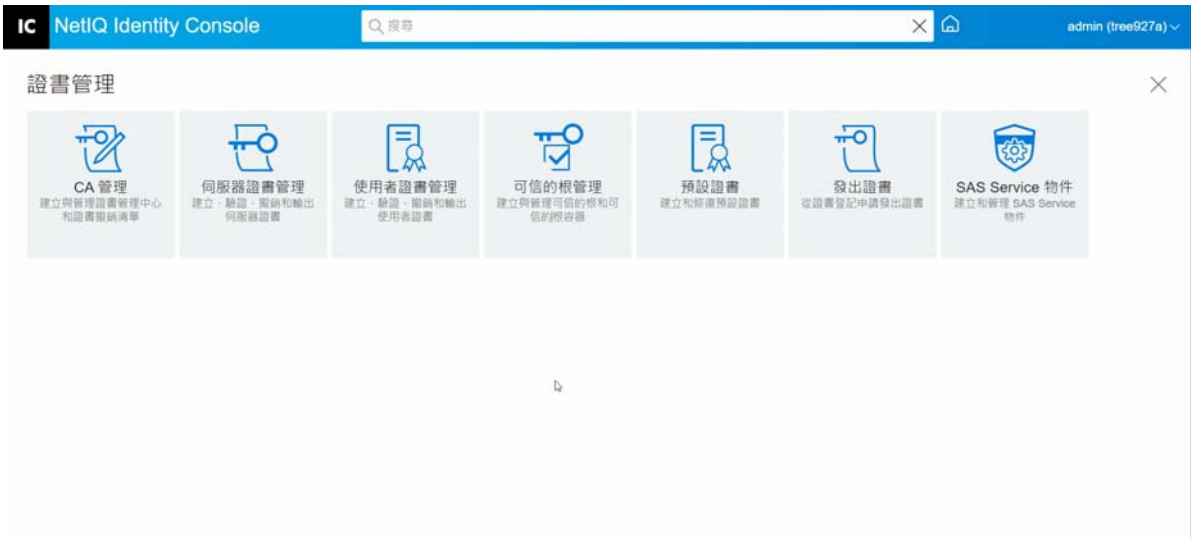
如果組織 CA 有 ECDSA 證書，則 eDirectory 9.0 和更新版本會自動建立 ECDSA 證書。

如果這些證書因為某種原因而損毀或無效，或者如果您只是想取代現有的預設證書，您可以使用「建立預設伺服器證書精靈」，如下列程序所述：

1. 按一下 Identity Console 抵達頁面上的**「證書管理」**>**「預設證書」**選項。
2. 選取您想要為其建立預設證書的伺服器，然後按**「下一步」**。
3. 如果您想要覆寫現有的預設伺服器證書，請選取「是」，如果您只想要在現有的預設伺服器證書無效時覆寫，則選取「否」。
4. (僅限單一伺服器) 如果您想要使用現有的 DNS 位址，請選取該選項。如果您想使用不同的 DNS 位址，請選取該選項並指定新的 DNS 位址。
5. (僅限單一伺服器) 如果您想要使用現有的預設 IP 位址，請選取該選項。如果您想使用不同的 IP 位址，請選取該選項並指定新的 IP 位址。
6. 按**下一步**。
7. 檢視摘要頁面，然後按一下**「完成」**。

如果您想要對伺服器證書物件的建立有更多控制權，您可以手動建立伺服器證書物件。如需詳細資訊，請參閱 「建立伺服器證書物件」(第 93 頁)。

圖 17-5 *建立預設伺服器證書物件*



簽發公用金鑰證書

您的組織 CA 的工作方式與外部 CA 相同。這意味著，其能夠從證書登記申請 (CSR) 中簽發證書。當使用者將 CSR 傳送給您進行簽署時，您可以使用您的組織 CA 簽發證書。然後，申請證書的使用者可以採用已簽發的證書並且直接將其輸入已啟用加密的應用程式。

此任務允許您為無法辨識伺服器證書物件的已啟用加密應用程式，產生證書。

若要簽發證書，請執行以下步驟：

1. 按一下 Identity Console 抵達頁面上的 **「證書管理」** > **「簽發證書」**選項。
2. 瀏覽並選取 CSR 檔案。
3. 根據 「關鍵使用規範」選取適當的金鑰類型和對應的金鑰使用。這些選項允許您選取金鑰類型。每個金鑰類型均具有預先定義並與之相關的金鑰使用值。
   - **3a** **未指定 :** 此選項預設為選取，未在證書中啟動任何金鑰使用。
   - **3b** **證書管理中心：** 此選項會啟動 「證書登記」與 「CRL 簽署」金鑰使用。
   - **3c** **加密 :** 此選項會啟動 「鍵密碼」金鑰使用。
   - **3d** **簽名 :** 此選項會啟動 「數位簽名」金鑰使用。
   - **3e** **SSL 或 TSL:** 此選項會設定金鑰，使其可用於 SSL 或 TLS 交易。
   - **3f** **自定 :** 此選項可讓您手動選取任何或所有的金鑰使用選項。
   - **3g** **將金鑰使用延伸設定為重要 :** 選取除了 「未指定」以外的任何金鑰類型，您可以將金鑰使用延伸標示為重要。接收軟體必須瞭解重要的延伸，才可以將證書用於任何用途。因此，將延伸標示為重要會產生一些危險，因為並非所有應用程式都可以使用該證書。但是，對於常見的延伸 (如金鑰使用) 而言，危險性是很小的。一般而言，如果您指定了金鑰使用，則應該將延伸標示為重要。
4. 您可以選擇將 **「延伸金鑰使用」**延伸編碼在證書中。若要啟動此功能，請選取 **「啟用延伸金鑰使用」**。
   - **4a** **伺服器 :** 此選項會啟動 「伺服器驗證」延伸金鑰使用。
   - **4b** **使用者 :** 此選項會啟動 「使用者驗證」及 「電子郵件保護」延伸金鑰使用。
   - **4c** **自定 :** 此選項可讓您選取任何或所有的 「延伸金鑰使用」。
   - **4d** **任何 :** 讓金鑰能用於任何延伸金鑰使用。
   - **4e** **將延伸金鑰使用延伸設定為重要 :** 接收軟體必須瞭解重要的延伸，才可以將證書用於任何用途。因此，將延伸標示為重要會產生一些危險，因為並非所有應用程式都可以使用該證書。由於許多應用程式不瞭解 「延伸金鑰使用延伸」，將此延伸標示為重要會產生重大的風險，可能讓特定的應用程式不接受該證書；因此只有在必要時才應該設定為重要。

5 選取適當的 **「基本限制」**：

5a 證書類型：

5a1 未指定：如果您不想在證書中新增基本限制延伸，請選取這個選項。

5a2 證書管理中心：選取這個選項可以新增 「證書管理中心」基本限制延伸到證書。如果證書是針對 「證書管理中心」，您必須選取這個選項。

5a3 終端實體：選取這個選項，以新增基本限制延伸到證書，證書中會指定這是「終端實體」(非 「證書管理中心」) 證書。注意：如果證書的類型為 「終端實體」，路徑長度應該設為 「未指定」。

5b 路徑長度：

5b1 未指定：如果您不想要指定在此 CA 之下可以建立的次 CA 階層數，請選取這個選項。

附註：如果證書的類型為 「終端實體」，路徑長度應該只設為 「未指定」。

5b2 特定：如果您想要指定在此 CA 之下可以建立的次 CA 階層數，請選取這個選項。按一下向上箭頭與向下箭頭，以指定路徑長度。

附註：如果建立中的證書是從屬 CA，路徑長度必須與上層 CA 一致。例如，如果上層 CA 的路徑長度為 3，次 CA 的路徑長度必須為 2 以下。如果上層 CA 未指定路徑長度，次 CA 的路徑長度可能也是未指定，或是任何想要使用的特定路徑長度。

5c 將基本限制延伸設定為重要：一般而言，CA 證書的 「基本限制延伸」必須設定為重要。接收軟體必須瞭解重要的延伸，才可以將證書用於任何用途。因此，將延伸標示為重要會產生一些危險，因為並非所有應用程式都可以使用該證書。但是，對於常見的延伸 (例如 「基本限制」) 而言，危險性是很小的。

6 指定以下證書參數：

6a 接收者名稱：顯示您 eDirectory 網路樹的完整鍵入名稱。

6b 接收者名稱：顯示您 eDirectory 網路樹的完整鍵入名稱。

6c 有效期間：使用下拉清單來指定證書有效的期間。範圍從六個月至最大時間值，即西元 2036 年 (根據 32 位元時間值定的時間限制)。如果您選取 「指定日期」選項，則可以編輯 「生效日期」和 「過期日期」欄位，以建立自定的有效期間。選定的最大日期必須在 CA 的有效日期內。

6c1 生效日期： 讓您顯示或編輯證書生效的時間與日期。

6c2 過期日期：讓您顯示或編輯證書失效的時間與日期。

6d 自定延伸：讓 Certificate Server 能夠支援您要在建立證書時包含的任何標準或自定延伸。延伸必須先前已建立並儲存在檔案中 (每個檔案一個延伸)。任何延伸必須編碼為 ASN.1，如 IETF RFC 2459/3280 的 4.2 節中所定義。

如果您要在建立的證書中包含一個以上的自定延伸，請按一下 「新增」然後瀏覽包含自定延伸的檔案，並將它新增到證書中。可以重複此程序來新增多個延伸。

若要刪除自定延伸檔案，請選取然後按一下  圖示。

7 從以下選項中選取適當的證書格式：

7a 二進位 DER 格式的檔案：此選項可讓您將證書儲存或輸出至「檔名」欄位所顯示的檔案中。根據預設，證書檔案是以 .DER 副檔名輸出至 Windows Identity Console 工作站磁碟機 C: 的根目錄，以及 Linux Identity Console 工作站的主目錄。

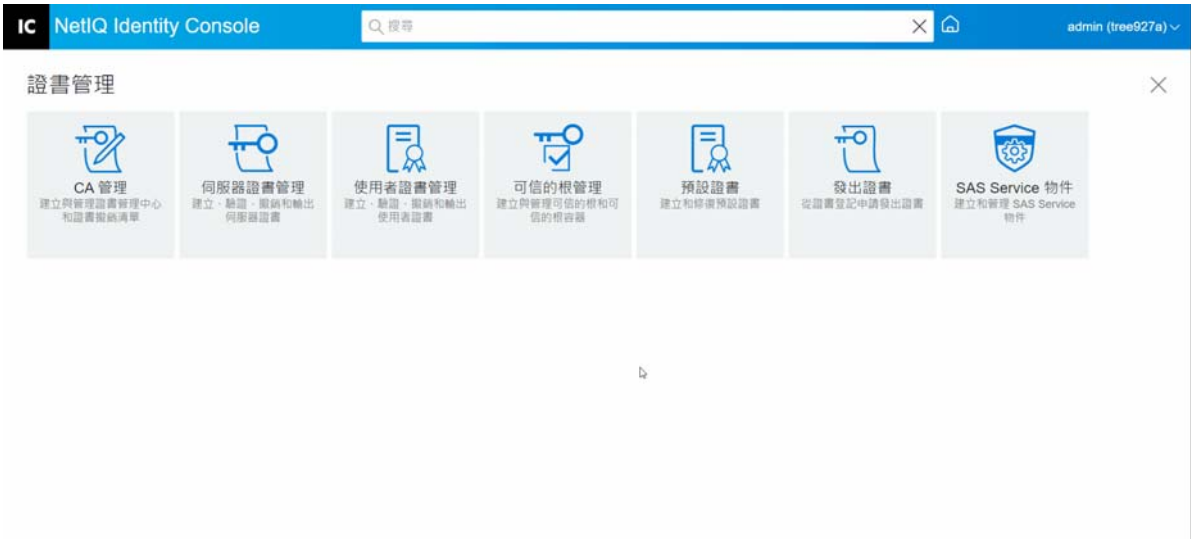
7b Base64 格式的檔案：此選項可讓您儲存 CSR 或將證書輸出至「檔名」欄位所顯示的檔案中。根據預設，證書和 CSR 檔案會以 .B64 副檔名輸出到 Windows Identity Console 工作站的 C: 磁碟機根目錄，以及 Linux Identity Console 工作站的主目錄。

7c CER 格式的檔案：此選項可讓您儲存 CSR 或將證書輸出至「檔名」欄位所顯示的檔案中。根據預設，證書和 CSR 檔案會以 .CER 副檔名輸出到 Windows Identity Console 工作站的 C: 磁碟機根目錄，以及 Linux Identity Console 工作站的主目錄。

8 在下一個畫面上檢閱證書摘要，然後按一下「**確定**」。

9 隨即顯示確認，指出已成功簽發證書。

圖 17-6 *簽發公用金鑰證書*



管理 SAS Service 物件

SAS Service 物件能協助伺服器與其伺服器證書之間的通訊。如果您從 eDirectory 移除伺服器，則也需要刪除與該伺服器相關的 SAS Service 物件。如果您要將伺服器放回網路樹，就必須建立 SAS Service 物件與該伺服器搭配。否則，您無法建立新的伺服器證書。

SAS Service 物件會自動在伺服器狀態檢查時建立。您不需要手動建立。

只有在與伺服器物件相同的容器中沒有適當命名的 SAS Service 物件時，您才可以建立新的 SAS Service 物件。例如，若伺服器名稱為 WAKE，SAS Service 物件的名稱將會是「SAS Service - WAKE」。公用程式會新增從「伺服器」物件到 SAS 物件的 DS 指標，以及從 SAS 物件到「伺服器」物件的 DS 指標，也會在 SAS Service 物件上設定正確的 ACL 項目。

如果具適當名稱的 SAS Service 物件已存在，您無法建立新的 SAS Service 物件。舊的 SAS Service 物件的 DS 指標可能錯誤或遺漏，或是 ACL 可能不正確。此時您可以刪除毀損的 SAS Service 物件，並使用 Identity Console 入口網站來建立新的 SAS Service 物件。

建立或刪除 SAS Service 物件

若要建立或刪除 SAS Service 物件，請執行以下步驟：

1 按一下 Identity Console 抵達頁面上的「**證書管理**」>「**SAS Service 物件**」選項。

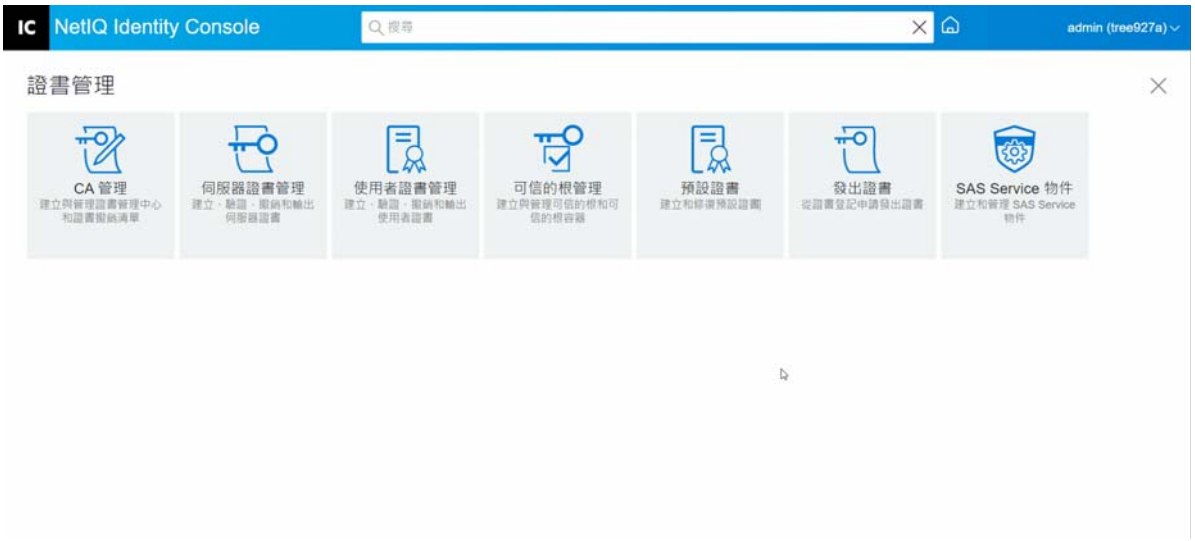
2 如果沒有為現有伺服器建立的 SAS Service 物件，則按一下 ＋ 圖示以建立新的服務物件。

3 隨即顯示確認訊息，指出已成功建立 SAS Service 物件。

4 若要移除 SAS Service 物件，請按一下 圖示。

5 在確認畫面中按一下「**確定**」以成功移除 SAS Service 物件。

圖 17-7 *管理 SAS Service 物件*



18 管理驗證框架

使用驗證模組，您可以執行以下任務：

- 「管理登入和登入後方法和序列」(第 105 頁)
- 「管理密碼規則」(第 111 頁)
- 「管理安全集」(第 115 頁)

管理登入和登入後方法和序列

NMAS 包括支援來自 NetIQ 和第三方驗證開發人員的一些登入和登入後方法。有些方法需要額外的硬體與軟體。確保您擁有所有必要的硬體和軟體，以實現您要使用的方法。

本節描述了如何安裝、設定和配置 NMAS 的登入和登入後方法和序列。

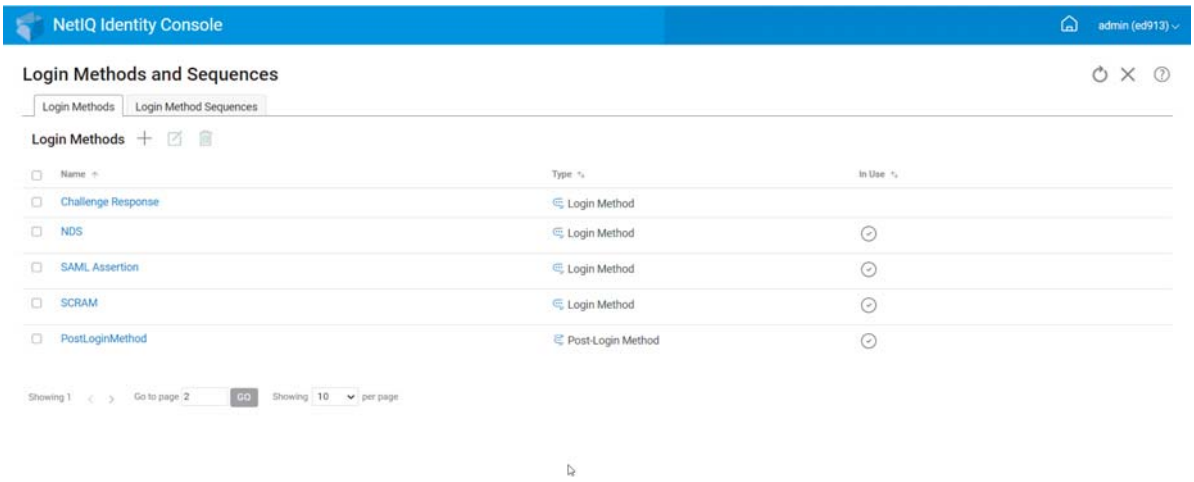
- 「安裝登入或登入後方法」(第 105 頁)
- 「更新現有登入或登入後方法」(第 106 頁)
- 「解除安裝登入或登入後方法」(第 107 頁)
- 「建立新的登入方法序列」(第 107 頁)
- 「修改登入方法序列」(第 108 頁)
- 「授權或取消授權登入方法序列」(第 109 頁)
- 「設定預設登入方法序列」(第 109 頁)
- 「刪除登入方法序列」(第 110 頁)

安裝登入或登入後方法

若要安裝登入方法，請執行以下任務：

1. 按一下 Identity Console 抵達頁面的 **「驗證管理」** > **「登入方法和序列」**選項。
2. 按一下 ＋ 圖示以安裝新的登入方法。
3. 瀏覽並選取您想要安裝的登入方法 (.zip) 檔案，然後按 **「下一步」**。
4. 遵循安裝精靈完成登入方法安裝程序。

圖 18-1 安裝新登入方法

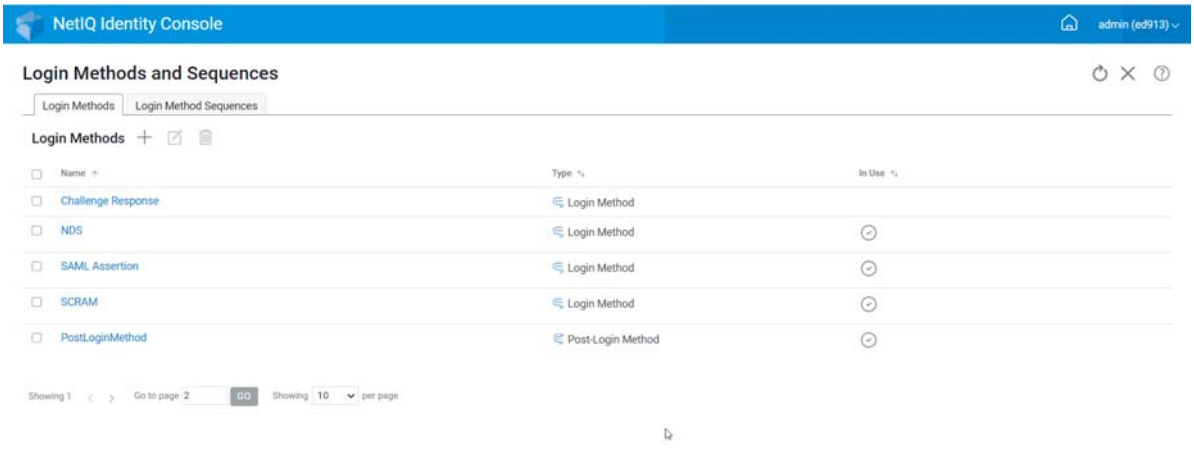


更新現有登入或登入後方法

若要更新現有登入方法，請執行以下步驟：

1. 按一下 Identity Console 抵達頁面的 「驗證管理」 > 「登入方法和序列」選項。
2. 選取要從清單中更新的登入方法，然後按一下 圖示。
3. 瀏覽並選取您想要更新的登入方法 (.zip) 檔案，然後按 「下一步」。
4. 遵循更新精靈完成更新登入方法。

圖 18-2 更新現有登入方法

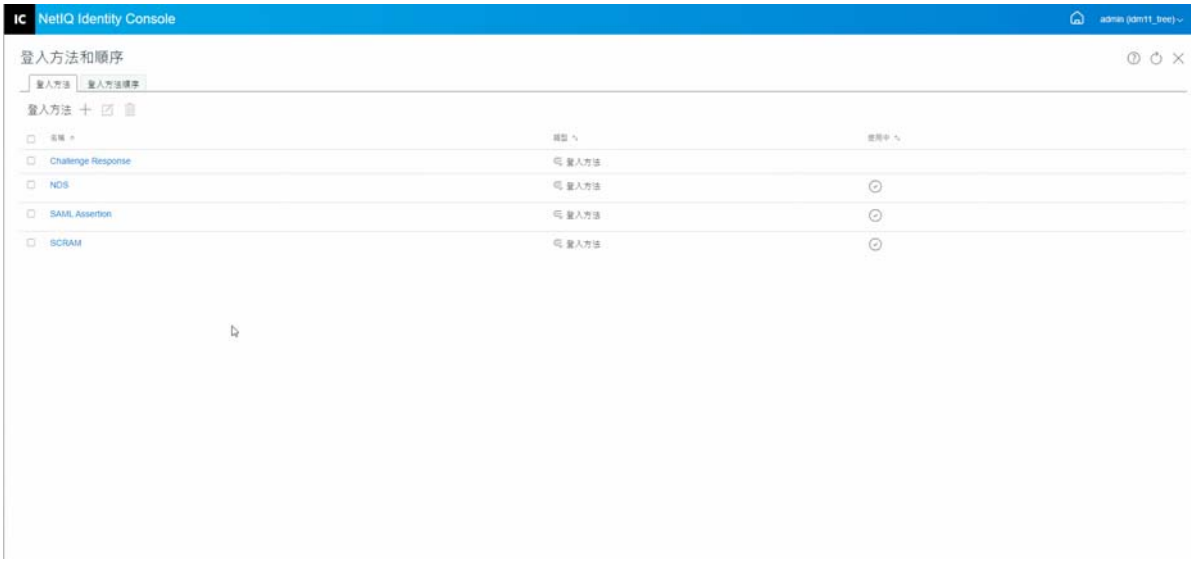


解除安裝登入或登入後方法

若要解除安裝登入或登入後方法，請執行以下步驟：

1. 按一下 Identity Console 抵達頁面的 「驗證管理」 > 「登入方法和序列」選項。
2. 選取要從清單中解除安裝的登入方法，然後按一下 圖示。
3. 在接下來的畫面上，按一下 「確定」。
4. 隨即顯示確認訊息，指出已解除安裝登入方法。

圖 18-3 *解除安裝登入方法*



建立新的登入方法序列

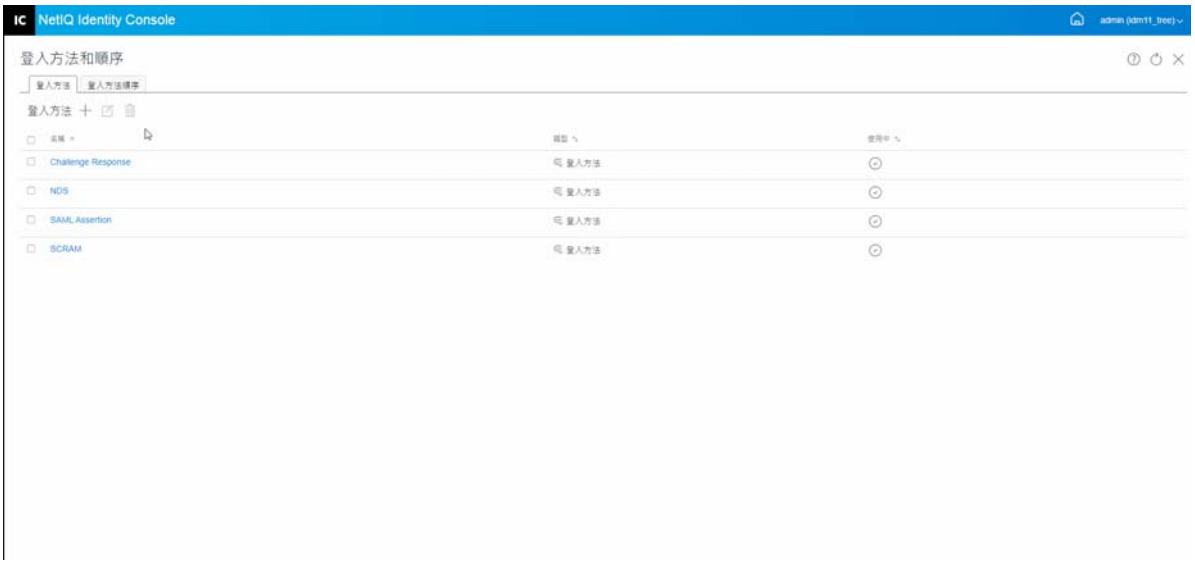
一旦為您的環境建立各種登入方法，您可以決定應使用這些方法的順序。若要建立新的登入方法序列，請執行以下步驟：

1. 按一下 Identity Console 抵達頁面的 「驗證管理」 > 「登入方法和序列」選項。
2. 選取 「登入方法序列」索引標籤。
3. 按一下 ＋ 圖示以建立新的登入方法序列。
4. 指定 「名稱」並且選取 「序列類型」。
5. 從可用的登入和登入後方法清單中選取必要的登入和登入後方法。

   附註：您可以藉由按一下可以在登入方法物件上看到的向上和向下箭頭，決定登入方法的順序。

6. 按一下 「建立」按鈕。
7. 隨即顯示確認訊息，指出已成功建立新登入方法序列。

圖 18-4 建立登入方法序列

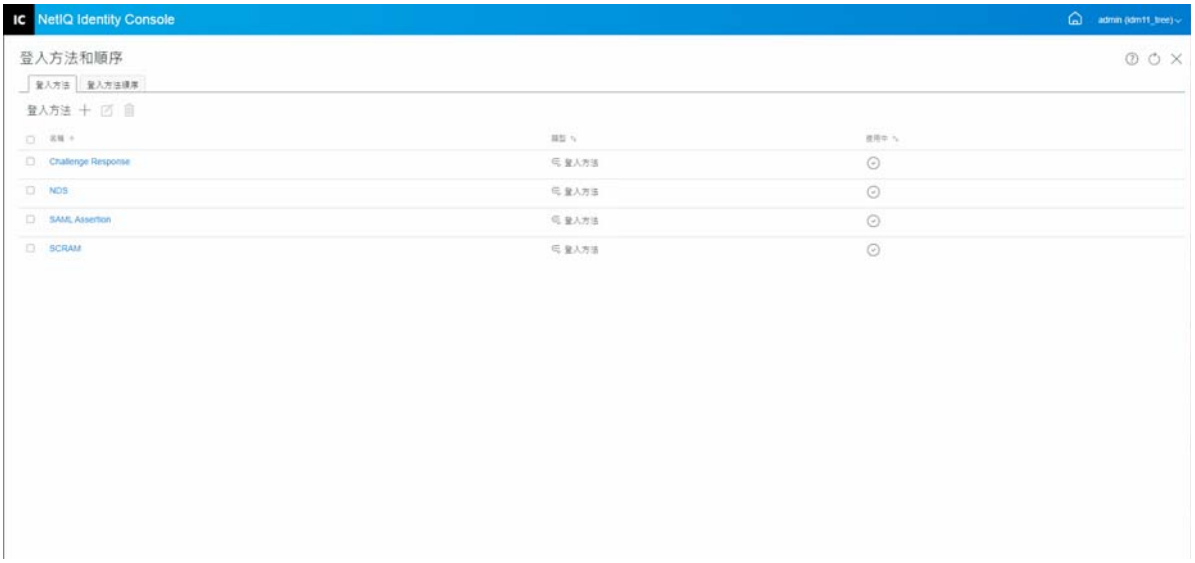


修改登入方法序列

若要修改現有登入方法序列，請執行以下步驟：

1. 按一下 Identity Console 抵達頁面的 「驗證管理」 > 「登入方法和序列」選項。
2. 選取 「登入方法序列」索引標籤。
3. 按一下 圖示以修改現有登入方法序列。
4. 在 「修改登入方法序列」頁面中進行必要的變更，然後按一下 「儲存」。
5. 隨即顯示確認訊息，指出已成功修改登入方法序列。

圖 18-5 修改登入方法序列



授權或取消授權登入方法序列

應該授權並設定為預設登入方法序列，以便將其與使用者、容器和分割區關聯在一起。若要授權登入方法序列，請執行以下步驟：

1 按一下 Identity Console 抵達頁面的 「驗證管理」 > 「登入方法和序列」選項。

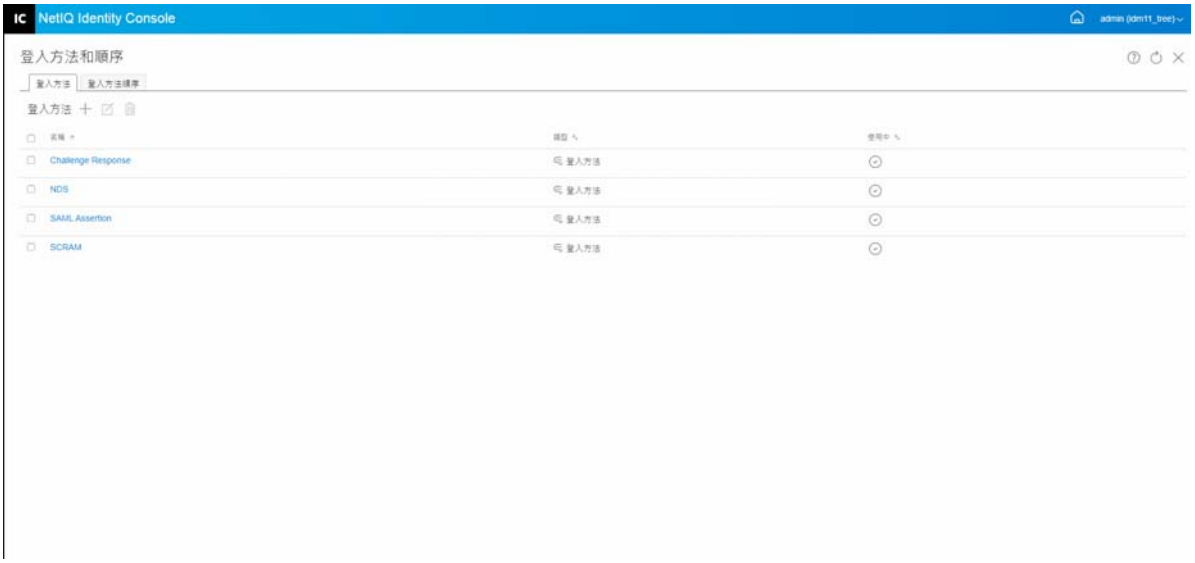
2 選取 「登入方法序列」索引標籤。

3 從清單選取適當登入方法序列，然後按一下 ✓ 圖示。

4 若要取消授權登入方法序列，請選取登入方法序列然後按一下 ⊗ 圖示。

5 或者，您也可以從 「登入方法序列」清單中 「授權」欄底下的下拉式清單，授權或取消授權登入方法序列。

圖 18-6 *授權或取消授權登入方法序列*



設定預設登入方法序列

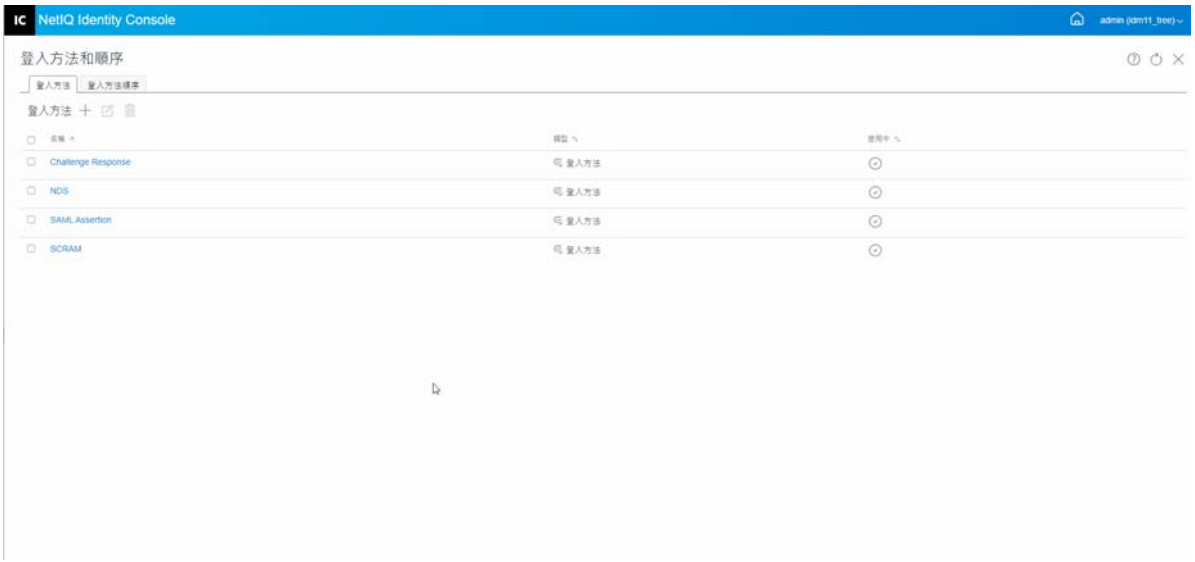
若要設定預設登入序列，讓使用者在登入時不需要指定登入序列：

1 按一下 Identity Console 抵達頁面的 「驗證管理」 > 「登入方法和序列」選項。

2 選取 「登入方法序列」索引標籤。

3 啟用 ✓ 圖示以將授權登入方法序列設定為預設值。

圖 18-7 設定預設登入方法序列

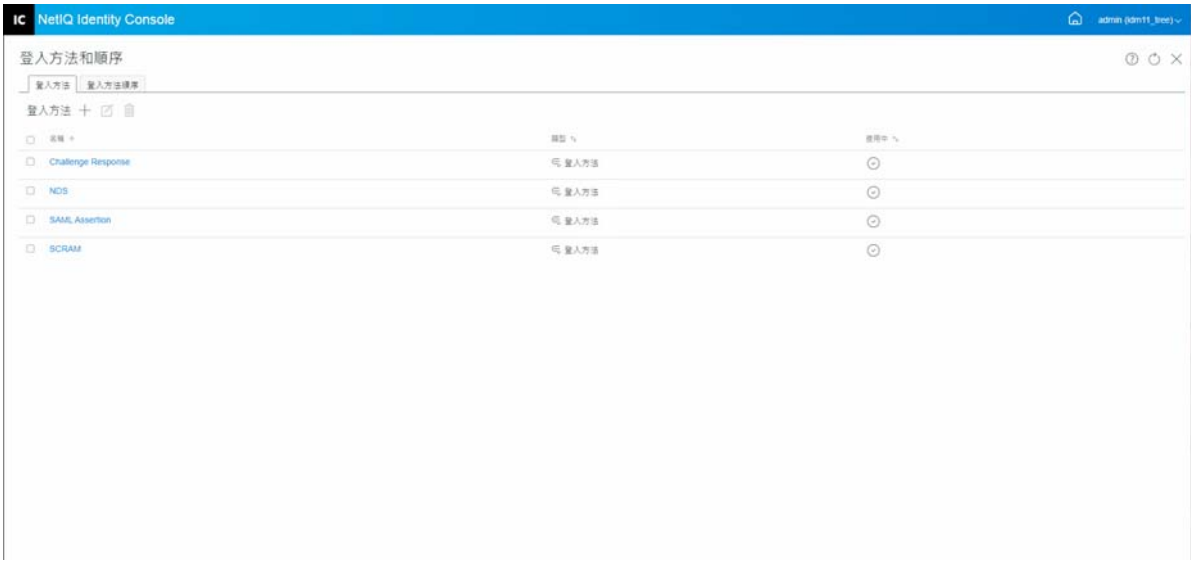


刪除登入方法序列

若要刪除登入方法序列：

1. 按一下 Identity Console 抵達頁面的 「**驗證管理**」 > 「**登入方法和序列**」選項。
2. 選取 「**登入方法序列**」索引標籤。
3. 從清單選取適當登入方法序列，然後按一下 圖示。
4. 按下一個確認畫面中的 「**確定**」。

圖 18-8 刪除登入方法序列



管理密碼規則

密碼規則 (Policy) 是指定建立和取代使用者密碼準則之管理員定義的規則 (Rule) 集合。NMAS 可讓您強制執行您在 eDirectory 中指派給使用者的密碼規則。密碼規則也可以包含 「忘記密碼自助」功能，減少因為忘記密碼而致電服務台的次數。另一個自助功能是 「重設密碼自助」，其可讓使用者在檢視管理員於密碼規則中指定的規則時變更其密碼。使用者透過 Identity Manager 使用者應用程式或 Identity Console 來存取這些功能。

使用密碼規則模組，您可以執行以下任務：

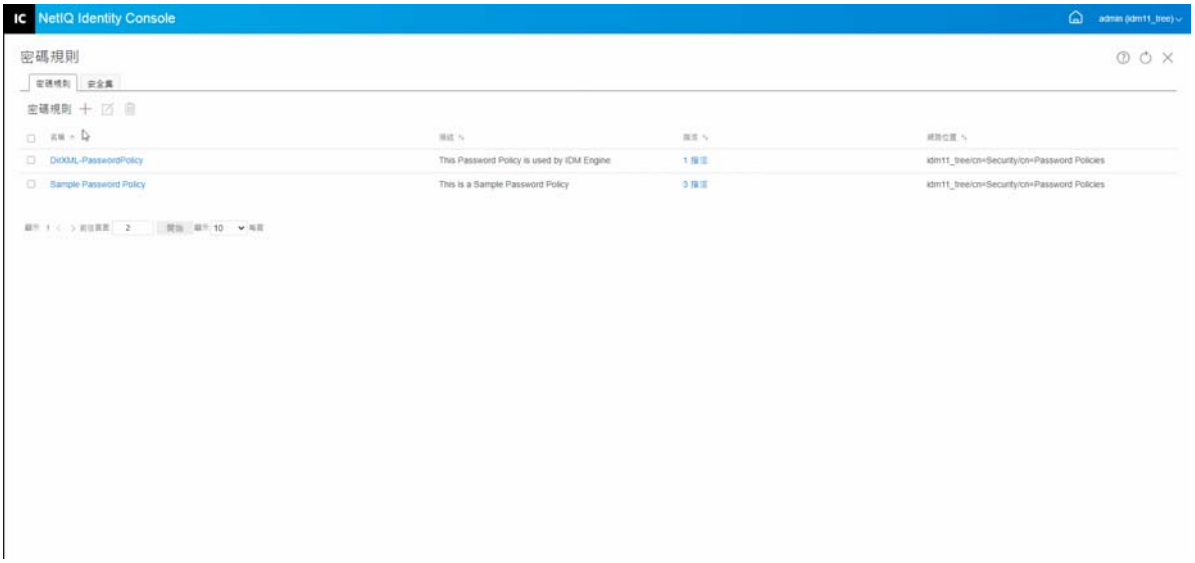
- 「使用預設設定來建立密碼規則」(第 111 頁)
- 「使用自定設定來建立密碼規則」(第 112 頁)
- 「修改密碼規則」(第 114 頁)
- 「刪除密碼規則」(第 115 頁)

使用預設設定來建立密碼規則

若要建立新的密碼規則，請執行下列步驟：

1. 按一下 Identity Console 抵達頁面上的 「**驗證管理**」 > 「**密碼規則**」選項。
2. 按一下 ＋ 圖示以建立新的密碼規則。
3. 在下一個畫面上指定名稱、網路位置、描述和密碼變更訊息。
4. 如果您想要使用預設設定建立密碼規則，請勾選 「**根據預設設定建立新的密碼規則**」方塊，然後按 「**下一步**」以檢視 「**摘要**」頁面。
5. 驗證 「**摘要**」頁面中的詳細資料，然後按一下 「**建立**」。
6. 隨即顯示確認訊息，指出已成功建立密碼規則。

圖 18-9 *使用預設設定來建立密碼規則*



使用自定設定來建立密碼規則

若要使用自定設定來建立密碼規則，請執行以下步驟：

1. 按一下 Identity Console 抵達頁面上的「驗證管理」>「密碼規則」選項。
2. 按一下 ＋ 圖示以建立新的密碼規則。
3. 在下一個畫面上指定名稱、網路位置、描述和密碼變更訊息。
4. 如果您想要使用自定設定來建立密碼規則，請按「下一步」。
5. 在「組態」頁面中執行下列動作：

   5a **啟用通用密碼：**啟用規則的「通用密碼」，可讓您在「密碼規則」功能中使用選項。但是，在為規則啟用通用密碼之前，您必須在環境中符合通用密碼的先決條件。

   5b **啟用進階密碼規則：**此選項會啟用「進階密碼規則」中找到的密碼規則。這些規則可協助您保護您的環境，方法是藉由給予您對於準則的控制權，準則包含密碼生命期間和密碼內容，例如字母、數字、大小寫字母和特殊字元的組合。您可排除您覺得不安全的密碼，如您的公司名稱。

   5c **密碼同步化：**這些選項會決定「通用密碼」在 eDirectory 之中，與其他類型 Identity Vault 密碼同步的方式。密碼同步化包含以下選項：

      5c1 **設定密碼時移除 NDS 密碼：**如果選取此選項，設定通用密碼時將停用 NDS 密碼。使用者無法使用透過 NDS 密碼 (而非與 NMAS 通訊) 直接登入的舊方法或公用程式。如果設定此選項，預設會停用下一個選項「設定密碼時同步化 NDS 密碼」。

      5c2 **設定密碼時同步化 NDS 密碼：**若您選取此選項，Identity Console 等應用程式中的「通用密碼」設定也會變更 NDS 密碼。

      5c3 **設定密碼時同步化簡易密碼：**此選項使用簡易密碼和使用者佈建，提供與 NetIQ 和第三方用戶端的相容性。

      5c4 **設定密碼時同步化配送密碼：**此選項可確定 Metadirectory 引擎是否可以在 eDirectory 中取回或設定使用者的通用密碼。

   5d **通用密碼取回：**可用的選項如下：

      5d1 **允許使用者取回密碼：**允許使用者代辦取回密碼。此選項會決定「已忘記密碼自助服務」是否能代表使用者取回密碼，或可將密碼以電子郵件寄送給使用者。若您未選擇此選項，密碼規則中「已忘記密碼」索引標籤的對應特性會成灰色而無法使用。

      5d2 **允許管理員取回密碼：**若您有特定服務需要此功能的話，請選取此方塊。Identity Manager 不需要管理員取回密碼。但是，某些第三方服務可能會利用此選項。

      5d3 **允許以下人員取回密碼：**藉由按一下 ＋ 圖示，選取應該取回密碼的適當使用者。

   5e **驗證：**

      5e1 **驗證現有密碼是否遵守密碼規則 (在登入時驗證):** 若您正在佈署新密碼規則，或變更現有規則的「進階密碼規則」，且您希望確定現有密碼遵守新的或變更的規則，則此選項非常實用。

若您選取此選項，當使用者登入時，會分析他們的現有密碼，並確認其密碼遵守新的或變更的密碼規則中的 「進階密碼規則」。若現有規則與新規則不符的話，使用者必須變更密碼。

完成之後，請按 **「下一步」**。

6 **「進階密碼規則」**透過讓您控制密碼的生命期間、變更密碼的頻率和密碼包含的內容等密碼詳細資訊，來協助您保護您的環境。

特殊字元為數字 (0-9) 與字母字元以外的字元。

在 「進階密碼規則」頁面中執行以下動作 :

6a 您可以使用 Microsoft 複雜度規則 (先前稱為 Microsoft Windows Server 2008)、Microsoft Server 2008 密碼規則或 Novell 語法，管理密碼語法設定。

6b 在精靈中指定變更密碼、密碼生命期間、密碼長度和構成的必要選項，然後按 **「下一步」**。

7 您可以透過為忘記密碼的使用者啟用 **「忘記密碼」**自助服務，來減少服務台成本。這些自助功能可透過 Identity Console 入口網站提供給使用者。在 「忘記密碼」頁面中執行以下動作 :

附註 : 如果您啟用 「忘記密碼」，則必須同時指定是否需要 「安全集」，以協助使用者登入。

7a **安全集 :** 如果您使用 「安全集」，使用者在回答 「安全集」問題之前無法使用 「忘記密碼」自助服務。若要確定使用者會透過 Identity Console 入口網站收到要輸入此資訊的提示，請選取 **「需要安全集」**選項。

7b **動作 :** 這個索引標籤下的可用選項可讓您的使用者使用 「安全集」和 「通用密碼」來重設密碼，讓目前密碼或密碼提示透過電子郵件傳送，以及顯示密碼提示選項。

7c **驗證 :** 選取 **「強制使用者設定驗證時的安全問題和 / 或提示」**方塊，以確保使用者收到提示，要指定 「安全集」或密碼提示。

完成之後，請按 **「下一步」**。

8 您必須將規則指定至一或多物件，規則才會生效。建議您盡可能將規則指定為網路樹上的最高位置，以簡化管理。密碼規則可以指派給以下物件 :

8a **登入規則物件 :** 我們建議您為樹狀結構中的所有使用者建立預設密碼規則，並且指派至位於安全性容器中的 「登入規則」物件。

8b **身為分割區根部的容器 :** 若您將規則指派至身為分割區根部的容器，則該分割區中的所有使用者，包括子容器中的使用者，都會承襲規則指派。

8c **不是分割區根部的容器 :** 若您將規則指定至不是分割區根部的容器，則僅有該特定容器中的使用者會承襲規則指定。子容器中的使用者不會承襲到規則。

若要將規則套用至非分割區根容器以下的所有使用者，請單獨為各子容器指派規則。

8d **使用者 :** 您可將規則指定至一或多使用者。

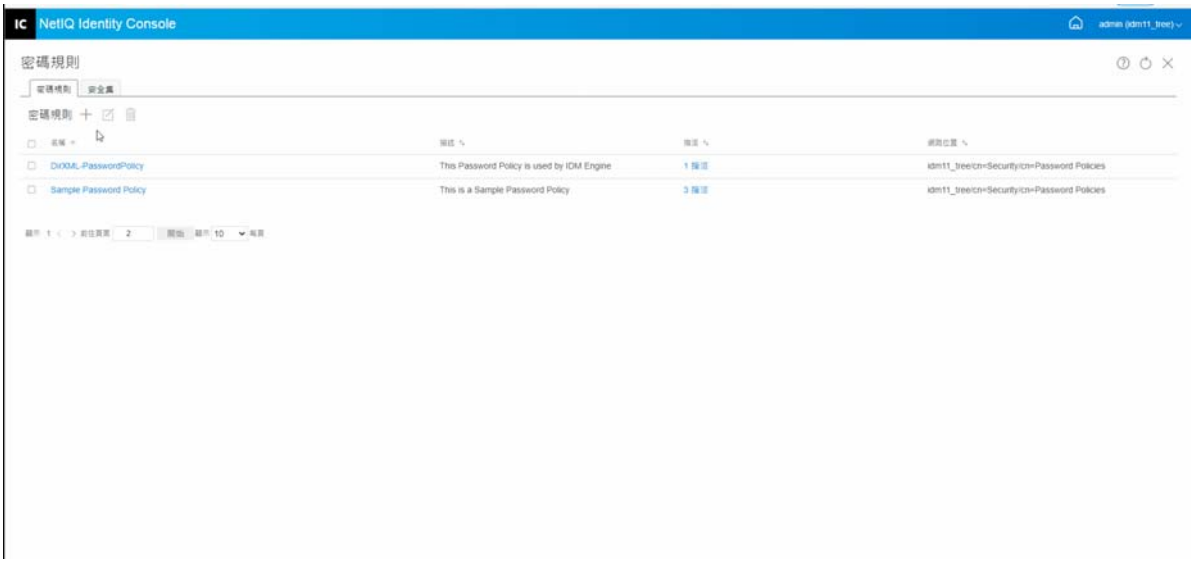
若要指派規則，請按一下 ＋ 圖示。然後瀏覽並選取適當的物件來指派密碼規則。

如果您想要移除規則關聯，請從清單中選取規則並按一下 🗑 圖示。

9 驗證 **「摘要」**頁面中的詳細資料，然後按一下 **「建立」**。

10 隨即顯示確認訊息，指出已成功建立密碼規則。

圖 18-10 使用自定設定來建立密碼規則

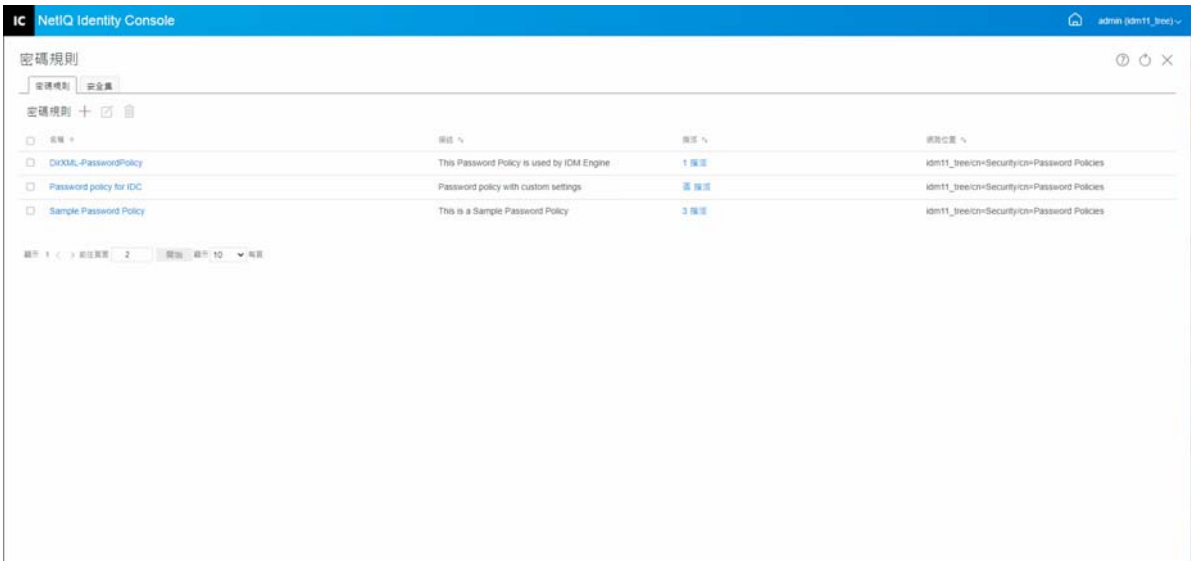


修改密碼規則

若要修改現有密碼規則，請執行以下步驟：

1. 按一下 Identity Console 抵達頁面上的 **「驗證管理」** > **「密碼規則」**選項。
2. 從清單選取適當的「密碼規則」，然後按一下 圖示。
3. 在 **「修改密碼規則」**頁面中進行必要的變更，然後按一下 **「儲存」**。

圖 18-11 修改密碼規則



刪除密碼規則

若要刪除密碼規則，請執行以下步驟：

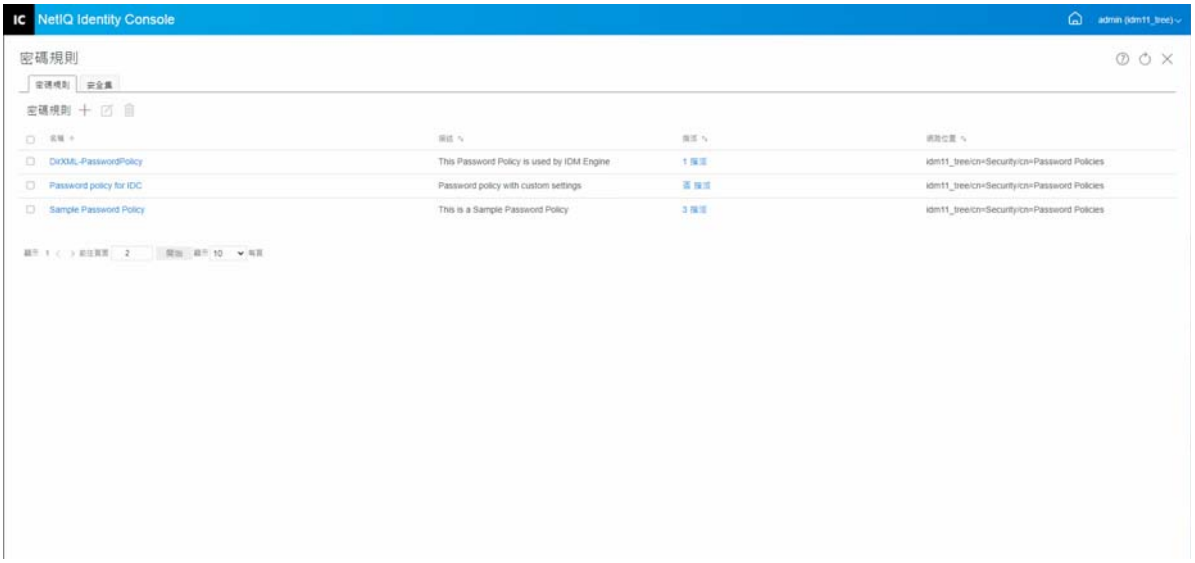
1 按一下 Identity Console 抵達頁面上的「驗證管理」>「密碼規則」選項。

2 從清單選取適當的「密碼規則」，然後按一下 圖示。

3 在接下來的警告畫面上，按一下「確定」。

4 隨即顯示確認訊息，指出已刪除密碼規則。

圖 18-12 刪除密碼規則



管理安全集

「處理安全集」是使用者用來驗證身份識別的一或多個問題。「處理安全集」是「密碼自助服務」的一部分。

當使用者無法記起或使用自己的密碼時，即可使用「密碼自助服務」而不需要呼叫「服務台」。「處理安全集」可讓使用者驗證身份識別，然後透過電子郵件接收提示或密碼，或使用 Web 瀏覽器重設密碼。

您可允許使用者建立並回答自己的問題，或要求使用者回答您建立的問題。

「處理安全集」頁可讓您搜尋現有的處理安全集、建立新處理安全集和編輯現有的處理安全集。

- 「建立新的安全集」(第 116 頁)
- 「修改安全集」(第 116 頁)
- 「刪除安全集」(第 117 頁)

建立新的安全集

若要建立新的安全集，請執行下列步驟：

1 按一下 Identity Console 抵達頁面上的「驗證管理」>「密碼規則」>「安全集」。

2 按一下 ＋ 圖示以建立新的安全集。

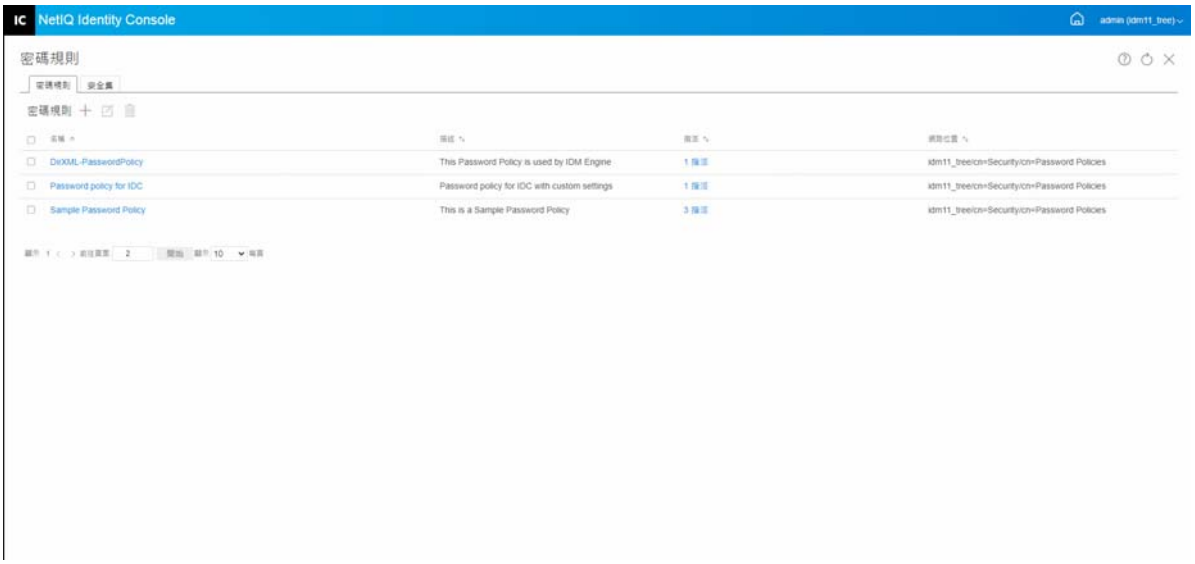
3 指定「安全集」物件的名稱，並選取應該在其中建立安全集的容器或子容器。

4 建立一組新的問題，在取回使用者的密碼時提問。您也可以從現有的隨機問題集中選取。

5 設定要詢問的問題數目，然後按一下「建立」。

6 隨即顯示確認訊息，指出已成功建立安全集。

圖 18-13 建立安全集



修改安全集

若要修改現有的安全集，請執行以下步驟：

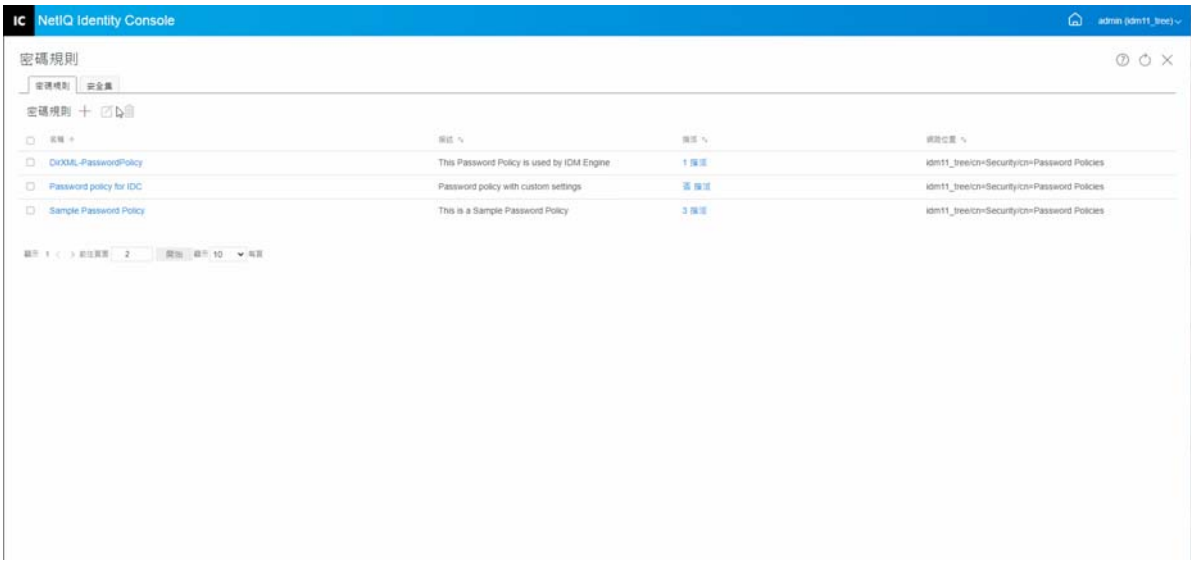
1 按一下 Identity Console 抵達頁面上的「驗證管理」>「密碼規則」>「安全集」。

2 從清單選取適當的「安全集」，然後按一下 圖示。

3 在「修改安全集」頁面中進行必要的變更，然後按一下「儲存」。

4 隨即顯示確認訊息，指出已成功修改安全集。

圖 18-14 修改安全集

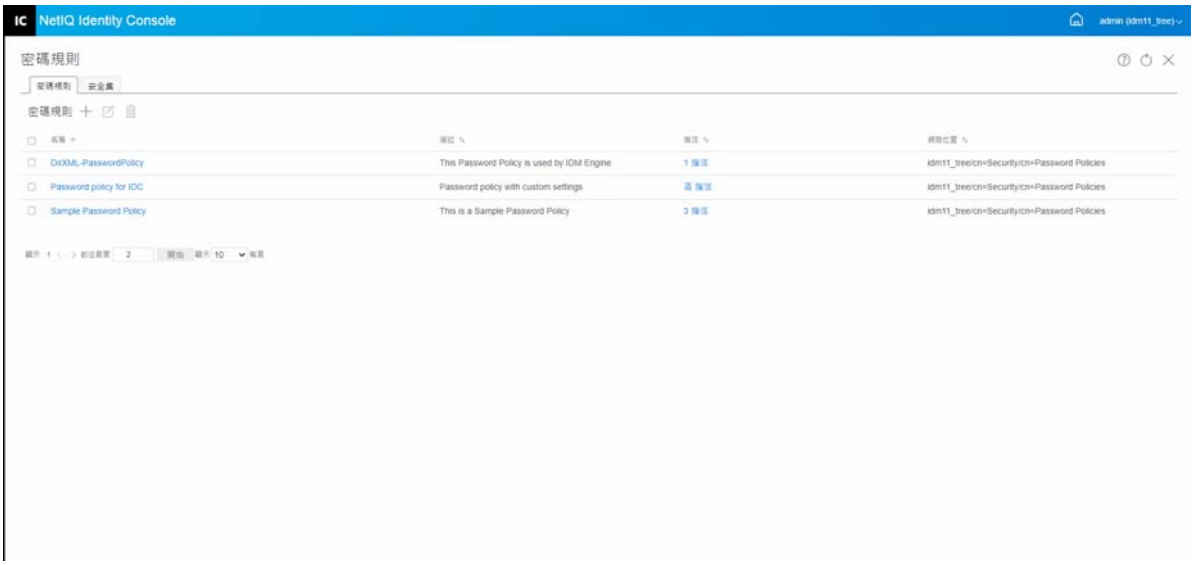


刪除安全集

若要刪除安全集，請執行以下步驟：

1. 按一下 Identity Console 抵達頁面上的 **「驗證管理」** > **「密碼規則」** > **「安全集」**。
2. 從清單選取必要的「安全集」，然後按一下 圖示。
3. 按一下確認畫面上的 **「確定」**。
4. 隨即顯示確認訊息，指出已成功刪除安全集。

圖 18-15 刪除安全集



19 管理 SNMP 群組物件

簡易網路管理協定 (SNMP) 是網際網路的標準操作和維護協定，用於在管理主控台應用程式與管理裝置之間交換管理資訊。

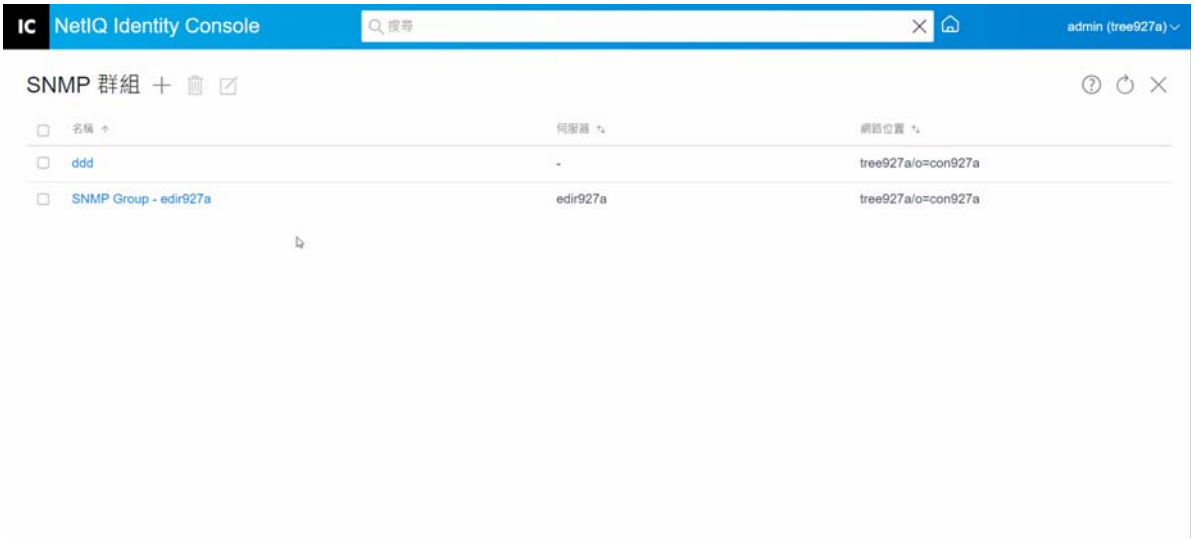
使用 SNMP 模組，您可以執行以下任務：

建立 SNMP 群組物件

若要建立 SNMP 群組物件，請執行以下步驟：

1. 從 Identity Console 抵達頁面按一下 「**SNMP**」模組。
2. 按一下 ＋ 圖示以建立新的 SNMP 群組物件。
3. 指定名稱並選取網路位置以建立新的 SNMP 群組物件。
4. 按一下 「**建立**」按鈕。
5. 隨即在您的螢幕上顯示訊息，確認已成功建立 SNMP 群組物件。

圖 19-1 *建立 SNMP 群組物件*

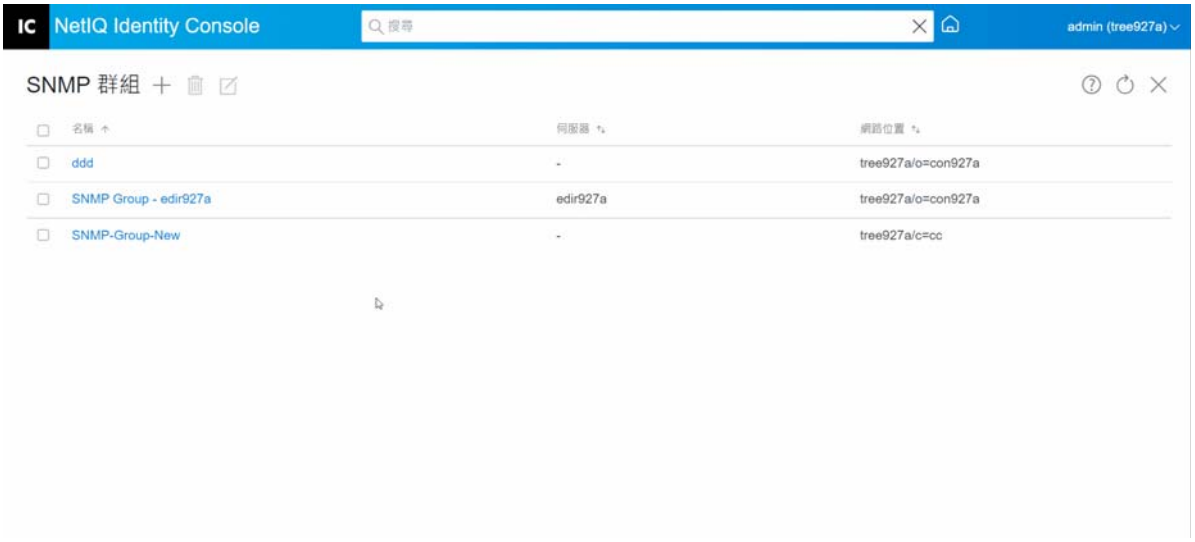


修改 SNMP 群組物件

若要修改 SNMP 群組物件，請執行以下步驟：

1. 從 Identity Console 抵達頁面按一下 「SNMP」模組。
2. 選取要修改的 SNMP 群組物件，然後按一下 圖示。
3. 在 「一般」 / 「設陷」頁面中修改可設定的參數。
4. 完成之後，按一下 「儲存」按鈕。
5. 隨即在您的螢幕上顯示訊息，確認已成功修改 SNMP 群組物件。

圖 19-2 修改 SNMP 群組物件

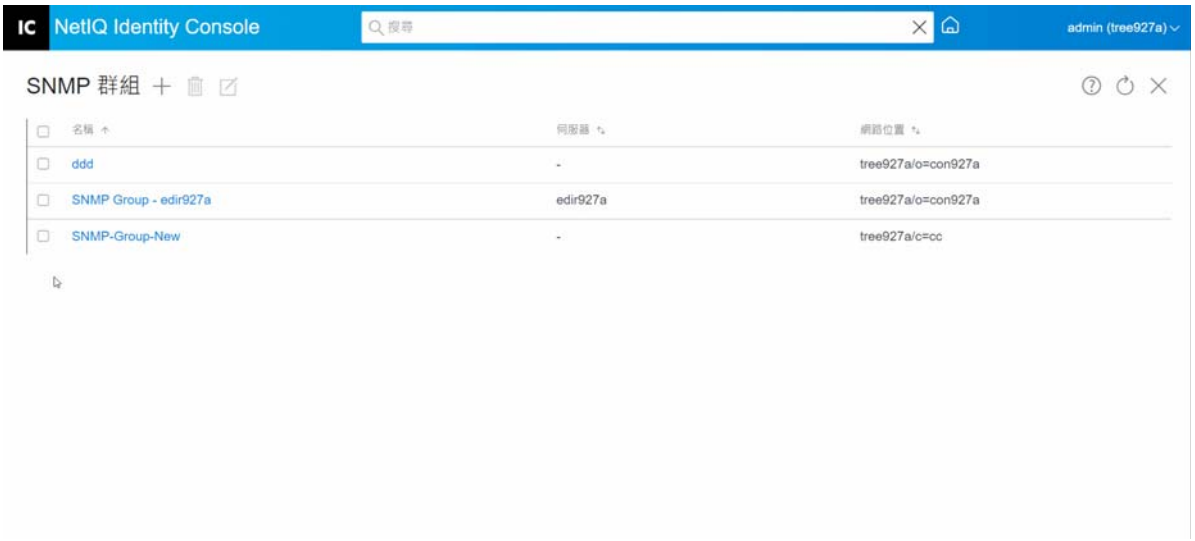


刪除 SNMP 群組物件

若要刪除 SNMP 群組物件，請執行以下步驟：

1. 從 Identity Console 抵達頁面按一下 「SNMP」模組。
2. 選取要修改的 SNMP 群組物件，然後按一下 圖示。
3. 按下一個畫面中的 「確定」。
4. 隨即在您的螢幕上顯示訊息，確認已成功刪除 SNMP 群組物件。

圖 19-3 刪除 SNMP 群組物件



20 管理增強性背景驗證

若要從 Identity Console 的 EBA 外掛程式存取 eDirectory，您的樹狀結構中必須有一個已啟用 EBA 的伺服器，其中包含有效的 eba.p12 檔。如需如何在 eDirectory 樹狀結構上啟用 EBA 的詳細資訊，請參閱 NetIQ eDirectory 管理指南中的*在 eDirectory 樹狀結構上啟用 EBA*。

附註：如果您想要搭配使用 EBA 模組與 Identity Console，則必須將您的 eDirectory 伺服器升級至 9.2.4 HF2。

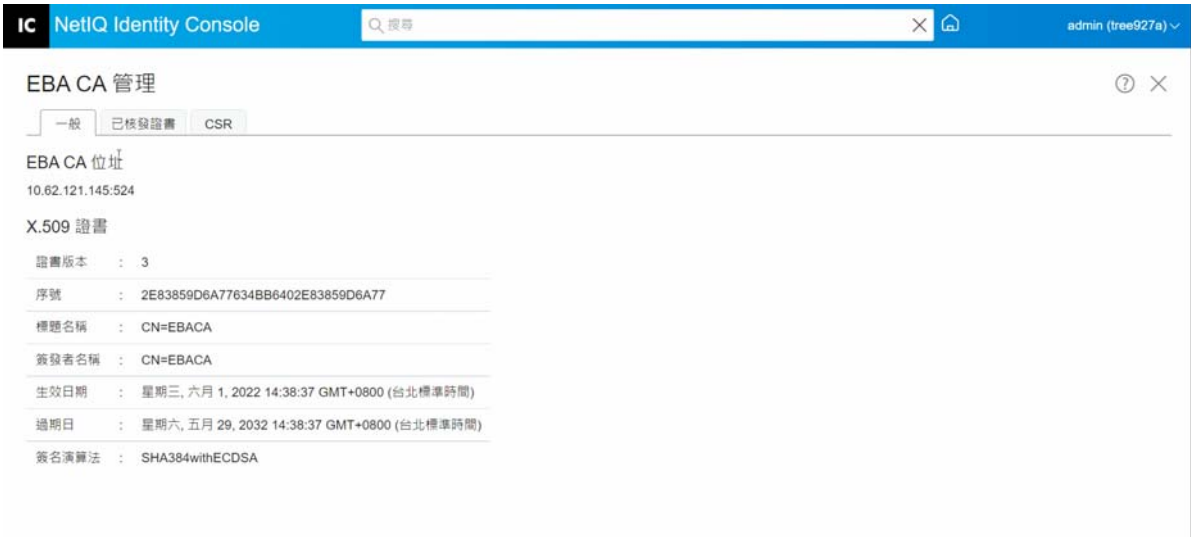
若要開啟 EBA CA 管理頁面，請登入 Identity Console 入口網站，然後按一下 **EBA** 模組。

EBA CA 管理頁面包括下列索引標籤，以管理不同的 EBA CA 層面：

- **一般**： 顯示 EBA CA 的 IP 位址及其證書。
- **證書已發行 :** 將 NCP CA 證書和其 IP 位址與連接埠一併顯示。

  若要撤銷證書，請選取該證書，然後按一下 ⊘。只有在極端情況下才使用此選項，因為擁有 NCP CA 證書的伺服器將會在您撤銷其證書時變成無作用。通常，伺服器遭到破壞時，需要撤銷證書。
- **CSR:** 列出待處理證書登記申請，以供管理員進行核准。若要核准證書登記申請，請從清單中選取證書，然後按一下「**核准**」。

圖 20-1 *管理增強性背景驗證*



II 使用 Identity Console 管理 Identity Manager

本節描述了您可以執行的各種任務，以使用 Identity Console 入口網站管理您的 Identity Manager 伺服器。

21 管理驅動程式和驅動程式集

驅動程式集是一個可容納多個 Identity Manager 驅動程式的容器。一次只能有一個驅動程式集在伺服器上處於使用中狀態。因此，所有使用中的驅動程式必須組成相同的驅動程式集。驅動程式集可以使用「設計工具」工具來建立。如需詳細資訊，請參閱《*NetIQ Designer for Identity Manager Administration Guide*》(NetIQ Designer for Identity Manager 管理指南) 中的 Configuring Driver Sets(設定驅動程式集)。

新增或刪除伺服器

驅動程式集一次只能關聯至一或多部伺服器。但是，根據您的要求，您可以將不同的驅動程式集物件關聯到可用的伺服器。

若要新增新的伺服器，請按一下特定驅動程式集物件上的 圖示 > 選取 **「新增伺服器」**，然後從內容瀏覽器中選取適當的伺服器。

若要刪除現有伺服器，請選取 **「移除伺服器」**選項。

圖 21-1 將伺服器新增至驅動程式集

使用啟用碼啟動驅動程式集

在使用任何驅動程式集和驅動程式集內的驅動程式之前，您必須使用在您的電子郵件 ID 中收到的啟用代碼來啟動。購買授權之後，您會從 NetIQ 收到啟用代碼。使用您的啟用代碼執行以下步驟以啟動驅動程式集：

1 按一下 Identity Console 主畫面上的 「IDM 管理」索引標籤。

2 按一下您想要啟動的特定驅動程式集方塊上的 「動作」圖示 ，然後按一下 「啟動安裝」。

套用 「啟動」時，「IDM 管理」磚中的每個驅動程式集索引標籤都會顯示與該驅動程式集關聯的所有伺服器啟動資訊。此資訊有助於識別啟動何時到期。

3 如果您已在電腦上下載啟動檔案，則選取 「選取包含身分證明的檔案」核取方塊。

4 瀏覽並選取啟動檔案，然後按一下 「提交」。

5 或者，您可以使用啟動檔案的內容啟動驅動程式集。選取 「輸入身分證明」核取方塊。

5a 開啟 「產品啟用身分證明」檔案，然後將 「產品啟用身分證明」的內容複製到簡貼簿。

5b 如果您選擇複製內容，請不要包含任何多餘的行或空格。您應該從身分證明的第一個破折號 (-) 開始複製 (----BEGIN PRODUCT ACTIVATION CREDENTIAL)，一直複製到最後一個破折號 (-) (END PRODUCT ACTIVATION CREDENTIAL-----)，然後按一下 「完成」。

6 隨即顯示確認訊息，指出已成功啟動驅動程式集。

圖 21-2 啟動驅動程式集

檢視驅動程式集的啟動資訊

啟動驅動程式集之後，您必須驗證驅動程式集已成功啟動。若要驗證，請執行以下步驟：

1. 按一下 Identity Console 主畫面上的「**IDM 管理**」索引標籤。
2. 按一下您想要驗證其啟動資訊之特定驅動程式集物件上的「動作」圖示 ⋮，然後按一下「**啟動資訊**」。
3. 啟動相關資訊視窗會快顯在您的電腦上。您可以驗證此頁面上特定驅動程式集的啟動詳細資料。

圖 21-3 檢視驅動程式集的啟動資訊

啟動和停止驅動程式

建立驅動程式時，預設會停止。若要讓驅動程式運作，您必須啟動驅動程式。Identity Manager 是事件驅動的系統，因此在驅動程式啟動之後，在發生事件之前會閒置。執行以下步驟以啟動 / 停止驅動程式。

1 按一下 Identity Console 主畫面上的 「IDM 管理」索引標籤。

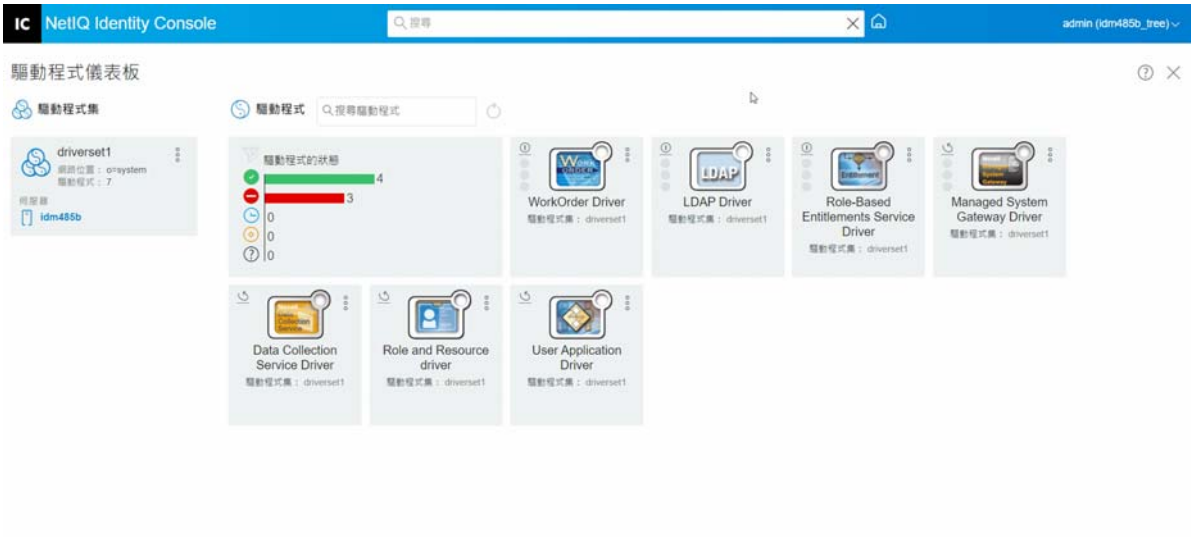
2 按一下您電腦螢幕右側的特定驅動程式集物件，以顯示與其相關聯的所有驅動程式。

3 按一下特定驅動程式上的 「動作」圖示 ，然後選取 「啟動驅動程式」。

4 若要停止驅動程式物件，請按一下特定驅動程式上的 「動作」圖示 ，然後選取 「停止驅動程式」。

5 (選擇性) 另外，您可以同時啟動或停止位於相同驅動程式集物件內的所有驅動程式。按一下驅動程式集物件上的 「動作」圖示 ，然後選取 「啟動所有驅動程式」或 「停止所有驅動程式」。

圖 21-4 啟動和停止驅動程式



搜尋驅動程式

Identity Console 提供選項，可以在您的伺服器中搜尋特定驅動程式。若要搜尋驅動程式，請執行以下步驟：

1 按一下 Identity Console 主畫面上的 「IDM 管理」索引標籤。

2 在 「搜尋」方塊中指定驅動程式的名稱。特定驅動程式物件會顯示在您的電腦螢幕上。您也可以按一下 圖示來重新整理驅動程式清單。

圖 21-5 搜尋驅動程式

篩選驅動程式和驅動程式集

驅動程式可以根據其在「IDM 管理」頁面上的狀態進行篩選。若要篩選驅動程式：

1. 按一下 Identity Console 主畫面上的「IDM 管理」索引標籤。
2. 按一下「驅動程式狀態」磚上的下列圖示，根據其狀態篩選驅動程式：
   - 按一下 圖示以篩選您的伺服器中的所有執行中驅動程式。
   - 按一下 圖示以篩選您的伺服器中的所有已停止驅動程式。
   - 按一下 圖示以篩選已啟動的所有驅動程式。
   - 按一下 圖示以篩選已停止的所有驅動程式。
   - 按一下 圖示以篩選出沒有相關聯狀態的那些驅動程式。當驅動程式集沒有相關聯的伺服器時，位於該驅動程式集中的驅動程式會顯示「未知」狀態。

   若要清除針對驅動程式套用的任何篩選器，請按一下可以在「驅動程式狀態」磚上看到的 圖示。
3. 也可以使用 Identity Console 入口網站篩選驅動程式集。根據預設，Identity Console 入口網站會顯示與您的伺服器中所有驅動程式集相關聯的所有驅動程式。如果您想要檢視特定驅動程式集底下的驅動程式，您必須從 Identity Console 入口網站左側的驅動程式集清單選取適當的驅動程式集。若要清除驅動程式集選項，請再次按一下選取的驅動程式集。

圖 21-6 篩選驅動程式和驅動程式集

刪除驅動程式集

若要刪除驅動程式集，請執行下列步驟：

1 按一下 Identity Console 主畫面上的「**IDM 管理**」索引標籤。

2 按一下您要刪除之適當驅動程式集上的動作按鈕 ⋮。

3 選取「**刪除**」。

驅動程式動作

按一下個別驅動程式磚上的動作圖示 ⋮，以支援下列動作：

- **啟動驅動程式**：啟動驅動程式
- **停止驅動程式**：停止驅動程式
- **重新啟動驅動程式**：重新啟動已停止的驅動程式
- **刪除驅動程式**：刪除驅動程式
- **統計資料**：檢視驅動程式的效能統計資料
- **複製資料**：將驅動程式的資料從一部伺服器複製至另一部伺服器。此選項僅適用於多伺服器環境。

22 管理驅動程式集內容

本節提供有關所有驅動程式集常見內容的資訊。這包括所有內容 (具名密碼、記錄層級、驅動程式集審查器等等)。

本節分為以下幾個類別 :

設定驅動程式集

若要修改驅動程式集的組態，請執行以下步驟 :

1 按一下「IDM 管理」> 按一下適當驅動程式集的內容功能表 (三個點) >「驅動程式集內容」。

2 根據預設，「驅動程式集組態」頁面隨即顯示。驅動程式集組態選項分為以下類別 :

具名密碼

Identity Manager 允許您安全地儲存驅動程式集的多個密碼。此功能稱為具名密碼。每個不同的密碼可以透過金鑰或名稱進行存取。

您可以對驅動程式集或個別驅動程式新增具名密碼。驅動程式集的具名密碼適用於集合中的所有驅動程式。

若要在驅動程式規則中使用具名密碼，請依密碼名稱來參考密碼，而不是使用實際的密碼，Identity Manager 引擎會將密碼傳送給驅動程式。本節中所述的儲存和取回具命密碼的方法，可用於任何驅動程式，不需要對驅動程式 Shim 進行任何變更。

藉由選取「IDM 管理」> 按一下適當驅動程式集的內容功能表 (三個點) >「驅動程式集內容」>「驅動程式集組態」底下的「具名密碼」，來存取「具名密碼」。

若要新增具名密碼，請按一下 ＋ 圖示。若要移除現有的具名密碼，請選取適當的密碼然後按一下 圖示。

全域組態值

顯示「全域組態」物件的排序清單。物件包含驅動程式的延伸 GCV 定義，Identity Manager 會在驅動程式啟動時載入。您可以新增或移除「全域組態」物件，且您可以變更物件的執行順序。按一下 圖示以儲存 GCV。若要重新整理 GCV 的清單，請按一下 圖示。

設定 Java 環境參數

若要設定 Java 環境參數，請執行以下步驟：

1. 在 Identity Console 中，選取 **「IDM 管理」** > **按一下適當驅動程式集的內容功能表 (三個點)** > **「驅動程式集內容」**。
2. 按一下 **「驅動程式集組態」**底下的 **「Java 環境參數」**，以顯示其中包含 Java 環境參數的內容頁面。
3. 視需要修改下列設定：

   類別路徑增加部分：指定 JVM 要在其中搜尋套件 (.jar) 和類別 (.class) 檔案的其他路徑。使用此參數，與使用 java -classpath 指令相同。輸入多個類別路徑時，如果是 Windows JVM，請用分號 (;) 隔開，如果是 UNIX 或 Linux JVM，則請用冒號 (:) 隔開。

   JVM 選項：指定其他與 JVM 搭配使用的選項。請參閱 JVM 文件，以取得有效的選項。

   DHOST_JVM_OPTIONS 是對應的環境變數。其指定了 JVM 1.2 的引數，例如：

   -Xnoagent -Xdebug -Xrunjdwp: transport=dt_socket,server=y, address=8000

   每個選項字串都以空白字元隔開。如果選項字串包含空白字元，則必須將其以雙引號括住。

   驅動程式集屬性選項優先於 DHOST_JVM_OPTIONS 環境變數。此環境變數附加在驅動程式集屬性選項的末尾。

   啟始堆積大小：指定 JVM 可用的啟始 (最小) 堆積大小。增加啟始堆積大小可以改善啟動時間和生產量效能。使用數值，後面接續著 G、M 或 K。如果未指定字母大小，則大小預設為位元組。使用此參數，與使用 java -Xms 指令相同。

   DHOST_JVM_INITIAL_HEAP 是對應的環境變數。以十進位位元組數字指定啟始 JVM 堆積大小。其優先於驅動程式集屬性選項。

   如需 JVM 預設啟始堆積大小的相關資訊，請參閱 JVM 文件。

   最大堆積大小：指定 JVM 可用的最大堆積大小。使用數值，後面接續著 G、M 或 K。如果未指定字母大小，則大小預設為位元組。使用此參數，與使用 java -Xmx 指令相同。

   DHOST_JVM_MAX_HEAP 是對應的環境變數。以十進位位元組數字指定最大 JVM 堆積大小。其優先於驅動程式集屬性選項。

   如需 JVM 預設最大堆積大小的相關資訊，請參閱 JVM 文件。

4 按一下 以儲存變更。

5 重新啟動 Identity Vault 以套用變更。

管理值屬性清單

若要將屬性新增至特定 「驅動程式集」的值屬性清單，請執行下列步驟：

1 在 Identity Console 中，選取**物件管理**模組。

2 從下拉式清單中選取 **DirXML-DriverSet** 類型，然後按一下 「搜尋」按鈕。

3 從搜尋清單中按一下適當的驅動程式集。

4 若要將無值屬性新增至屬性值清單，請按一下 **「值屬性」**旁邊的 圖示，並從清單中選取適當的無值屬性。

5 完成之後，請按一下 **「確定」**。

圖 22-1 *管理驅動程式集組態參數*

管理驅動程式集的工作

Identity Console 可讓您使用 「工作」選項為個別驅動程式集內的所有驅動程式排程事件。

「工作排程器」頁面包括工作名稱、工作為啟用或停用、排程執行工作的時間、和工作描述。按一下工作名稱以帶出 「工作」頁面。按一下 「已啟用」欄下的啟用 / 停用圖示，以啟用或停用工作。按一下工作描述以查看工作的完整描述。

藉由選取 Identity Console 主要頁面的 **「IDM 管理」** > **按一下適當驅動程式集的內容功能表 (三個點)** > **「驅動程式集內容」** > **「進階」**索引標籤，存取 「工作」頁面。「工作」索引標籤中有一個表格，會顯示選定驅動程式的現有工作物件 (驅動程式會在 「驅動程式」項目中以完整可辨識名稱列出)。

「工作排程器」頁面允許您執行以下任務：

- **建立工作**：按一下  圖示以建立新工作。

  在 **「新工作」**快顯中，若要建立新工作，請執行以下步驟：

  1. 指定工作名稱。
  2. 選取工作類型。
  3. 按一下  圖示，然後從可用伺服器清單中選取要執行工作的伺服器。否則，請指定伺服器名稱，然後選取伺服器。
  4. 按一下 「建立」按鈕。
- **啟動工作**：按一下工作左邊的方塊以選取該工作，再按一下  圖示。
- **停止工作**：按一下工作左邊的方塊以選取該工作，再按一下  圖示。
- **啟用工作**：按一下工作左邊的方塊以選取該工作，再按一下  圖示。
- **停用工作**：按一下工作左邊的方塊以選取該工作，再按一下  圖示。
- **取得狀態**：按一下工作左邊的方塊以選取該工作，再按一下 圖示。
- **刪除工作**：按一下工作左邊的方塊以選取該工作，再按一下  圖示。

按一下工作，以存取 **「工作內容」**頁面。您可在此設定您希望如何執行工作。

一般：顯示工作的 Java 類別名稱。使用此頁面啟用或停用工作、在執行後刪除工作、選取應執行工作的伺服器、指定電子郵件伺服器，並賦予工作不同的顯示名稱與描述。

排程：可讓您設定希望執行工作的時間。指定「啟動工作於」以設定時間，以及是否每天、每週、每月、每年執行工作。您也可以自定要執行工作的時間，或選擇啟用切換開關以手動執行工作。

範圍：可讓您定義此工作適用的物件。物件可以是容器、動態群組、群組，或葉物件。按一下「新增」，選取您希望套用此工作的物件。您可使用「瀏覽」按鈕選取物件，再按一下「確定」。若要從範圍清單中移除物件，請按一下 DN 物件左側方塊選取範圍物件，再按一下「移除」。

新增物件時，請選取物件以顯示更多選項。若您選取群組物件，則可選擇將工作套用至群組成員，或僅套用至群組。若您選取容器物件，可選擇將工作套用到容器內所有的下階物件、容器中所有子物件，或僅套用至容器。

參數：可讓您將其他參數新增至工作，並檢視參數目前設定的狀況。根據所選取的工作類型而定，這些參數也有所變更。

結果：可讓您定義要如何處理工作結果。「結果」頁面分為兩部份：「中介結果」與「最終結果」，所允許的結果有：成功、警告、錯誤和中止。「結果」欄的右邊為「動作」欄。按一下「動作」欄，可讓您設定通知各結果的方式。「動作」包括完成結果時寄送稽核結果或寄送電子郵件。若您未選擇選項，則不會對結果進行任何動作。

在 **「追蹤」**索引標籤中，您可以為特定驅動程式設定追蹤。如需詳細資訊，請參閱 「設定追蹤層級」(第 162 頁)

管理特定驅動程式集的程式庫

程式庫物件會儲存由一或多個驅動程式共用的多個規則和其他資源。程式庫物件可以在驅動程式集物件或任何 eDirectory 容器中建立。多個程式庫可以存在於 eDirectory 網路樹中。只要執行驅動程式的伺服器保留程式庫物件的讀取 / 寫入或主複製本，驅動程式可以參考網路樹中的程式庫。

樣式表、規則 (Policy)、規則 (Rule) 和其他資源物件可以儲存在程式庫中，並由一或多個驅動程式參考。

使用程式庫管理模組，您可以執行以下任務：

- 「檢視和刪除現有程式庫」(第 137 頁)
- 「從程式庫檢視和刪除物件」(第 137 頁)

檢視和刪除現有程式庫

若要檢視和刪除現有程式庫，請執行以下步驟：

1. 在 Identity Console 中，選取「**IDM 管理**」>**按一下適當驅動程式集的內容功能表 (三個點)** >「**驅動程式集內容**」>「**進階**」>「**程式庫**」。
2. 從清單中選取適當的程式庫。
3. 按一下 圖示。按一下**確定**以確認。

從程式庫檢視和刪除物件

您可以從程式庫物件檢視和刪除規則和對應表。若要刪除物件，請執行以下步驟：

1. 在 Identity Console 中，選取「**IDM 管理**」>**按一下適當驅動程式集的內容功能表 (三個點)** >「**驅動程式集內容**」>「**進階**」>「**程式庫**」。
2. 從清單中按一下適當的程式庫。
3. 若要刪除規則，請選取「**規則**」索引標籤。
4. 從清單選取適當的規則，然後按一下 圖示。
5. 若要刪除對應表，請選取「**對應表**」索引標籤。
6. 從清單選取適當的對應表，然後按一下 圖示。
7. 按一下**確定**以確認。

圖 22-2 管理驅動程式集的工作和程式庫

設定驅動程式集的記錄和追蹤層級。

若要為您的驅動程式集設定記錄和追蹤，請從 Identity Console 主要頁面選取 **「IDM 管理」** > **按一下適當驅動程式集的內容功能表 (三個點)** > **「驅動程式集內容」** > **「記錄和追蹤組態」**索引標籤。本節分為以下幾個類別：

- 「設定記錄層級」 (第 138 頁)
- 「設定追蹤層級」 (第 139 頁)
- 「追蹤 DirXML 程序檔」 (第 140 頁)

設定記錄層級

每個驅動程式集都有記錄層級欄位，您可以在其中定義應該追蹤的錯誤層級。此處指定的層級決定要納入記錄的訊息。依照預設，已設定記錄層級以追蹤錯誤訊息 (這也包括嚴重訊息)。若要追蹤其他訊息類型，請變更記錄層級。若要設定記錄層級，請在 Identity Console 中選取 **「IDM 管理」** > **按一下適當驅動程式集的內容功能表 (三個點)** > **「驅動程式集內容」** > **「記錄和追蹤組態」** > **「記錄層級」**。下表描述記錄層級設定：

選項	描述
關閉記錄至 「驅動程式集」、「訂閱者」和 「發行者」記錄。	關閉驅動程式集物件、「訂閱者」通道和 「發行者」通道上所有驅動程式的所有記錄。
記錄中的最大項目數 (50-500)	記錄中的項目數。預設值為 50。

選項	描述
記錄層級	可以選取以下記錄層級： ◆ 記錄錯誤：只記錄錯誤 ◆ 記錄錯誤和警告：記錄錯誤和警告 ◆ 記錄特定事件：記錄已選取的事件。選取此選項可啟用以下事件清單： ◆ Metadirectory 引擎事件 ◆ 狀態事件 ◆ 操作事件 ◆ 轉換事件 ◆ 身分證明佈建事件 ◆ 僅更新上次記錄時間：更新上次記錄時間。 ◆ 關閉記錄：關閉驅動程式的記錄。

設定追蹤層級

您可以為特定驅動程式集設定追蹤。根據為驅動程式集指定的追蹤層級，追蹤會在引擎處理事件時顯示驅動程式相關事件。驅動程式追蹤層級僅影響已設定追蹤的驅動程式或驅動程式集。如果您正在使用遠端載入器，遠端載入器追蹤檔案將直接設定在遠端載入器上，並且僅包含驅動程式 Shim 追蹤。

若要設定驅動程式集的追蹤，請選取 **「IDM 管理」** > **按一下適當驅動程式集的內容功能表 (三個點)** > **「驅動程式集內容」** > **「記錄和追蹤組態」** > **「追蹤」**索引標籤。下表描述追蹤設定：

參數	驅動程式
追蹤層級	隨著驅動程式追蹤層級增加，在 「追蹤」中顯示的資訊量也會增加。 追蹤層級一顯示錯誤，但不會顯示錯誤原因。如果您想要查看密碼同步化資訊，請將追蹤層級設為五。 如果您選取 **「使用驅動程式集的設定」**，則會採用驅動程式集的值。
XSL 追蹤層級	追蹤」會顯示 XSL 事件。只有在疑難排解 XSL 樣式表時才設定此追蹤層級。如果您不想要查看 XSL 資訊，請將層級設為零。
Java 除錯埠	允許開發人員連接 Java 除錯程式。附加 Java 除錯程式之後，重新啟動 Identity Vault。
追蹤檔案	為選取的驅動程式指定寫入 Identity Manager 資訊所在的檔案名稱和位置。 如果您選取 **「使用驅動程式集的設定」**，則會採用驅動程式集的值。

參數	驅動程式
追蹤檔案編碼	追蹤檔案會使用系統的預設編碼。您可以依需要指定另一種編碼。 如果您選取 「使用驅動程式集的設定」，則會採用驅動程式集的值。
追蹤檔案大小限制	允透設定 Java 追蹤檔案的限制。如果您將檔案大小設為沒有限制，則檔案大小會一直增加，直到沒有剩餘的磁碟空間為止。 **附註：**如果指定了檔案大小限制，則會在多個檔案中建立追蹤檔案。Identity Manager 會自動將最大檔案大小除以 10，並且建立 10 個個別檔案。這些檔案的合併大小等於最大追蹤檔案大小。 如果您選取 「使用驅動程式集的設定」，則會採用驅動程式集的值。

追蹤 DirXML 程序檔

「DirXML 程序檔追蹤」選項可讓您選取驅動程式集的追蹤層級。選項會套用到驅動程式集中的所有規則。可以選取下列 DirXML 程序檔追蹤選項：

- 所有 DirXML 程序檔追蹤開啟
- 所有 DirXML 程序檔追蹤關閉
- DirXML 程序檔規則追蹤開啟
- DirXML 程序檔規則追蹤關閉

按一下 以儲存變更。

圖 22-3 *管理驅動程式集的記錄和追蹤層級*

管理驅動程式集審查器和統計資料

您可以使用驅動程式集審查器以檢視與驅動程式集相關聯之物件的詳細資訊。本節分為以下幾個類別：

檢視驅動程式集統計資料

您可以使用 Identity Console 入口網站來檢視單一驅動程式或整個驅動程式集的各種統計資料。這包括各種依據類別 (新增、移除、修改等等) 的統計資料，例如快取檔案大小、快取檔案中未處理交易的大小、最舊和最新的交易，以及未處理交易的總數。若要檢視驅動程式集統計資料：

1 在 Identity Console 中，選取 **「IDM 管理」** > **按一下適當驅動程式集的內容功能表 (三個點)** > **「驅動程式集內容」** > **「審查器和統計資料」** > **「統計資料」**。

2 從下拉式清單中選取適當的伺服器。

隨即顯示一個頁面，允許您檢視驅動程式集中包含的所有驅動程式的統計資料。

- 若要重新整理統計資料，請按一下 圖示。
- 若要關閉驅動程式的統計資料，請按一下驅動程式統計資料視窗右上角的 按鈕。
- 若要開啟所有驅動程式的統計資料，請按一下 **「動作」** > **「全部顯示」**。
- 若要收合驅動程式未處理交易的清單，請按一下位於清單上方的 按鈕。若要收合所有驅動程式未處理交易的清單，請按一下 **「動作」** > **「收合所有交易」**。
- 若要展開交易的清單，請按一下 按鈕。若要展開所有驅動程式未處理交易的清單，請按一下 **「動作」** > **「展開所有交易」**。
- 若要關閉已停用驅動程式的統計資料儀表板，請按一下 **「動作」**，然後選取 **「關閉停用的驅動程式」**。

檢視版本資訊

Identity Manager 引擎、驅動程式 Shim 和驅動程式組態檔案分別包含個別版本號碼。Identity Console 中的 「版本探查」工具可協助您尋找 Identity Manager 引擎的版本和驅動程式 Shim 版本。驅動程式組態檔案包含自己的命名慣例。若要檢視版本資訊：

1 在 Identity Console 中，選取 **「IDM 管理」** > **按一下適當驅動程式集的內容功能表 (三個點)** > **「驅動程式集內容」** > **「審查器和統計資料」** > **「版本探查」**。

2 檢視版本設定資訊的最上層顯示：

- 您已通過驗證的 eDirectory 網路樹

附註：eDirectory 在 Identity Manager 環境中使用時稱為 Identity Vault。

- 您所選的驅動程式集
- 與驅動程式集關聯的伺服器

  若驅動程式集與兩個或多個伺服器相關聯，您可檢視各伺服器的 Identity Manager 資訊。
- 驅動程式

3 按一下 **「檢視」**圖示 以顯示最上層檢視中所含之相同資訊的文字表達。

4 按一下 「輸出」按鈕 以將文字輸出並儲存至您本機或網路磁碟機上的檔案。

檢視關聯統計資料

藉由使用 Identity Manager 關聯統計資料功能，您可以尋找 Identity Manager 管理之身分識別的關聯詳細資料。Identity Manager 會使用關聯統計資料來取得 Identity Manager 驅動程式的關聯計數。

若要取得驅動程式的作用中、非作用中和系統受管理物件，請執行關聯統計資料工作。您可以依照每日、每週、每月或每年的基礎，排程關聯統計資料工作。根據預設，工作會排程為每週執行。

「關聯統計資料」儀表板會顯示關聯詳細資料。或者，您可以藉由將關聯輸出到檔案來檢視詳細資訊。

附註：

- 每部伺服器的驅動程式關聯計數。如果物件與多個驅動程式關聯，則會單獨為每個驅動程式計算關聯計數。
- 如果您有超過 200,000 個關聯，我們建議您將驅動程式的最大堆積大小設為 2 GB 以上。如需有關設定堆積大小的詳細資訊，請參閱 「設定 Java 環境參數」(第 134 頁)。

若要檢視關聯統計資料：

1 在 Identity Console 中，選取 **「IDM 管理」** > **按一下適當驅動程式集的內容功能表 (三個點)** > **「驅動程式集內容」** > **「審查器和統計資料」** > **「關聯統計資料」**。

2 選取想要執行關聯統計資料的伺服器。

3 關聯計數會顯示以前計算的結果。

Identity Console 會顯示與驅動程式集相關聯之所有驅動程式的作用中、非作用中和系統受管理物件的關聯計數。

Identity Console 會將群組和組織單位視為系統受管理物件。如果物件中的 Login Disabled 屬性設為 True 且物件未在最近 120 天內進行修改，則 Identity Console 會將物件視為非作用中。所有剩餘的物件都會被視為作用中受管理物件。

4 按一下 圖示以取得更新的結果。

當驅動程式在伺服器上停用時，Identity Console 不會在儀表板中顯示驅動程式。

5 按一下 圖示以輸出與伺服器相關聯之驅動程式的系統詳細資料和關聯計數詳細資料。

6 若要輸出與特定驅動程式相關聯的物件，請按一下必要物件旁邊的 ，並且儲存檔案。

附註：如果是擴送驅動程式，則只會輸出獨特的物件。如果物件與擴送驅動程式的例項相關聯，則 Identity Console 會在儀表板中顯示所有關聯計數。但是，如果您選擇輸出檔案中的物件，Identity Console 只會輸出獨特的物件。

7 按一下「動作」並且選取必要選項以組織關聯計數儀表板。

圖 22-4 管理驅動程式集統計資料

23 管理驅動程式內容

本節提供有關所有驅動程式常見內容的資訊。這包括所有內容 (具名密碼、引擎控制項值、記錄層級等等)。

將顯示驅動程式的啟動資訊，提醒您進行啟動過期驅動程式的動作。

若要修改驅動程式的組態，請執行以下步驟：

1 按一下 Identity Console 主畫面上的「**驅動程式**」索引標籤。

2 按一下個別驅動程式的磚以查看驅動程式的組態頁面。

根據預設，「**連接參數**」頁面隨即顯示。驅動程式組態選項分為以下類別：

連接參數

連接參數控制驅動程式應該在本端執行還是在遠端執行。

- **Java:** 使用此選項以指定針對驅動程式的 Shim 元件例項化的 Java 類別。此類別可以是類別目錄中的類別檔案，或是 lib 目錄中的 .jar 檔案。選取此選項以在本端執行驅動程式。您也必須指定驅動程式物件密碼和驅動程式快取限制。您可以藉由按一下「**設定密碼**」連結來設定新密碼。

  例如，com.microfocus.nds.dirxml.driver.scim.SCIMDriverShim

- **原生：**此選項是用來指定 .dll 的名稱，該檔案是以適用於驅動程式的原生語言 (例如 C++) 進行開發。您也必須指定驅動程式物件密碼和驅動程式快取限制。您可以藉由按一下「**設定密碼**」連結來設定新密碼。

  例如，addriver.dll

- **連接至遠端載入器：**此選項是在驅動程式遠端連接至連接的系統時使用。如果選取此選項，您必須指定以下子選項：

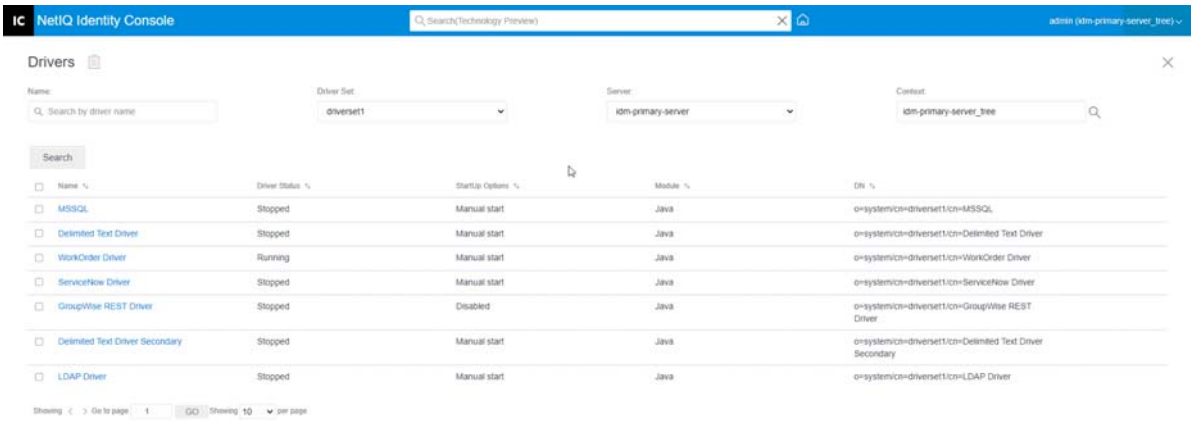
  - **遠端載入器連接參數**：包括「遠端載入器」環境詳細資料的相關資訊，例如主機名稱、連接埠等等。

- **遠端載入器密碼**：遠端載入器的密碼。
- **驅動程式物件密碼**：指定驅動程式物件的密碼。如果您正在使用「遠端載入器」，則必須在此頁面上輸入密碼。「遠端載入器」使用此密碼來對遠端驅動程式 Shim 進行自我驗證。

- **驗證**：驗證參數用於驗證 Identity Manager 引擎和遠端載入器伺服器。指定以下參數：
  - **驗證 ID**：指定使用者應用程式 ID。此 ID 用於將 Identity Vault 訂閱資訊傳送至該應用程式。
  - **驗證網路位置**：指定應用程式 Shim 應該與之進行通訊的伺服器 IP 位址或名稱。
  - **應用程式密碼**：用來設定應用程式驗證密碼的選項。

完成之後，按一下 圖示以儲存組態。

***圖 23-1** 管理連接參數*



驅動程式組態

驅動程式組態區段可讓您設定驅動程式特定參數、引擎控制項值、全域組態值等等。當您變更驅動程式參數時，您會調整驅動程式行為使其與您的網路環境密切合作。本節分為以下幾個類別：

- 「驅動程式參數」（第 147 頁）
- 「全域組態值」（第 147 頁）
- 「引擎控制值」（第 147 頁）
- 「啟動選項」（第 150 頁）
- 「具名密碼」（第 150 頁）
- 「安全性相等」（第 151 頁）

- 「排除的物件」(第 151 頁)
- 「管理值屬性清單」(第 151 頁)

驅動程式參數

驅動程式參數會分割成驅動程式設定、「訂閱者」設定和「發行者」設定。這些設定會根據您的驅動程式組態填入。如需驅動程式參數的詳細資訊，請參閱 Identity Manager 驅動程式文件上的特定驅動程式指南。

完成之後，您可以藉由按一下 來儲存參數。如果您想要將參數設為其預設值，請按一下 圖示。若要使用 xml 檔案修改驅動程式組態，請按一下 圖示。

全域組態值

顯示「全域組態」物件的排序清單。物件包含驅動程式的延伸 GCV 定義，Identity Manager 會在驅動程式啟動時載入。您可以使用 XML 編輯器，在 **「全域組態值」**索引標籤底下檢視或修改物件。按一下 圖示以儲存 GCV。若要重新整理 GCV 的清單，請按一下 圖示。若要刪除 GCV，請選取適當的 GCV 物件，然後按一下 圖示。

引擎控制值

引擎控制項值是變更 Identity Manager 引擎之特定預設行為的一種方式。這些值只能在伺服器與驅動程式集物件相關聯時進行存取。

選項	描述
訂閱者通道重試間隔 (以秒為單位)	「訂閱者」通道重試間隔控制在應用程式 Shim 的訂閱者物件傳回重試狀態之後，Identity Manager 引擎重試快取交易處理的頻率。
DN 語法屬性值的合法形式	DN 語法屬性值的合法規格會控制 DN 語法屬性值是以不合法或合法的斜線格式呈現。True 設定表示將以合法格式顯示值。
重新命名事件的合法格式	重新命名事件的合法格式會控制 Identity Vault 重新命名事件的新名稱部分是否會呈現至具有類型修飾詞的「訂閱者」通道。例如，CN=。True 設定表示將以合法格式顯示名稱。
最大 eDirectory 複寫等候時間 (以秒為單位)	此設定控制 Identity Manager 引擎等候特定變更在本端複製本與遠端複製本之間進行複寫的時間最大值。這只會影響 Identity Manager 引擎必須聯絡相同網路樹中遠端 eDirectory 伺服器的操作，以便執行操作並且可能需要等候到部分變更複寫到遠端伺服器或從中複寫，操作才能完成 (例如，當 Identity Manager 伺服器不保留已移動物件的主複製本時，物件才會移動；從範本建立之使用者的檔案系統正確操作。)

選項	描述
為 XSLT 使用違規向後相容模式	此控制項會將 Identity Manager 引擎使用的 XSLT 處理器設定為向後相容模式。反向相容模式會導致 XSLT 處理器使用一或多種不符合 XPath 1.0 和 XSLT 1.0 標準的行為。這是為了與依賴非標準行為的現有 DirXML 樣式表的反向相容而進行的。 例如，XPath "!=" 運算子的行為，當其中一個運算元是節點集，而另一個運算元是節點集以外的項目時，在發行最高包括 Identity Manager 2.0 在內的 DirXML 中是不正確的。此行為已修正；但是，修正的行為預設會透過此控制項停用，以便與現有 DirXML 樣式表反向相容。
一次移轉的最大應用程式物件	此控制項是用來限制 Identity Manager 引擎在單一查詢 (從應用程式移轉物件操作的一部分) 期間向應用程式要求的應用程式物件數目。 如果在從應用程式移轉操作期間遇到 java.lang.OutOfMemoryError 錯誤，此數目應該設為低於預設值。預設值為 50。 **附註：**此控制不會限制可移轉的應用程式物件；其只會限制批次大小。
在 Identity Vault 中建立的物件上設定 creatorsName	Identity Manager 引擎會使用此控制項來確定，對於在 Identity Vault 中由此驅動程式建立的所有物件，是否應將 creatorsName 屬性設定為此驅動程式的 DN。 設定 creatorsName 屬性便可輕鬆識別驅動程式所建立的物件，但也會對效能造成負面的影響。如果沒有設定，creatorsName 屬性就會預設為代管該驅動程式之「NCP 伺服器」物件的 DN。
寫入等待中關聯	此控制項會確定 Identity Manager 引擎是否在「訂閱者」通道處理期間寫入有關物件的等待中關聯。 寫入等待中關聯給予的優點很少，甚至沒有優點，但確實會對效能造成負面影響。然而，存在開啟以進行反向相容性的選項。
使用密碼事件值	此控制項可決定為「訂閱者」通道新增和修改事件的 nspmDistributionPassword 屬性所報告的值來源。 將控制項設為 False，表示已取得 nspmDistributionPassword 目前的值，並呈報為該屬性事件的值。這表示只有目前的密碼值可使用。這是預設的行為。 將控制項設為 True，表示以此 eDirectory 事件記錄的值會解密，並呈報為該屬性事件的值。這表示在該事件期間同時有舊密碼值 (若有的話) 和取代的密碼值。這可用於將密碼與需要舊密碼來設定新密碼的特定應用程式同步化。
重試超出範圍事件	此控制項會決定如果收到超出範圍同步化事件的重試狀態，是否應該重試超出範圍同步化事件。 如果控制項設為 False，則不會重試超出範圍同步化。如果設為 True，超出範圍同步化會重試直到成功為止。

選項	描述
使用 Rhino ECMAScript 引擎	決定 Identity Manager 引擎是否使用 Rhino ECMAScript 引擎。引擎會使用 Rhino 作為預設 ECMAScript 引擎。 此控制項預設為 **True**，如果您將此控制項設為 **false**，則引擎會使用 Nashorm 程序檔。
啟用訂閱者服務通道	決定 Identity Manager 引擎是否會處理驅動程式的訂閱者服務通道的超出範圍查詢。這些查詢的一些常見範例是代碼對應重新整理、資料收集和由 dxcmd 觸發的查詢。 當此控制項設為 True 時，通道會個別處理這些查詢，而不會中斷事件的正常處理。 目前，此控制項僅適用於 JDBC 擴送驅動程式 (預設啟用)。
啟用密碼同步化狀態報告	此控制項會決定 Identity Manager 引擎是否回報 「訂閱者」通道密碼變更事件的狀態。 回報 「訂閱者」通道密碼變更事件的狀態，可允許如 「Identity Manager 使用者應用程式」這類的應用程式，來監控應該與所連接應用程式同步化的密碼變更同步化進度。
將範本物件的值與新增操作的值結合在一起	此值決定 Identity Manager 引擎是否將像是建立範本的值，與執行新增操作時的新增操作結合在一起。將值設定為 True 會導致除了使用在新增操作中指定的同一個屬性的值之外，還會使用範本的多值屬性值。將值設定為 False 會導致如果在新增操作中指定的同一個屬性含有值，則會忽略範本。
允許從發行者到訂閱者通道的事件迴路	此值決定 Identity Manager 引擎是否允許從驅動程式的 「發行者」通道到 「訂閱者」通道的事件迴路。若將此值設定為 False，Identity Manager 引擎將不允許事件迴路。若將此值設定為 True，Identity Manager 引擎將允許事件從 「發行者」通道迴路到 「訂閱者」通道。
回復到計算的成員資格值行為	此值決定 Identity Manager 引擎在執行與群組成員資格相關的讀取和搜尋動作時，使用的方法。 若將此值設定為 False (預設設定)，則 Identity Manager 引擎在讀取或搜尋 Identity Vault 物件的成員和群組成員屬性時，僅會傳回 「靜態」值。靜態值是透過直接指定給群組，而非透過巢狀群組繼承指定，來接收群組成員資格的物件。 若將此值設定為 True，則 Identity Manager 引擎回復為使用 Identity Manager 3.6 之前版本所用的方法。在早於 3.6 的版本中，Identity Manager 引擎在搜尋成員和群組成員屬性時會擷取所有 「計算的」值。計算值包括 1) 靜態指定給成員資格的物件或 2) 透過 eDirectory 所使用的巢狀群組階層計算的功能來動態指定給成員資格的物件。搜尋群組的 「成員」屬性會傳回直接指派給群組的物件，或者是透過巢狀群組指派成員資格的物件。
等候驅動程式關閉的最大時間 (以秒為單位)	此設定會控制 Identity Manager 引擎等候驅動程式的 「發行者」通道關閉的最大時間。如果驅動程式未在指定的時間間隔內關閉，Identity Manager 引擎會終止驅動程式。

選項	描述
規則運算式逸出中繼字元	此控制項會決定在規則運算式內容中使用時，於擴充本端變數時逸出的中繼字元。需要逸出的所有字元必須新增為此控制項值的逗號分隔清單。 如果控制項值中沒有中繼字元，則不會在包含規則運算式的本端變數擴充期間逸出。 在使用此控制項時，請確保以下幾點： ◆ 值不留空。根據預設，會填入 ***$***。本端變數擴充需要此字元。 ◆ 值應該是有效的逗號 (,) 分隔清單，否則您會在規則評估期間遇到錯誤。 ◆ 若要逸出所有中繼字元，請指定 "\、$、^、.、?、*、+、[,]、(,)、|" 作為值。 ◆ 如果不需要逸出中繼字元，請從值中移除該字元。 ◆ 若要逸出任何中繼字元，請指定中繼字元，後面接續著反斜線 (\)。
忽略其他驅動程式的授權變更	此控制項會決定 Identity Manager 引擎忽略或處理其他驅動程式的授權變更。預設值為 True。這表示驅動程式會自動忽略其他驅動程式的授權變更。如果此控制項設為 False，則系統會快取其他驅動程式的授權變更，並且由此驅動程式進行處理。
允許從 CPRS 到訂閱者通道的授權事件迴路	此控制項會決定 Identity Manager 引擎是否允許 CPRS 指定產生的授權事件可以迴路到驅動程式的「訂閱者」通道。預設值為偽。這表示事件不會迴路到「訂閱者」通道。如果此控制項設為 True，事件會流向驅動程式的「訂閱者」通道。

啟動選項

「啟動選項」允許您在 Identity Manager 伺服器啟動時設定驅動程式狀態。

- **自動啟動**：每次 Identity Manager 伺服器啟動時，驅動程式就會啟動。
- **手動**：Identity Manager 伺服器啟動時，驅動程式不會啟動。驅動程式必須使用 Identity Console 入口網站啟動。
- **已停用**：驅動程式具有會儲存所有事件的快取檔案。當驅動程式設為「已停用」時，這個檔案會遭到刪除且不會在檔案中儲存新的事件，直到驅動程式狀態變更為「手動」或「自動啟動」。

在設定偏好的啟動選項之後，請按一下 圖示以儲存。若要重設啟動選項，請按一下 圖示。

具名密碼

Identity Manager 允許您安全地儲存驅動程式的多個密碼。此功能稱為具名密碼。每個不同的密碼可以透過金鑰或名稱進行存取。

您可以對驅動程式集或個別驅動程式新增具名密碼。驅動程式集的具名密碼適用於集合中的所有驅動程式。個別驅動程式的具名密碼僅適用於該驅動程式。

若要在驅動程式規則中使用具名密碼，請依密碼名稱來參考密碼，而不是使用實際的密碼，Identity Manager 引擎會將密碼傳送給驅動程式。本節中所述的儲存和取回具命密碼的方法，可用於任何驅動程式，不需要對驅動程式 Shim 進行任何變更。

若要新增具名密碼，請按一下 ＋ 圖示。若要移除現有的具名密碼，請按一下  圖示。若要儲存您的清單，請按一下  圖示。

安全性相等

使用「安全性相等」頁面以檢視或變更驅動程式明確地與安全性等值的物件清單。此物件有效具有所列出物件的全部權限。

您可以藉由按一下 ＋ 圖示，在安全性相等清單中新增新的物件。如果您新增或刪除此清單中的物件，則系統會自動將此物件新增至該物件的「安全性相等於我」內容中或將其從中刪除。您不需新增 [Public] 託管者或此物件的父容器到此清單中，因為此物件的安全性已隱含地與其等值。

若要從此清單移除現有的物件，請按一下  圖示。若要儲存您的清單，請按一下  圖示。

排除的物件

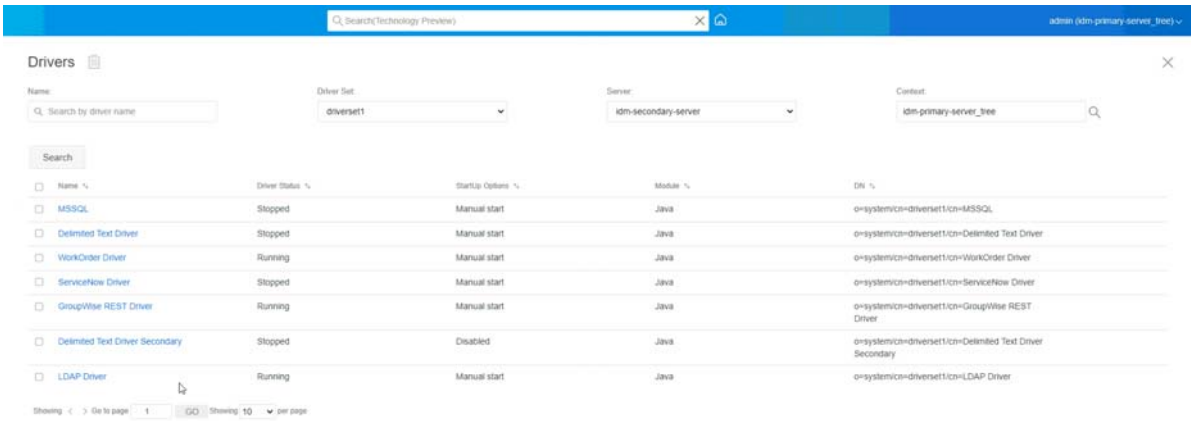
使用此選項，建立一份不會複製到應用程式的物件清單。建議您將代表管理角色 (例如，Admin 物件) 的所有物件，都加入此清單。您可以藉由按一下 ＋ 圖示，在此清單中新增新的物件。若要從此清單移除現有的物件，請按一下  圖示。若要儲存您的清單，請按一下  圖示。

管理值屬性清單

若要將屬性新增至特定驅動程式的值屬性清單，請執行下列步驟：

1. 在 Identity Console 中，選取**物件管理**模組。
2. 從下拉式清單中選取 **Dir-XML-Driver** 類型，然後按一下「搜尋」按鈕。
3. 從搜尋清單中按一下適當的驅動程式。
4. 若要將無值屬性新增至屬性值清單，請按一下**「值屬性」**旁邊的 ＋ 圖示，並從清單中選取適當的無值屬性。
5. 完成之後，請按一下**「確定」**。

圖 23-2 管理驅動程式組態



資料轉換和同步

本節分為以下幾個類別：

- 「資料同步檢視」（第 152 頁）
- 「類別屬性篩選器」（第 155 頁）
- 「ECMA 程序檔」（第 156 頁）
- 「相互屬性對應」（第 156 頁）

資料同步檢視

驅動程式的綜覽頁面分割成下列類別：

- 「過濾器」（第 153 頁）
- 「所有規則」（第 153 頁）
- 「將資料移轉至 Identity Vault」（第 153 頁）
- 「從 Identity Vault 移轉資料」（第 154 頁）
- 「同步化物件」（第 154 頁）
- 「追蹤 DirXML 程序檔」（第 154 頁）

過濾器

過濾器位於驅動程式上，並可讓您指定哪一些類別和屬性可由應用程式傳送至 Identity Vault，並從 Identity Vault 接收。如果要指定須通過以供 Metadirectory 引擎處理的類別，您應將類別新增至適當通道上的類別。您也可以按所定義的特定屬性值篩選物件。

若要新增希望包含在同步中的類別和屬性，並修改驅動程式篩選器，請按一下 「發行者」或「訂閱者」通道上的 **「篩選器」**。

附註：注意：「綜覽」圖形描述會顯示 「發行者」或 「訂閱者」通道上驅動程式過濾器的兩個不同物件。雖然顯示兩個物件，但是這兩個通道均參考同一個過濾器。

所有規則

根據預設，「所有規則」頁面隨即顯示。您可以按一下 圖示，在容器中輸入現有規則。

您也可以移除任何不需要的規則。若要為您的驅動程式選取追蹤層級，請按一下 圖示。

您可以使用 和 圖示，上下移動清單中的規則。

附註：Identity Console 不支援為驅動程式新增和部署新規則。我們建議您使用 iManager 和 Identity Designer 來新增和部署新規則。

將資料移轉至 Identity Vault

使用此任務，您可以定義 Identity Manager 用來從應用程式將物件移轉至 Identity Vault 所使用的準則。當您移轉物件時，Metadirectory 引擎會將所有的 「相符」、「佈置」和 「建立」規則以及 「 發行者」過濾器均套用至該物件。物件會使用在 「類別」清單中指定的順序，移轉至 Identity Vault。您可以使用此選項來執行下列任務：

1. **新增類別和屬性**：若要新增或移除您想要移轉的類別和屬性，請按一下 圖示。然後選取您想要新增的類別及其個別的屬性。選取類別和屬性之後，按一下 **「新增」**以儲存您的變更。
2. **編輯屬性值**：若要變更您在編輯清單時指定的移轉屬性值，請按一下編輯屬性 圖示。
3. **重新排序類別清單**：使用 和 按鈕以變更清單中類別的順序。物件會使用在 「類別」清單中指定的順序，移轉至 Identity Vault。
4. **重新整理：**按一下 圖示以重新整理清單。

從 Identity Vault 移轉資料

使用 「**輸出**」索引標籤，您可以選取想要從 Identity Vault 移轉至應用程式的容器或物件。當您移轉物件時，Metadirectory 引擎會將所有的 「相符」、「建立」和 「佈置」規則以及 「訂閱者」過濾器均套用至該物件。

若要將物件或容器從 Identity Vault 移轉至其他應用程式，請按一下  圖示。瀏覽至您要移轉的物件並選取，再按一下 「**確定**」將該物件新增至移轉清單。若要將物件從移轉清單中移除，請按一下  圖示。

在您完成選取您要移轉的物件之後，請按一下  開始移轉。螢幕上將會顯示移轉進度。如果您想要停止移轉，請按一下  按鈕。

同步化物件

該同步化操作會搜尋已修改過的物件並對其進行同步化。或者您可以選取 「**檢查所有物件**」以立即啟動同步化。或者，您可以設定開始同步化的日期 / 時間。

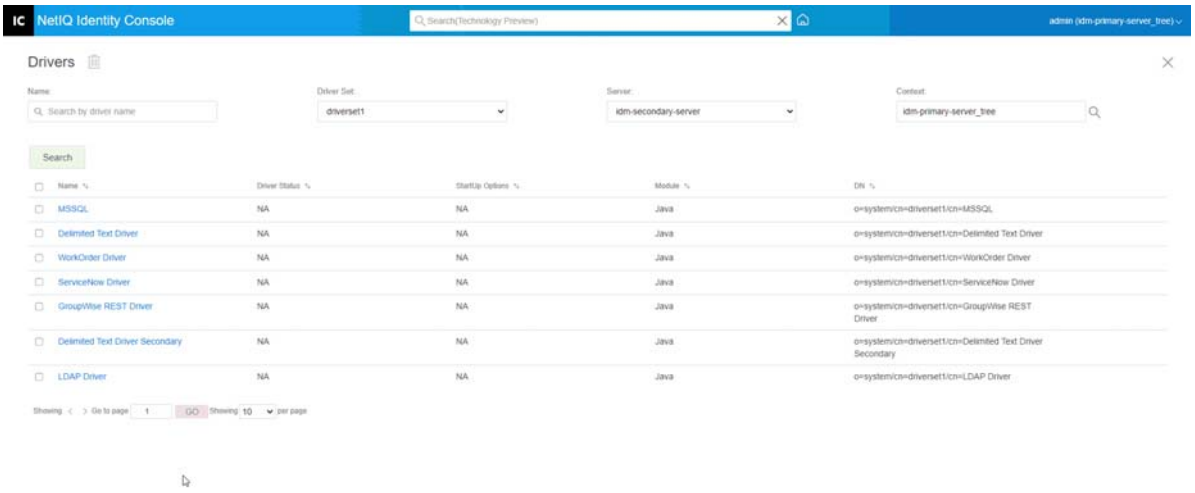
追蹤 DirXML 程序檔

「追蹤 DirXML 程序檔」選項可讓您選取驅動程式的追蹤層級。它還會將追蹤設定套用於所有發行者和訂閱者通道。可以選取下列 DirXML 程序檔追蹤選項 :

- 所有 DirXML 程序檔追蹤開啟
- 所有 DirXML 程序檔追蹤關閉
- DirXML 程序檔規則追蹤開啟
- DirXML 程序檔規則追蹤關閉

按一下 以儲存變更。

圖 23-3 管理驅動程序的資料同步



類別屬性篩選器

類別屬性篩選器可讓您指定應用程式可向 Identity Vault 傳送以及從 Identity Vault 接收哪些類別和屬性。如果要指定須通過以供 Metadirectory 引擎處理的類別，您應將類別新增至適當通道上的類別。您也能夠按照您定義的特定屬性來過濾物件。使用此選項可執行以下動作：

- **設定範本**：使用此選項為新增至篩選器的所有屬性設定預設選項。按一下「類別屬性篩選器」標籤旁邊的 圖示。
- **新增新的類別**：藉由按一下 圖示來新增新的類別。
- **新增新的屬性**：按一下 圖示來新增新的屬性。
- **從此處複製篩選器**：此選項可讓您從其他驅動程式複製篩選器。按一下圖示 以複製篩選器。
- **編輯 XML**: 使用編輯 XML 檔案 圖示，編輯類別和屬性篩選器設定。
- **刪除類別或屬性**：藉由按一下個別類別或屬性旁邊的 圖示，刪除任何類別或屬性。

您可以在「發行者」和「訂閱者」通道上針對類別和屬性值設定下列選項：

- 同步化
- 忽略
- 通知
- 重設

合併權限

如果屬性不是在任一通道上同步化，則不會發生合併。

如果屬性在一個通道上同步化，而不在另一個通道上同步化，則該通道之目的地上的所有現有值便會移除，並取代為來自該通道之來源的值。如果來源有多個值，且目的地只能容納單一值，則在目的地端只會使用其中一個值。

如果屬性在兩個通道上都同步化，而且兩端都只能容納單一值，則連接的應用程式會取得 Identity Vault 中儲存的值，除非 Identity Vault 中沒有值。在此情況下，Identity Vault 會取得連接的應用程式的值。

如果屬性在兩個通道上都同步化，而且只有一端可以容納多個值，則單一值通道的值會新增至多值通道 (如果該值尚未在多值通道)。如果單一值端沒有值，您可以選擇值並將其新增至單一值端。您可以為「合併權限」設定下列選項：

- 預設值
- Identity Vault
- 應用程式
- 無

按一下 以儲存變更。

ECMA 程序檔

顯示 ECMAScript 資源檔案的排序清單。檔案包含驅動程式的延伸函數，Identity Manager 會在驅動程式啟動時載入。您可以按一下 輸入其他檔案、按一下 移除現有檔案，或變更檔案的執行順序。您還可以上下移動清單中的程序檔。您可以按一下 圖示來儲存「ECMA 程序檔」清單。

相互屬性對應

相互屬性對應可讓您建立並管理物件之間的相互連結或參照。例如，「群組」物件包含參考屬於該「群組」之所有使用者物件的「成員」屬性。同樣，每個「使用者」物件包含參考使用者所屬之「群組」物件的「群組成員資格」屬性。為了讓 Metadirectory 引擎使「群組物件」>「成員」屬性與 Identity Vault 中所有「群組」物件和「使用者」物件的「使用者物件」>「群組成員資格」屬性保持同步，必須連結這些屬性。物件屬性之間的連結稱為相互屬性對應。

使用此模組可執行以下動作：

- 「建立自定相互屬性對應」(第 157 頁)
- 「新增新的相互屬性對應」(第 157 頁)
- 「移除相互屬性對應」(第 157 頁)
- 「從相互對應清單移除屬性」(第 157 頁)
- 「重排對應屬性的順序」(第 158 頁)
- 「移除自定相互屬性對應」(第 158 頁)
- 「編輯相互屬性 XML」(第 158 頁)

建立自定相互屬性對應

本節僅在「相互屬性對應」頁面顯事實適用**驅動程式不包含自定相互屬性對應。按一下上方的 '+' 圖示以建立基本相互屬性對應** 提示。

1 按一下 ＋ 圖示以建立新的自定相互屬性對應清單。

2 驅動程式的預設屬性對應即會顯示。您現在可以新增對應、修改現有對應或刪除其他對應。

新增新的相互屬性對應

當您建立相互屬性對應時，您必須先將其中一個屬性新增至相互對應清單。

1 按一下「動作」下拉式選單旁邊的 ＋ 圖示。

2 在新的屬性項目中，從下拉式清單選取想要的屬性。

3 指定相互對應的詳細資料：

3a **來源類別**：指定對應清單中的屬性關聯的類別名稱。例如，如果您將「群組成員資格」屬性放在相互對應清單中，則關聯的「來源類別」是「使用者」。

3b **目的地類別**：指定與您想要建立相互對應之屬性關聯的類別名稱。例如，如果您將「群組成員資格」屬性放在相互對應清單中，則關聯的「目的地類別」是「群組」。

3c **相互屬性**：指定您想要建立相互對應的屬性名稱。

4 若您想要將屬性對應至其他相互屬性，可按一下屬性名稱右邊的 ＋ 圖示。

即會在屬性清單結尾處新增一個新的屬性區段。選取來源類別、目的地類別及相互屬性。

移除相互屬性對應

若要移除相互屬性對應：

1 在**「來源類別」**前面，選取您想要刪除之相互屬性對應的核取方塊。

2 按一下屬性下拉式清單旁邊的 🗑 圖示。

從相互對應清單移除屬性

若要從相互對應清單移除屬性：

1 藉由選取屬性前面的核取方塊，選取您想要移除的屬性。

2 按一下**「動作」**下拉式清單旁邊的 🗑 圖示。

重排對應屬性的順序

屬性對應會依所列順序由上往下來解析。您可以將清單中的對應屬性向上或向下移動，確定會以正確的順序來解決。一般而言，您應會先列出特定的對應，之後才列出更多的一般對應。例如，「群組」物件上「成員」屬性的對應應會列在任何物件 (「< 任何類別 >」選項) 上「成員」屬性的對應之前。

請選取您要移動之對應屬性前方的核取方塊，然後按一下 ↑，將對應向上移動，或者按一下 ↓，將對應向下移動。

移除自定相互屬性對應

您可以刪除所建立的自定屬性對應。這會導致 Metadirectory 引擎使用驅動程式的預設屬性對應。

若要移除自定相互屬性對應，請按一下螢幕頂端的 圖示。

編輯相互屬性 XML

如果需要，您可以針對相互屬性直接編輯 XML。若要這麼做，請按一下「自定相互屬性對應」頁面上的「編輯 XML」圖示。這樣會開啟基本 XML 編輯器，可讓您修改 XML。完成之後，按一下「確定」或「取消」以關閉 XML 編輯器。

進階設定

進階設定會分為以下類別 :

- 「管理授權」(第 158 頁)
- 「管理物件對應表」(第 159 頁)
- 「管理驅動程式的工作」(第 159 頁)

管理授權

「授權」頁面包含一表格，顯示目前定義於所選伺服器中的所有授權 (以完整可辨識名稱列出)。在此頁面上允許以下動作 :

- **在 XML 中編輯** : 若要在 XML 檔案中編輯授權，請從清單中選取授權，然後按一下 圖示。然後勾選 **「啟用 XML 編輯」**方塊。
- **刪除** : 若要刪除授權，按一下授權名稱左邊的方塊，然後按一下 圖示。您可看到一訊息，說明此操作無法復原，且詢問您是否確定要刪除所選授權。按一下 **「確定」**刪除授權，或按一下 **「取消」**停止操作。您可以按一下多個方塊刪除多個授權，或按一下左上角的方塊刪除所有列出的授權。

管理物件對應表

Identity Manager 規則使用映射表，將一組值映射至另一組對應值。當您安裝授權套件時，此套件的規則會新增到驅動程式啟動規則集中。驅動程式只會在驅動程式啟動時執行這些原則一次。如需詳細資訊，請參閱 《NetIQ Identity Manager Driver Administration Guide》 (NetIQ Identity Manager 驅動程式管理指南) 中的 「*Mapping Table Objects*」 (對應表物件)。

使用物件對應表，您可以執行下列動作：

- **修改現有對應：**若要修改現有的物件對應表，請按一下清單中的對應，然後執行下一個畫面上的下列動作：
  - 新增新的欄。

    指定欄的值，再選取值是否區分大小寫，或為數值。
  - 新增新的列並指定列的值。
  - 按一下 圖示。
- **刪除對應**：若要移除清單中的對應，請選取清單中的適當對應，然後按一下 圖示。
- **在 XML 中編輯**：若要在 XML 檔案中編輯對應，請按一下清單中的對應，然後選取 圖示。然後勾選 **「啟用 XML 編輯」**方塊。

管理驅動程式的工作

Identity Console 可讓您使用 「工作」選項，為所有個別驅動程式排程事件。

「工作排程器」頁面包括工作名稱、工作為啟用或停用、排程執行工作的時間、和工作描述。按一下工作名稱以帶出 「工作」頁面。按一下 「已啟用」欄下的啟用 / 停用圖示，以啟用或停用工作。按一下工作描述以查看工作的完整描述。

「工作」索引標籤中有一個表格，會顯示選定驅動程式的現有工作物件 (驅動程式會在 「驅動程式」項目中以完整可辨識名稱列出)。

「工作排程器」頁面允許您執行以下任務：

- **建立工作**：按一下 圖示以建立新工作。

  在 **「新工作」**快顯中，若要建立新工作，請執行以下步驟：

  1. 指定工作名稱。
  2. 選取工作類型。
  3. 按一下 圖示，然後從可用伺服器清單中選取要執行工作的伺服器。否則，請指定伺服器名稱，然後選取伺服器。
  4. 按一下 **「建立」**按鈕。
- **啟動工作**：按一下工作左邊的方塊以選取該工作，再按一下 圖示。
- **停止工作**：按一下工作左邊的方塊以選取該工作，再按一下 圖示。
- **啟用工作**：按一下工作左邊的方塊以選取該工作，再按一下 圖示。

- **停用工作**：按一下工作左邊的方塊以選取該工作，再按一下 ⊗ 圖示。
- **取得狀態**：按一下工作左邊的方塊以選取該工作，再按一下 ⓘ 圖示。
- **刪除工作**：按一下工作左邊的方塊以選取該工作，再按一下 🗑 圖示。

按一下工作，以存取 **「工作內容」**頁面。您可在此設定您希望如何執行工作。

一般：顯示工作的 Java 類別名稱。使用此頁面啟用或停用工作、在執行後刪除工作、選取應執行工作的伺服器、指定電子郵件伺服器，並賦予工作不同的顯示名稱與描述。

排程：可讓您設定希望執行工作的時間。指定「啟動工作於」以設定時間，以及是否每天、每週、每月、每年執行工作。您也可以自定要執行工作的時間，或選擇啟用切換開關以手動執行工作。

範圍：可讓您定義此工作適用的物件。物件可以是容器、動態群組、群組，或葉物件。按一下「新增」，選取您希望套用此工作的物件。您可使用「瀏覽」按鈕選取物件，再按一下「確定」。若要從範圍清單中移除物件，請按一下 DN 物件左側方塊選取範圍物件，再按一下「移除」。

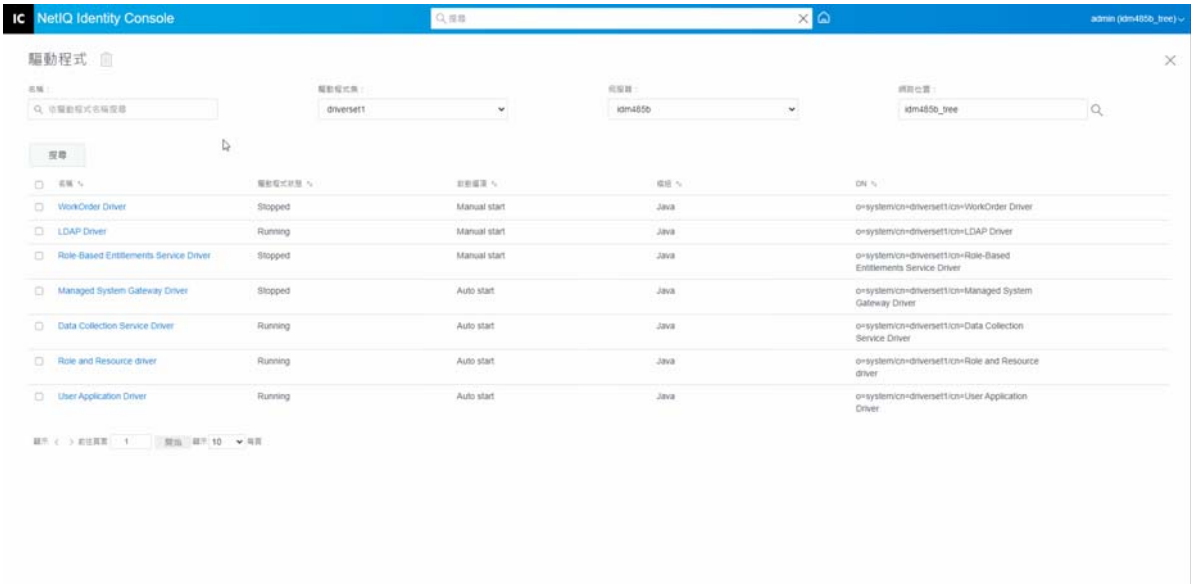
新增物件時，請選取物件以顯示更多選項。若您選取群組物件，則可選擇將工作套用至群組成員，或僅套用至群組。若您選取容器物件，可選擇將工作套用到容器內所有的下階物件、容器中所有子物件，或僅套用至容器。

參數：可讓您將其他參數新增至工作，並檢視參數目前設定的狀況。根據所選取的工作類型而定，這些參數也有所變更。

結果：可讓您定義要如何處理工作結果。「結果」頁面分為兩部份：「中介結果」與「最終結果」，所允許的結果有：成功、警告、錯誤和中止。「結果」欄的右邊為「動作」欄。按一下「動作」欄，可讓您設定通知各結果的方式。「動作」包括完成結果時寄送稽核結果或寄送電子郵件。若您未選擇選項，則不會對結果進行任何動作。

在 **「追蹤」**索引標籤中，您可以為特定驅動程式設定追蹤。如需詳細資訊，請參閱 「設定追蹤層級」(第 162 頁)

圖 23-4 *管理進階設定*



設定驅動程式的記錄和追蹤層級。

若要設定驅動程式的記錄和追蹤，請從 Identity Console 主要頁面選取 「驅動程式」 > 「記錄和追蹤組態」索引標籤。本節分為以下幾個類別：

- 「設定記錄層級」 (第 161 頁)
- 「設定追蹤層級」 (第 162 頁)

設定記錄層級

每個驅動程式都有記錄層級欄位，您可以在其中定義應該追蹤的錯誤層級。此處指定的層級決定要納入記錄的訊息。依照預設，已設定記錄層級以追蹤錯誤訊息 (這也包括嚴重訊息)。若要追蹤其他訊息類型，請變更記錄層級。若要設定記錄層級，請選取 「記錄和追蹤組態」 > 「記錄層級」索引標籤。下表描述記錄層級設定：

選項	描述
使用來自驅動程式集的記錄設定	如果選取此選項，驅動程式會根據驅動程式集物件的記錄設定來記錄事件。
關閉驅動程式集、「訂閱者」和 「發行者」記錄的記錄	關閉驅動程式集物件、「訂閱者」通道和 「發行者」通道上此驅動程式的所有記錄。
記錄中的最大項目數 (50-500)	記錄中的項目數。預設值為 50。

記錄層級	可以選取以下記錄層級：
	• 記錄錯誤：只記錄錯誤
	• 記錄錯誤和警告：記錄錯誤和警告
	• 記錄特定事件：記錄已選取的事件。選取此選項可啟用以下事件清單：
	  ◆ Metadirectory 引擎事件
	  ◆ 狀態事件
	  ◆ 操作事件
	  ◆ 轉換事件
	  ◆ 身分證明佈建事件
	• 僅更新上次記錄時間：更新上次記錄時間。
	• 關閉記錄：關閉驅動程式的記錄。

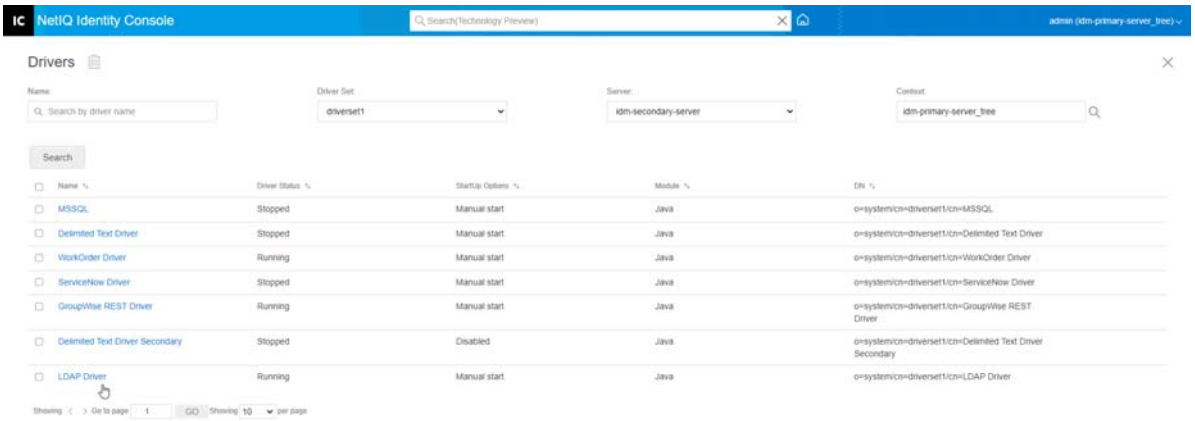
設定追蹤層級

您可以為特定驅動程式設定追蹤。根據為驅動程式指定的追蹤層級，追蹤會在引擎處理事件時，顯示驅動程式相關事件。驅動程式追蹤層級僅影響已設定追蹤的驅動程式或驅動程式集。如果您正在使用遠端載入器，遠端載入器追蹤檔案將直接設定在遠端載入器上，並且僅包含驅動程式 Shim 追蹤。

若要設定驅動程式的追蹤，請選取 **「記錄和追蹤組態」** > **「追蹤」**索引標籤。下表描述追蹤設定：

參數	驅動程式
追蹤層級	隨著驅動程式追蹤層級增加，在「追蹤」中顯示的資訊量也會增加。 追蹤層級一顯示錯誤，但不會顯示錯誤原因。如果您想要查看密碼同步化資訊，請將追蹤層級設為五。 如果您選取 **「使用驅動程式集的設定」**，則會採用驅動程式集的值。
追蹤檔案	為選取的驅動程式指定寫入 Identity Manager 資訊所在的檔案名稱和位置。 如果您選取 **「使用驅動程式集的設定」**，則會採用驅動程式集的值。
追蹤名稱	驅動程式追蹤訊息前面會放置輸入的值，而不是驅動程式名稱。在驅動程式名稱非常長的時候使用。
追蹤檔案編碼	追蹤檔案會使用系統的預設編碼。您可以依需要指定另一種編碼。
追蹤檔案大小限制	允透設定 Java 追蹤檔案的限制。如果您將檔案大小設為沒有限制，則檔案大小會一直增加，直到沒有剩餘的磁碟空間為止。 **附註：**如果指定了檔案大小限制，則會在多個檔案中建立追蹤檔案。Identity Manager 會自動將最大檔案大小除以 10，並且建立 10 個個別檔案。這些檔案的合併大小等於最大追蹤檔案大小。 如果您選取 **「使用驅動程式集的設定」**，則會採用驅動程式集的值。

圖 23-5 管理驅動程式的記錄和追蹤層級



審查驅動程式

您可以使用驅動程式審查器以檢視與驅動程式相關聯之物件的詳細資訊。本節分為以下幾個類別：

- 「驅動程式審查器」(第 163 頁)
- 「驅動程式快取審查器」(第 164 頁)
- 「超出範圍同步化快取審查器」(第 165 頁)
- 「驅動程式資訊清單」(第 165 頁)
- 「監控驅動程式的狀態」(第 166 頁)

驅動程式審查器

若要檢視與驅動程式相關聯的物件：

1. 在 Identity Console 中，選取 **「驅動程式」** > **「審查器」** > **「驅動程式審查器」**索引標籤。
2. 在 **「驅動程式」**欄位中，指定您想要審查之驅動程式的完整可辨識名稱，或按一下瀏覽圖示以瀏覽並選取想要的驅動程式。
3. 在您選取要審查的驅動程式之後，按一下 **「確定」**以顯示「驅動程式審查器」頁面。

   此頁面可顯示所選取驅動程式相關聯的物件相關資訊。您可以執行以下任何動作：

   - **刪除：**移除驅動程式和物件之間的關聯。選取您不會想要再與驅動程式產生關聯之物件前端的核取方塊，按一下 圖示，然後按一下 **「確定」**以確認刪除。
   - **重新整理：**選取重新整理 圖示這個選項可以重新讀取驅動程式關聯的所有物件，然後重新整理資訊。

- **顯示 :** 選取每頁要顯示的關聯數目。您可以選取預先定義的數字 (25、50 或 100)，或者為您的選擇設定其他數字。預設值是每頁 10 個關聯。若關聯數目多於所顯示的數目，您可以使用箭頭按鈕來顯示關聯的上一頁與下一頁。
- **動作 :** 在與驅動程式相關聯的物件上執行動作。按一下 **「動作」**，然後選取下列其中一個選項 :
  - **顯示所有關聯 :** 顯示與驅動程式關聯的所有物件。
  - **已停用關聯的篩選器 :** 顯示與具有 「已停用」狀態的驅動程式關聯的所有物件。
  - **手動關聯的篩選器 :** 顯示與具有 「手動」狀態的驅動程式關聯的所有物件。
  - **移轉關聯的篩選器 :** 顯示與具有 「移轉」狀態的驅動程式關聯的所有物件。
  - **等待中關聯的篩選器 :** 顯示與具有 「等待中」狀態的驅動程式關聯的所有物件。
  - **已處理關聯的篩選器 :** 顯示與具有 「已處理」狀態的驅動程式關聯的所有物件。
  - **未定義關聯的篩選器 :** 顯示與具有 「未定義」狀態的驅動程式關聯的所有物件。
  - **關聯摘要 :** 顯示與驅動程式關聯之所有物件的狀態。
- **物件 DN:** 顯示關聯物件的 DN。
- **狀態 :** 顯示物件的關聯狀態。
- **物件 ID:** 顯示關聯的值。

驅動程式快取審查器

您可以使用 Identity Console 來檢視驅動程式快取檔案中的交易。**「驅動程式快取審查器」**會顯示有關快取檔案的資訊，包括由驅動程式處理的事件清單。

1 在 Identity Console 中，選取 **「驅動程式」** > **「審查器」** > **「驅動程式快取審查器」**索引標籤。

2 在 **「驅動程式」**欄位中，指定要審查其快取之驅動程式的完整可辨識名稱，或按一下瀏覽圖示以瀏覽和選取所需的驅動程式，然後按一下 **「確定」**以顯示 「驅動程式快取審查器」頁面。

只有當驅動程式未執行時，才能讀取驅動程式的快取檔案。如果驅動程式停止，則 「驅動程式快取審查器」頁面將會顯示快取。如果驅動程式正在執行，則頁面會顯示 「驅動程式未停止，無法讀取快取」備忘記事以代替快取項目。若要停止驅動程式，請按一下 按鈕，然後就能讀取和顯示快取。

- **伺服器上的驅動程式快取 :** 列出包含快取檔案例項的伺服器。如果驅動程式在多部伺服器上執行，您可以選取清單中的其他伺服器以檢視該伺服器的驅動程式快取檔案。
- **「啟動 / 停止驅動程式」圖示 :** 顯示驅動程式目前的狀態，並可讓您啟動或停止驅動程式。快取只能在驅動程式停止時讀取。
- **刪除 :** 選取快取中的項目，然後按一下 圖示以從快取檔案中將其移除。

- **動作：**可讓您對快取檔案中的項目執行動作。按一下「動作」展開功能表，然後選取下列其中一個選項：
  - **清除所有快取事件：**可讓您清除所有快取事件。
  - **快取摘要：**摘要快取檔案中儲存的所有事件。

檢視驅動程式的已連接系統詳細資料

若要檢視特定驅動程式的已連接系統詳細資料，請執行下列動作：

1. 在 Identity Console 中，按一下「物件管理」模組。
2. 瀏覽並選取您要顯示已連接系統的特定驅動程式物件。
3. 您的電腦上將會顯示，所選取驅動程式物件的所有已連接系統詳細資料。

超出範圍同步化快取審查器

若要檢視「超出範圍同步化」快取中的事件：

1. 在 Identity Console 中，選取「驅動程式」>「審查器「>「超出範圍同步化快取審查器」索引標籤。
2. 在「驅動程式」欄位中，指定您想要審查之驅動程式的完整可辨識名稱，或按一下瀏覽圖示以瀏覽並選取想要的驅動程式，然後按一下「確定」。

   只有當驅動程式未執行時，才能讀取驅動程式的快取檔案。如果驅動程式停止，則「驅動程式快取審查器」頁面將會顯示快取。如果驅動程式正在執行，則頁面會顯示「驅動程式未停止，無法讀取快取」備忘記事以代替快取項目。若要停止驅動程式，請按一下  按鈕，然後就能讀取和顯示快取。
   - **快取檔案名稱：**顯示快取的檔案名稱。
   - **伺服器上的驅動程式快取：**列出包含快取檔案例項的伺服器。如果驅動程式在多部伺服器上執行，您可以選取清單中的其他伺服器以檢視該伺服器的驅動程式快取檔案。
   - **「啟動 / 停止驅動程式」圖示：**顯示驅動程式目前的狀態，並可讓您啟動或停止驅動程式。快取只能在驅動程式停止時讀取。
   - **刪除：**選取快取中的項目，然後按一下  圖示以從快取檔案中將其移除。
   - **動作：**可讓您對快取檔案中的項目執行動作。按一下「動作」展開功能表，然後選取下列其中一個選項：
     - **快取摘要：**摘要快取檔案中儲存的所有事件。
     - **清除所有快取事件：**可讓您清除所有快取事件。

驅動程式資訊清單

「驅動程式資訊清單」就像驅動程式的履歷表。其中會說明驅動程式支援內容，並包含一些組態設定。驅動程式開發人員會提供「驅動程式資訊清單」。網路管理員通常不需要編輯「驅動程式資訊清單」。如果管理員想要編輯驅動程式資訊清單，可以藉由選取「驅動程式」>「審查器」>「驅動程式資訊清單」>「啟用 XML 編輯」選項來進行操作。

監控驅動程式的狀態

驅動程式狀態監控可讓您檢視驅動程式目前的狀態是綠色、黃色或紅色，以及定義為了回應每一個狀態所執行的動作。

由您建立的條件 (準則) 來決定每個狀態，也由您定義每當驅動程式的狀態變更時要執行的動作。例如，如果驅動程式狀態從綠色變成黃色，您可以執行的動作包括重新啟動驅動程式、關閉驅動程式以及向負責解決驅動程式問題的人員傳送電子郵件。

使用此模組可執行以下任務：

- 「修改驅動程式狀態條件」(第 166 頁)
- 「修改驅動程式狀態」(第 168 頁)
- 「建立自定狀態」(第 169 頁)
- 「修改自定狀態」(第 170 頁)

修改驅動程式狀態條件

由您控制決定每個健康狀態的條件。綠色狀態是用來表示功能正常的驅動程式，紅色狀態是用來表示功能不正常的驅動程式。

先評估綠色狀態的條件。如果驅動程式不符合綠色的條件，就會評估黃色的條件。如果驅動程式不符合黃色的條件，就會自動指定紅色健康狀態給驅動程式。

修改狀態的條件：

1 在 Identity Console 中，針對想要修改條件的驅動程式開啟「驅動程式狀態組態」頁面：

1a 開啟 Identity Console 首頁。

1b 選取 **「驅動程式」** > **按一下清單中的適當驅動程式** > **「審查器」** > **「驅動程式狀態組態」**。

2 按一下您想修改的狀態 (綠色或黃色) 的索引標籤。

索引標籤下會顯示該健康狀態目前的條件。條件是以群組的方式組織，可用邏輯運算子 AND 或 OR 來結合各個條件和各個群組。請考慮以下綠色狀態的範例：

```
GROUP1
Condition1 and
Condition2
Or
GROUP2
Condition1 and
Condition2 and
Condition3
```

在這個範例中，如果 GROUP1 條件或 GROUP2 條件其中的任何一個評估結果成立，就會指定綠色狀態給驅動程式。如果兩個條件群組都不成立，就會去評估黃色狀態的條件。

可以評估的條件有：

- **驅動程式狀態 :** 執行中、已停止、啟動中、不在執行中或關閉中。例如，綠色狀態的其中一個預設條件是驅動程式正在執行中。

- **快取溢位中的驅動程式 :** 用於保留驅動程式交易的快取狀態。如果驅動程式處於快取溢位的狀況，表示已經使用了所有可用的快取。例如，綠色狀態的預設條件是「快取溢位中的驅動程式」條件為 False，黃色狀態的預設條件是 「快取溢位中的驅動程式」條件為 True。
- **最新 :** 快取中最新交易的存留期。
- **最舊 :** 快取中最舊交易的存留期。
- **大小總計 :** 快取的大小。
- **未處理的大小 :** 快取中所有未處理交易的大小。
- **未處理交易 :** 快取中未處理交易的數目。可以指定所有交易類型或是特定交易類型 (如新增、移除或重新命名)。
- **交易歷程 :** 在一段指定時間內，「訂閱者」或 「發行者」通道中不同點所處理的交易數目。這個條件使用多個元素，其格式如下 :

  < *交易類型* > < *交易位置與期間* > < *關係運算子* > < *交易數目* >。

  - < *交易類型* >：指定要評估的交易類型。可以是所有交易、新增、移除、重新命名等等。
  - < *交易位置與期間* >: 指定 「訂閱者」或 「發行者」通道中的位置，以及要評估的期間。例如，您可以評估在過去 48 個小時中以 「發行者」報告事件處理的交易總數。交易歷程資料預設會保留兩週，這表示您不可以指定超過兩週的期間，除非您變更預設的 「交易歷程資料期間」設定。
  - < *關係運算子* >：指定找出到交易必須等於、不等於、小於、小於等於、大於或大於等於 < 交易數目 >。
  - < *交易數目* >：指定評估中要使用的交易數目。

  以下是 「交易歷程」條件的範例：

  < 新增的數目 > < 為發行者指令 > < 過去 10 小時 > < 小於 > <1000>

- **可用的歷程 :** 可用於評估的交易歷程資料的數量。這個條件的主要目的是要確保交易歷程條件不會使目前狀態失敗，因為它在評估的期間之內收集的交易歷程資料還不夠。

  例如，假設您想用交易歷程條件評估過去 48 小時中新增為出版者指令的數目 (前面「交易歷程」小節中的範例)。但是，如果還沒收集足夠 48 小時的資料，您不希望條件失敗，可能狀況是驅動程式的健康狀態組態剛設定之後或是驅動程式的伺服器重新啟動 (因為交易歷程資料是保留在記憶體中)。因此，您建立類似這樣的條件：

  Group1 可用的歷程 < 小於 > <48 小時 > 或 Group2 可用的歷程 < 大於或等於 > <48 小時 > 且交易歷程 < 新增的數目 > < 為發行者指令 > < 過去 48 小時 > < 小於 > <1000>

  如果任一個條件群組成立，狀態評估結果就成立，表示 a) 有小於 48 小時的資料，或 b) 有至少 48 小時的資料但在過去 48 小時內新增為 「發行者」指令的資料數目小於 1000。

  如果兩個條件都評估為 false，狀態評估就果就為 false，表示 a) 有至少 48 小時的資料，且 b) 在過去 48 小時內新增為出版者指令的資料數目大於 1000。

3 視需要修改條件。

- 若要新增新的群組，請按一下 **「條件群組」**旁邊的 ┼ 圖示。

- 若要新增條件，請按一下邏輯運算子 (AND/OR) 旁邊的 ➕ 圖示。或者，您也可以按一下「**新增新的條件**」連結。
- 若要重新排序條件群組或個別條件，請選取您要移動的群組或條件旁邊的核取方塊，然後按一下箭頭按鈕將其上下移動。您也可以使用箭頭按鈕，將群組中的條件移動到另一個群組中。

4 完成之後，按一下「**儲存**」按鈕以儲存您的變更。

5 如果您想要變更與您已設定之條件相關聯的動作，請繼續 「修改驅動程式狀態」(第 168 頁)。

修改驅動程式狀態

由您決定當驅動程式健康狀態變更時所要執行的動作。例如，如果狀態由綠色變為黃色，您可以關閉或重新啟動驅動程式、產生事件或起始工作流程。或者，如果狀態由黃色變為綠色，就會執行所有與綠色狀態相關的動作。

狀態的動作只會在每次符合條件時執行一次；只要狀態保持為 True，動作就不會重複。如果因為條件改變而使狀態變更，當下一次符合條件時，就會再度執行動作。

1 在 Identity Console 中，針對想要修改動作的驅動程式開啟「驅動程式狀態組態」頁面：

1a 開啟 Identity Console 首頁。

1b 選取「**驅動程式**」>**按一下清單中的適當驅動程式**>「**審查器**」>「**驅動程式狀態組態**」。

2 按一下「**綠色**」、「**黃色**」或「**紅色**」索引標籤以取得您想要修改其動作的狀態。

3 按一下「**動作**」標題旁的加號 (+) 圖示按鈕即可新增動作，然後選取您想要的動作類型：

- **Start Driver:** 啟動驅動策 { C
- **Stop Driver:** 停止驅動策 { C
- **重新啟動驅動程式：**停止然後啟動驅動程式。
- **清除驅動程式快取：**從快取中移除所有交易，包括未處理交易。
- **傳送電子郵件：**向一或多個收件者傳送電子郵件。要在電子郵件訊息主體中使用的範本必須已經存在。若要在電子郵件中包含驅動程式名稱、伺服器名稱與目前的狀態資訊，請將 $Driver$、$Server$ 和 $HealthState$ 記號新增至電子郵件範本，然後在郵件文字中包含這些記號。例如：

  ```
  The current health state of the $Driver$ driver running on $Server$ is $HealthState$.
  ```

  重要：若要向多個使用者傳送電子郵件，僅使用逗號 (，) 分隔每個電子郵件地址。不要使用分號。

- **寫入追蹤訊息：**如果未在「驅動程式狀態」工作上設定追蹤檔案，則將訊息寫入「驅動程式狀態」工作的記錄檔案或驅動程式集的記錄檔案。
- **產生事件：**產生可由 Audit 和 Sentinel 使用的事件。
- **執行 ECMAScript:** 執行現有的 ECMAScript。

如需如何建構 ECMA 程序檔的詳細資訊，請參閱 *「NetIQ Identity Manager - 使用設計工具來建立規則」*中的「在規則中使用 ECMAScript」。

- **啟動工作流程：**啟動佈建工作流程。
- **發生錯誤時：**如果動作失敗，指示剩下的動作、目前的狀態，以及驅動程式狀態工作要怎麼做。
  - **動作改變方式：**可以繼續執行剩下的動作、停止執行剩下的動作或預設為目前的設定。只有當您有數個「發生錯誤時」動作，且「動作改變方式」選項是設定在前述「發生錯誤時」動作的其中一個時，才能套用目前設定。
  - **狀態改變方式：**可以儲存目前狀態、拒絕目前狀態或預設為目前設定。儲存狀態會使狀態的條件評估為 True。拒絕狀態會使狀態的條件評估為 False。只有當您有數個「發生錯誤時」動作，且「狀態改變方式」選項是設定在前述「發生錯誤時」動作的其中一個時，才能套用目前設定。
  - **驅動程式狀態工作改變方式：**可以繼續執行工作、中止並停用工作或預設為目前設定。繼續執行工作會完成條件評估，決定驅動程式的狀態，並執行所有與狀態相關的動作。中止並停用工作會停止工作目前的活動，並關閉工作；一直到您啟用工作之後，才會再度執行。只有當您有數個「發生錯誤時」動作，且「驅動程式健康狀態工作改變方式」設定是設定在前述「發生錯誤時」動作的其中一個時，才能套用目前設定。

4 完成之後，按一下**「儲存」**按鈕以儲存您的變更。

建立自定狀態

您可以建立一或多個自定狀態，來執行與驅動程式目前狀態 (綠色、黃色、紅色) 無關的動作。不論目前狀態為何，只要符合自定狀態的條件，就會執行其動作。

當狀態為綠色、黃色、紅色時，自定狀態的動作只會在符合自定狀態的條件時執行一次；只要狀態仍然有效，動作就不會重複。如果因為條件改變而使狀態變更，當下一次符合條件時，就會再度執行動作。

1 在 Identity Console 中，針對您想要建立自定狀態的驅動程式開啟「驅動程式狀態組態」頁面：

  1a 開啟 Identity Console 首頁。

  1b 選取**「驅動程式」** > **按一下清單中的適當驅動程式** > **「審查器」** > **「驅動程式狀態組態」**。

2 按一下驅動程式狀態圖示 (綠色、黃色和紅色) 旁邊的 ┼ 圖示

3 遵循 「修改驅動程式狀態條件」(第 166 頁) 和 「修改驅動程式狀態」(第 168 頁) 中的指示以定義自定狀態的條件和動作。

修改自定狀態

若要修改自定狀態，請執行以下步驟：

1 在 Identity Console 中，針對您想要建立自定狀態的驅動程式開啟「驅動程式狀態組態」頁面：

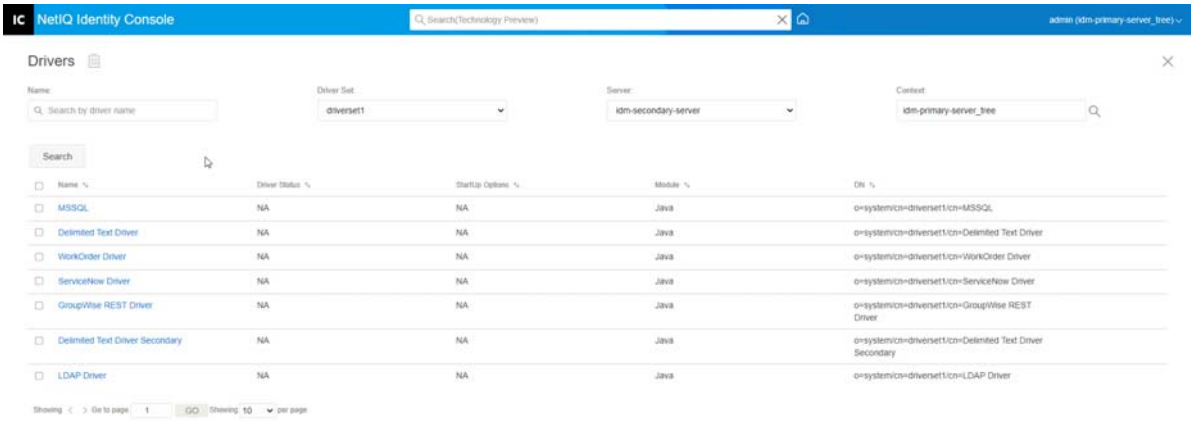
1a 開啟 Identity Console 首頁。

1b 選取**「驅動程式」**>**按一下清單中的適當驅動程式**>**「審查器」**>**「驅動程式狀態組態」**。

2 按一下驅動程式狀態圖示 (綠色、黃色和紅色) 旁邊的 圖示

3 遵循 「修改驅動程式狀態條件」(第 166 頁) 和 「修改驅動程式狀態」(第 168 頁) 中的指示以定義自定狀態的條件和動作。

圖 23-6 *管理驅動程式審查器*



24 管理驅動程式集統計資料

您可以使用 Identity Console 入口網站來檢視單一驅動程式或整個驅動程式集的各種統計資料。這包括各種依據類別 (新增、移除、修改等等) 的統計資料，例如快取檔案大小、快取檔案中未處理交易的大小、最舊和最新的交易，以及未處理交易的總數。若要檢視驅動程式集統計資料：

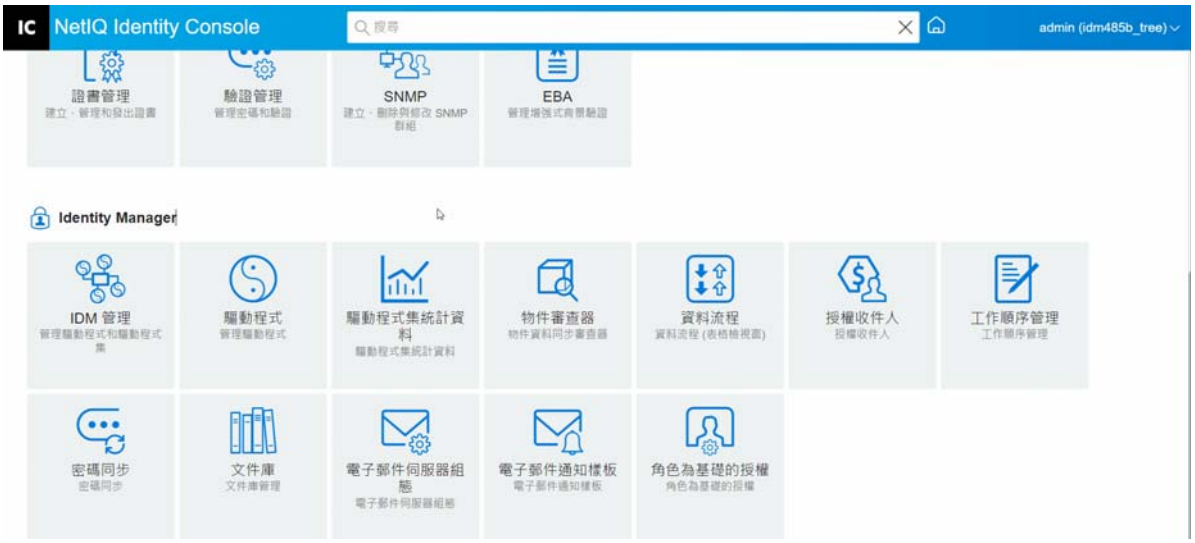
1 在 Identity Console 中，開啟 「驅動程式集統計資料」頁面。

2 從下拉式清單中選取適當的伺服器。

隨即顯示一個頁面，允許您檢視驅動程式集中包含的所有驅動程式的統計資料。

- 若要重新整理統計資料，請按一下 圖示。
- 若要關閉驅動程式的統計資料，請按一下驅動程式統計資料視窗右上角的 按鈕。
- 若要開啟所有驅動程式的統計資料，請按一下 「動作」 > 「全部顯示」。
- 若要收合驅動程式未處理交易的清單，請按一下位於清單上方的 按鈕。若要收合所有驅動程式未處理交易的清單，請按一下 「動作」 > 「收合所有交易」。
- 若要展開交易的清單，請按一下 按鈕。若要展開所有驅動程式未處理交易的清單，請按一下 「動作」 > 「展開所有交易」。
- 若要關閉已停用驅動程式的統計資料儀表板，請按一下 「動作」，然後選取 「關閉停用的驅動程式」。

圖 24-1 管理驅動程式集統計資料



25 審查 Identity Manager 物件

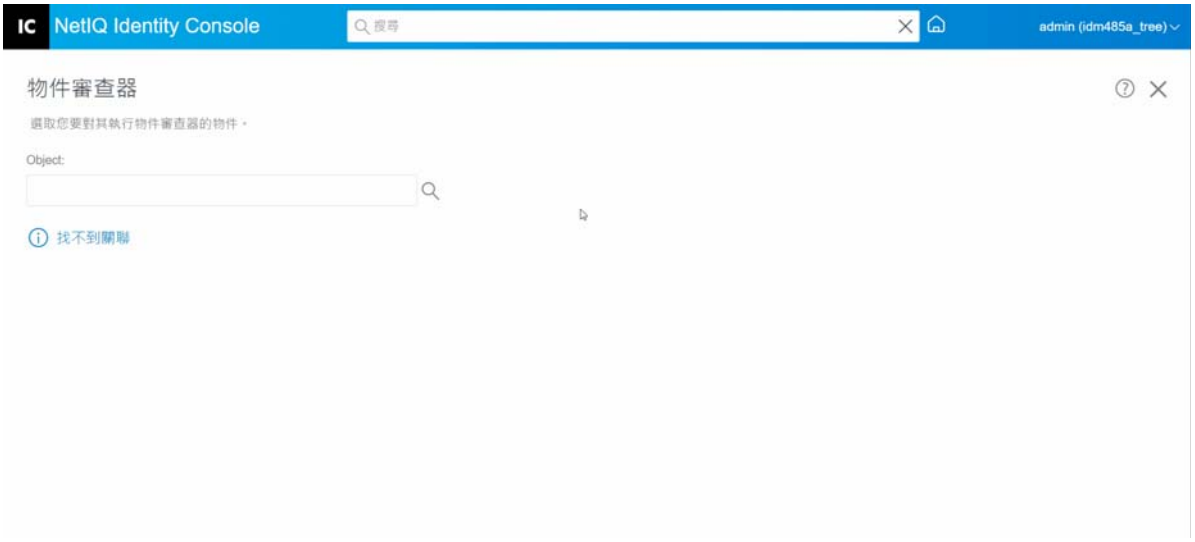
您可以使用「物件審查器」以檢視物件在 Identity Manager 關係中參與的詳細資訊。這些關係包括與物件相關聯的已連接系統、資料在 Identity Vault 與已連接系統間的流動方式、目前儲存於 Identity Vault 與已連接系統中的屬性值，以及已連接系統驅動程式組態等。

若要審查 Identity Manager 物件，請按一下 Identity Console 主頁面的 **「物件審查器」**選項。指定您想要審查之物件的完整可辨識名稱，或按一下瀏覽圖示以瀏覽並選取想要的物件。

「已連接系統」區段列出物件與之關聯的每個已連接系統。您可以使用 **「物件審查器」**頁面來執行以下動作：

- **新增關聯**：若要新增與已連接系統的新關聯，請按一下 ＋ 圖示。瀏覽並選取 **「整合驅動程式物件」**，然後指定 **「相關聯的物件 ID」**。
- **刪除關聯**：若要刪除與已連接系統的關聯，請選取該關聯左邊的核取方塊，然後按一下 🗑 圖示。若要刪除所有關聯，請選取「刪除」欄下的核取方塊，然後按一下 🗑 圖示。

圖 25-1 *審查 Identity Manager 物件*



26 管理資料流程

資料流程會以單一檢視窗，圖解多驅動程式的 「發行者」與 「訂閱者」通道。您可以使用此選項檢視和更新所有驅動程式的資料擁有權。

若要存取資料流程的表格檢視窗，請按一下 Identity Console 主頁面的 「資料流程 (表格檢視窗)」模組。然後，瀏覽並選取適當的容器以顯示驅動程式的清單。

若要管理個別驅動程式的資料擁有權，請執行以下步驟：

1 每個驅動程式都有兩個按鈕來管理通過 「發行者」和 「訂閱者」通道的資料流程。左側的按鈕管理 「發行者」通道上的資料流程，右側的按鈕管理 「訂閱者」通道上的資料流程。

   1a **同步化**：選取此選項以同步化特定屬性。選取此選項之後，「發行者」通道上的圖示會變更為 ↑，「訂閱者」通道上的圖示會變更為 ↓。

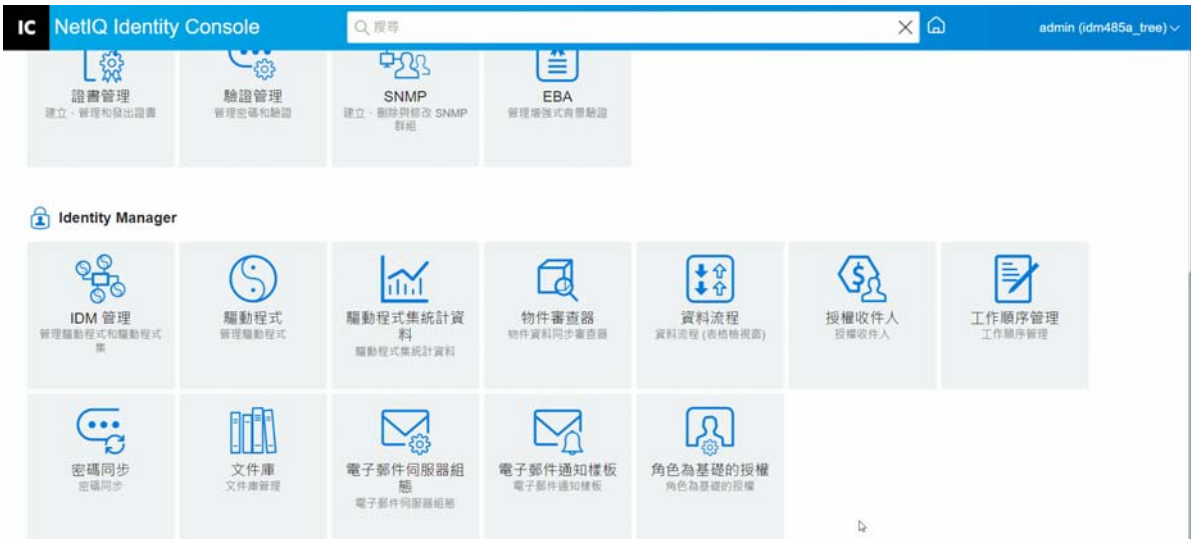
   1b **忽略**：選取此選項以停止同步化特定屬性。選取此選項之後，圖示會變更為 ⊘。

   1c **通知**：選取此選項以取得對特定屬性所做的任何變更的通知。但是變更不會自動同步化。選取此選項之後，圖示會變更為 🔔。

   1d **重設**：選取此選項將屬性值重設為其他通道指定的值。選取此選項之後，圖示會變更為 ↻。

   附註：您可以在 「發行者」通道或 「訂閱者」通道上設定此值。您不能同時在兩個通道上設定此值。

圖 26-1 管理資料流程



27 管理授權收件人

授權參考和結果會保存在已獲授權或授權已遭撤銷的物件上。授權參考和結果包含授權目前在該物件上授權或撤銷的相關資訊。授權收件者是任何包含對該授權參照的物件。

授權參考

若要檢視授權參考和結果，請按一下 Identity Console 主頁面的 「授權收件人」選項，然後選取 「授權參考」。然後填入為 DirXML-EntitlementRecipient 物件的 「完整可辨識名稱」。您可以按一下 「物件選擇器」 按鈕以選取物件。

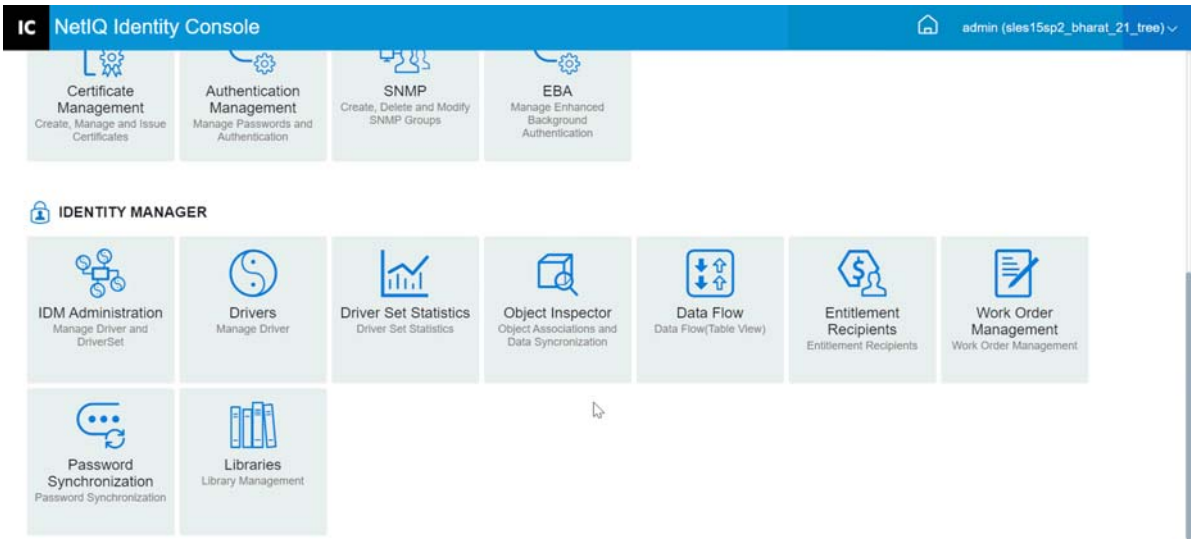
授權結果

「Identity Console 授權結果」表格列出與所選取物件相關聯的授權結果。若要檢視關聯授權，請選取 「授權 DN」。若要以 XML 格式檢視授權結果，請選取對應的 「結果 ID」。

- **授權結果欄標題**：欄標題包含授權的完整可辨識名稱、其目前所授予或撤銷的狀態、結果來源、結果狀態、任何附帶結果的訊息、結果時戳，以及結果識別。
  - **授權 DN**：按一下物件的授權完整可辨識名稱，開啟 「修改物件」頁面。此頁面可讓您檢視 eDirectory 屬性指定至物件上的方式。您亦可使用此頁面修改物件的屬性。「修改物件」頁面上顯示的類別數目取決於所選物件。
  - **狀態**：顯示授予還是撤銷授權。若外掛程式在 XML 資料流中找到其他值，會直接顯示該值。
  - **訊息**：DirXML shim 與結果狀態相關聯的任何訊息。資料儲存於 xml 結果檔案的 <msg></msg> 部份。按一 下 「結果 ID」項目，在 「XML 檢視器」頁面中查看結果的完整詳細資料。
  - **時戳**：授權引擎處理並寫入結果的時間。按一 下 「結果 ID」項目，在 「XML 檢視器」頁面中查看結果的完整詳細資料。
  - **結果 ID**：按一 下 「結果 ID」項目，在 「XML 檢視器」頁面中查看結果的完整詳細資料。當您檢視完此報告，請按一下 「關閉」。

  若要刪除授權結果項目，請按一下授權結果項目左邊的核取方塊，並選取 「刪除」。

圖 27-1 管理授權收件人



28 管理工作順序

Identity Manager 驅動程式可以建立工作順序，作為驅動程式所處理事件的結果。例如，如果您使用「人力資源」驅動程式 (SAP HR、PeopleSoft 等等)，您可以讓驅動程式在每當新增新的使用者時產生工作順序。

您可以使用 Identity Console 以建立和管理為支援此特定功能之各種驅動程式所建立的工作順序。

建立新的工作順序

若要建立新的工作順序，請執行下列步驟：

1 從 Identity Console 抵達頁面，按一下「工作順序」選項。

2 按一下 ＋ 圖示以建立新的工作順序。

3 指定工作順序的名稱，然後按一下「確定」。

名稱用於 Identity Vault 中 WorkOrder 物件的名稱。

4 填寫下列欄位：

狀態：新工作順序的狀態可以是「等待中」或「保留」。一般而言，工作順序的狀態為「等待中」。您可選取「暫停」，停止工作順序。處理工作順序之後，產生的工作順序狀態會顯示於此欄位中。

截止日期：您可以選擇讓驅動程式立即執行工作順序，也可以排程工作順序的執行時間。若要安排「到期日期」，請按一下行事曆圖示。使用行事曆來選擇日期。使用箭頭選取月、年與時間。

重複工作順序：選取此選項，以便多次處理工作順序。選擇週、日、小時或分鐘數指定時間間隔，工作順序才能重複。除非手動刪除、編輯或驅動程式傳回錯誤訊息，否則工作順序會在「刪除日期」停止重複。

刪除日期：使用行事曆控制來選取日期，在該日期刪除已設定的工作順序。除非您選取「即使工作順序有錯誤，也刪除工作順序」，否則不會刪除具有錯誤狀態的工作順序。

隸屬工作順序：建立新工作順序時，您可將其設為隸屬於一或多個工作順序。按一下 以瀏覽並選取相關工作順序。若要從清單中移除工作順序，請選取工作順序，然後按一下 。

類型：使用此欄位以指定工作順序類型。驅動程式不會變更這個屬性。在工作順序的處理期間，這個屬性會傳送到 WorkToDo 物件。

工作順序編號 : 唯一工作順序號碼。您可使用 NetIQ eDirectory 以外的企業工作順序系統指定此值，如工作順序資料庫。

聯絡資訊 : 負責此工作順序的人員連絡資訊。

工作順序處理記錄 : 處理工作順序之後，驅動程式會記錄工作順序結果，包括此欄位中的狀態。這樣可讓您檢查工作順序的目前狀態，並識別驅動程式在嘗試設定驅動程式組態時遇到的任何問題。

工作順序狀態屬性會保留為等待中，直到工作順序處理完成為止。工作順序在到期日到期時處理。驅動程式會將狀態屬性設定為 「已設定組態」、「警告」或 「錯誤」，報告處理結果。若工作順序為 「保留」，則會忽略該工作順序。

- **等待中 :** 驅動程式正在等待到期日期，完成工作順序。
- **已設定組態 :** 已成功處理工作順序。
- **錯誤 :** 驅動程式無法執行工作順序。
- **警告 :** 有關於工作順序的警告。例如，若工作順序為隸屬工作順序，有較晚的到期日期，則驅動程式會傳送警告。

描述 : 工作順序描述。

工作順序內容 : 驅動程式規則會使用此欄位中的資料處理工作順序。例如，這可能是「指令轉換」用來處理工作順序的 XML。

刪除現有工作順序

若要刪除現有工作順序，請執行以下步驟 :

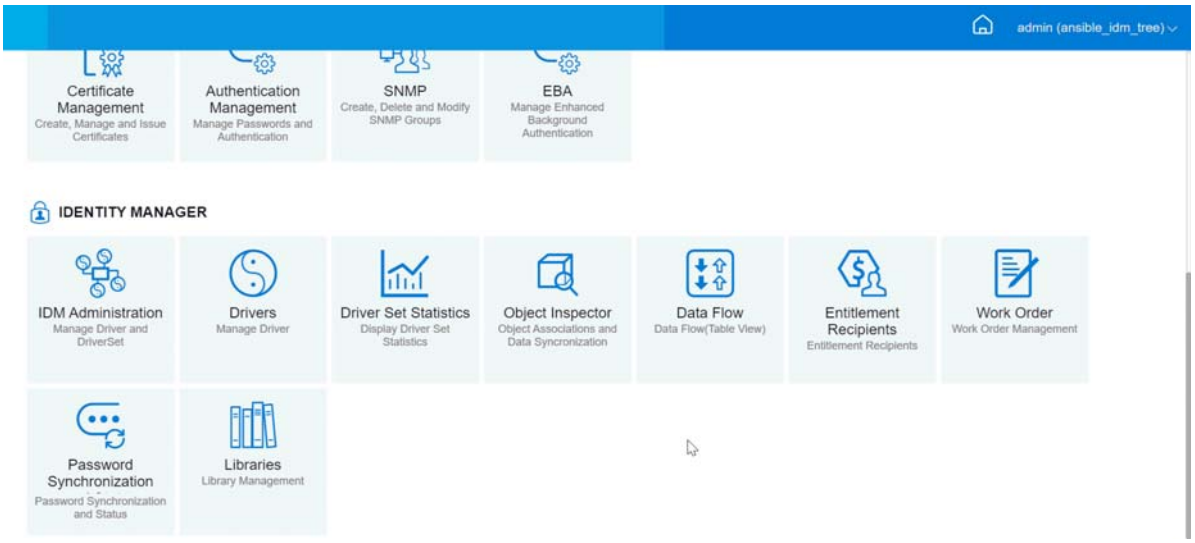
1. 從 Identity Console 抵達頁面，按一下 **「工作順序」**選項。
2. 選取要刪除的工作順序。
3. 按一下 圖示。

篩選工作順序清單

若要篩選出工作順序清單，請執行以下步驟 :

1. 從 Identity Console 抵達頁面，按一下 **「工作順序」**選項。
2. 按一下 「工作順序管理」底下的 **「動作」**。
3. 從下拉式功能表中，選取過濾類型 :
   - **顯示全部**： 列出與驅動程式關聯的所有工作順序。
   - **已設定組態 :** 僅列出與驅動程式關聯的已設定工作順序。
   - **錯誤 :** 僅列出具有錯誤狀態的工作順序。
   - **保留 :** 列出已手動放置於保留的工作順序。
   - **等待中 :** 列出尚未到期的工作順序。

圖 28-1 管理工作順序


admin (ansible_idm_tree)
Certificate Management
Create, Manage and Issue Certificates
Authentication Management
Manage Passwords and Authentication
SNMP
Create, Delete and Modify SNMP Groups
EBA
Manage Enhanced Background Authentication
IDENTITY MANAGER
IDM Administration
Manage Driver and DriverSet
Drivers
Manage Driver
Driver Set Statistics
Display Driver Set Statistics
Object Inspector
Object Associations and Data Syncronization
Data Flow
Data Flow(Table View)
Entitlement Recipients
Entitlement Recipients
Work Order
Work Order Management
Password Synchronization
Password Synchronization and Status
Libraries
Library Management

29 管理密碼狀態和同步

您可以使用 Identity Console 入口網站，驗證個別驅動程式的密碼同步和密碼狀態。若要驗證，請從 Identity Console 主頁面選取 「密碼同步」模組。

您可以使用此模組來執行下列動作：

- 「檢查密碼同步狀態」(第 183 頁)
- 「驗證密碼同步設定」(第 184 頁)

檢查密碼同步狀態

您可以判定特定使用者的 「配送密碼」是否與已連接系統中的密碼相同。執行以下步驟以檢查密碼同步狀態：

1. 在 Identity Console 中，選取 「密碼同步」 > 「密碼狀態」。
2. 瀏覽並選取要檢查其密碼狀態的使用者。
3. 可看到以下密碼狀態：
   - 密碼為同步。
   - 密碼未同步。
   - 密碼狀態未知，因為無法連上已連接系統，或需要檢查密碼。
   - 發生錯誤。

附註：若要查看關於上述每個狀態的更多詳細資料，您必須將滑鼠滑向**密碼狀態**欄位下的狀態。

「密碼狀態」任務會使驅動程式執行 「檢查物件密碼」動作。不是所有驅動策〇业銑店 K 碼檢查。必須在驅動程式的資訊清單中包含密碼檢查功能。Identity Console 不允許將密碼檢查操作傳送至在資訊清單中不包含此功能的驅動程式。

「檢查物件密碼」動作會檢查 「配送密碼」。如果 「配送密碼」不在更新中，則 「檢查物件密碼」可能會回報密碼沒有同步化。

如果發生下列任何一種情況，「配送密碼」將不會更新：

- 您使用的同步方法是使用 「NDS 密碼」來同步或使用 「通用密碼」來同步。如需詳細資訊，請參閱 「使用自定設定來建立密碼規則」(第 112 頁)。

附註：「密碼狀態」動作會檢查 「NDS 密碼」，而不是檢查 Identity Vault 的 「通用密碼」。因此，如果使用者的密碼規則未指定為同步 「NDS 密碼」與 「通用密碼」，則會一直將密碼報告為未同步。事實上，「配送密碼」和已連接系統上的密碼可能已同步，但 「檢查密碼狀態」不會是正確的，除非 「NDS 密碼」和 「配送密碼」都與 「通用密碼」同步。

驗證密碼同步設定

「密碼同步」可讓您使用 Identity Manager 同步已連結系統之間的密碼。若要檢視已連結系統的 「密碼同步」設定，請從下拉式清單選取適當的驅動程式集。

您可以使用 「密碼同步化」來設定已連接系統執行以下項目：

- 發行密碼至 Identity Manager。
- 訂閱 Identity Manager 或其他已連接系統的密碼。
- 在已連接系統上強制執行 「密碼規則」。
- 傳送通知電子郵件。

執行以下步驟以檢查密碼同步設定 :

1. 在 Identity Console 中，從主頁面選取 **「密碼同步」** > **「密碼同步」**。
2. 選取包含您想要檢查其設定之驅動程式的驅動程式集。
3. 按一下清單中的驅動程式名稱。

   附註：啟用和停用的設定因驅動程式而異。只有驅動程式支援的功能設定可用。

4. 驗證設置是否正確設定。

   Identity Manager 接受密碼 (發行者通道): 如果啟用此選項，則 Identity Manager 允許已連接系統中的密碼流向 Identity Vault。停用此選項表示不允許任何 <password> 元素流向 Identity Manager。「發行者」通道上的密碼同步化規則會將 XML 中的這些元素去除。

   此設定會套用到已連接系統本身提供的使用者密碼，以及使用 「發行者」通道上的規則所建立的密碼值。

   如果啟用此選項但是停用以下的 「配送密碼」選項，則來自已連結系統的 <password> 值會直接寫入 Identity Vault 中的 「通用密碼」。如果使用者的密碼規則未啟用 「通用密碼」，密碼會寫入 「NDS 密碼」。

   使用 「配送密碼」進行密碼同步化 : 只有在 **「Identity Manager 接受密碼 (發行者通道)」** 設定已啟用時，才能使用此設定。

   如果此選項啟用，則來自已連接系統的密碼值會寫入 「配送密碼」。「配送密碼」可以還原，這表示該密碼可從 Identity Vault 資料儲存中擷取以進行密碼同步化。Identity Manager 可使用此功能與已連接系統進行雙向密碼同步化。如需 Identity Manager 將密碼從這個系統配送到其他系統，則必須啟用此選項。

   只有在密碼遵守使用者的 「密碼規則」時才接受密碼 : 只有在 **「使用配送密碼進行密碼同步」** 設定已啟用時，才能使用此設定。

   如果選取此選項，除非密碼遵守符合使用者的密碼規則，否則 Identity Manager 不會將此已連接系統的密碼寫入 Identity Vault 的 「配送密碼」，或將密碼發行至已連接系統。

   如果密碼未遵守規則，則啟用 **「將使用者的密碼重設為配送密碼」** 設定，重設已連接系統上的使用者密碼。這樣可讓您在已連接系統和您的 Identity Vault 中強制執行密碼規則。如果您未選取此選項，則使用者密碼會在已連結系統上變成未同步化。但是，在決定是否使用此選項時，您需要考量已連接系統的密碼規則。有些已連接系統不允許重設密碼，因為這些系統不允許您有重複的密碼。

藉由使用**透過電子郵件，向使用者通知密碼同步失敗設定**，您可以在無法設定密碼或重設密碼時通知使用者。通知功能對於此選項特別有用。如果使用者變更已連接系統允許，但 Identity Manager 因密碼規則之故而拒絕的密碼，則使用者在收到通知或嘗試使用舊密碼登入已連接系統之前，無法知道密碼已重設。

永遠接受密碼；忽略「密碼規則」：只有在**「使用配送密碼進行密碼同步」**設定已啟用時，才能使用此設定。

如果您選取此選項，Identity Manager 不會強制執行此已連接系統的使用者密碼規則。Identity Manager 會將密碼從已連結系統寫入 Identity Vault 中的「配送密碼」，並且將密碼配送到其他已連接系統，無論是否遵守密碼規則。

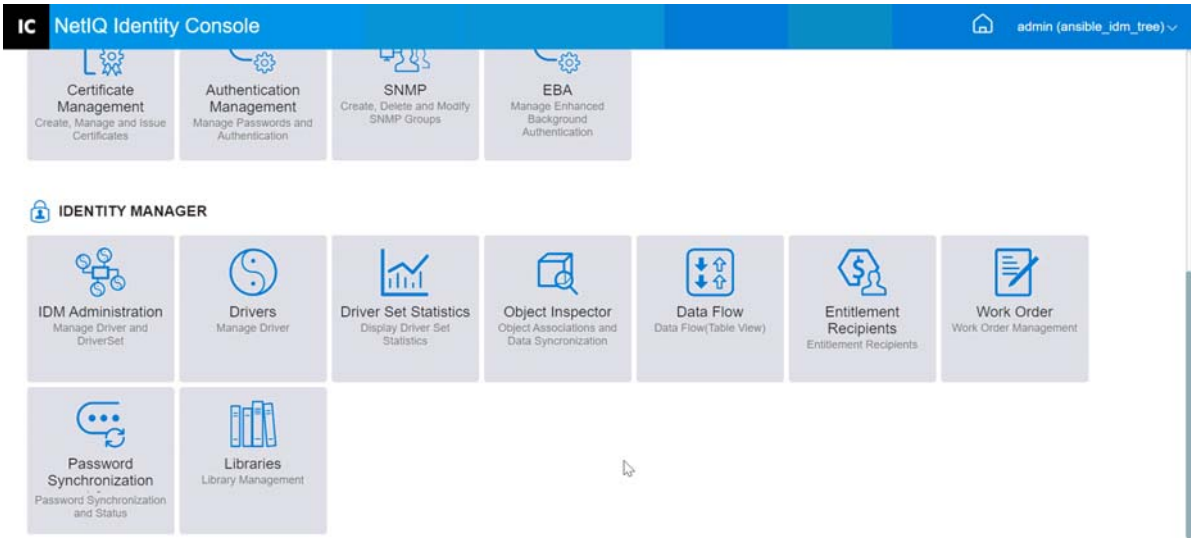
應用程式接受密碼 (訂閱者通道): 如果您啟用此選項，驅動程式會將 Identity Vault 的密碼傳送至此已連接的系統。這也表示如果使用者在其他已連接系統上變更密碼，而該系統將密碼發行至 Identity Vault 的「配送密碼」，則會變更此已連接系統上的密碼。

依照預設，「配送密碼」和 Identity Vault 中的「通用密碼」相同，因此對 Identity Vault 中「通用密碼」的變更也會傳送到已連接的系統。

透過電子郵件通知使用者密碼同步化失敗：如果您啟用此選項，則傳送電子郵件通知使用者密碼是否未同步化、設定或重設。傳送給使用者的電子郵件是以電子郵件範本為基礎。此範本由「密碼同步化」應用程式提供。但是，為了讓範本有作用，您必須自訂範本，並指定要傳送通知訊息的電子郵件伺服器。如需指示，請參閱 *《NetIQ Identity Manager 密碼管理指南》*中的「設定電子郵件通知」。

5 完成之後，按一下**「儲存」**以儲存變更。這些設定會儲存為「全域組態值」。

圖 29-1 *管理密碼同步化*



30 管理程式庫

程式庫物件會儲存由一或多個驅動程式共用的多個規則和其他資源。程式庫物件可以在驅動程式集物件或任何 eDirectory 容器中建立。多個程式庫可以存在於 eDirectory 網路樹中。只要執行驅動程式的伺服器保留程式庫物件的讀取 / 寫入或主複製本，驅動程式可以參考網路樹中的程式庫。

樣式表、規則 (Policy)、規則 (Rule) 和其他資源物件可以儲存在程式庫中，並由一或多個驅動程式參考。

使用程式庫管理模組，您可以執行以下任務：

檢視和刪除現有程式庫

若要檢視和刪除現有程式庫，請執行以下步驟：

1. 在 Identity Console 中，從首頁選取「**程式庫**」模組。
2. 從清單中選取適當的程式庫。
3. 按一下 圖示。按一下**確定**以確認。

從程式庫檢視和刪除物件

您可以從程式庫物件檢視和刪除規則和對應表。若要刪除物件，請執行以下步驟：

1. 在 Identity Console 中，從首頁選取「**程式庫**」模組。
2. 從清單中按一下適當的程式庫。
3. 若要刪除規則，請選取「**規則**」索引標籤。
4. 從清單選取適當的規則，然後按一下 圖示。
5. 若要刪除對應表，請選取「**對應表**」索引標籤。
6. 從清單選取適當的對應表，然後按一下 圖示。
7. 按一下**確定**以確認。

圖 30-1 管理程式庫


IC
NetIQ Identity Console
搜尋
admin (idm485b_tree)
證書管理
建立、管理和發出證書
驗證管理
管理密碼和驗證
SNMP
建立、刪除與修改 SNMP 群組
EBA
管理增強式商業驗證
Identity Manager
IDM 管理
管理驅動程式和驅動程式集
驅動程式
管理驅動程式
驅動程式集統計資料
驅動程式集統計資料
物件審查器
物件資料同步審查器
資料流程
資料流程 (表格檢視器)
授權收件人
授權收件人
工作順序管理
工作順序管理
密碼同步
密碼同步
文件庫
文件庫管理
電子郵件伺服器組態
電子郵件伺服器組態
電子郵件通知樣板
電子郵件通知樣板
角色為基礎的授權
角色為基礎的授權

31 管理電子郵件伺服器選項

您可以使用「電子郵件伺服器選項」指定 SMTP 電子郵件伺服器的設定。

主機名稱

您 SMTP 電子郵件伺服器的主機名稱。這可以是 IP 位址。您還可以指定一個自訂連接埠，後接主機名稱或 IP 位址。

重要：使用冒號 (:) 來分隔主機名稱或 IP 位址與連接埠。

自

您可以指定一個有效的電子郵件地址，該地址將顯示為電子郵件標頭的「寄件者」欄位。

逾時值

逾時選項可讓您設定傳送通知電子郵件的時間限制 (以秒為單位)。

啟用 SSL

如果需要，您可以選擇啟用 SSL 選項。

使用身分證明驗證伺服器

使用安全 SMTP 伺服器。若您的伺服器需要在傳送電子郵件前進行驗證，請在此只定使用者名稱與密碼。

雖然已在此指定驗證資訊，您可能還需要在傳送通知電子郵件的不同應用程式個別指定。

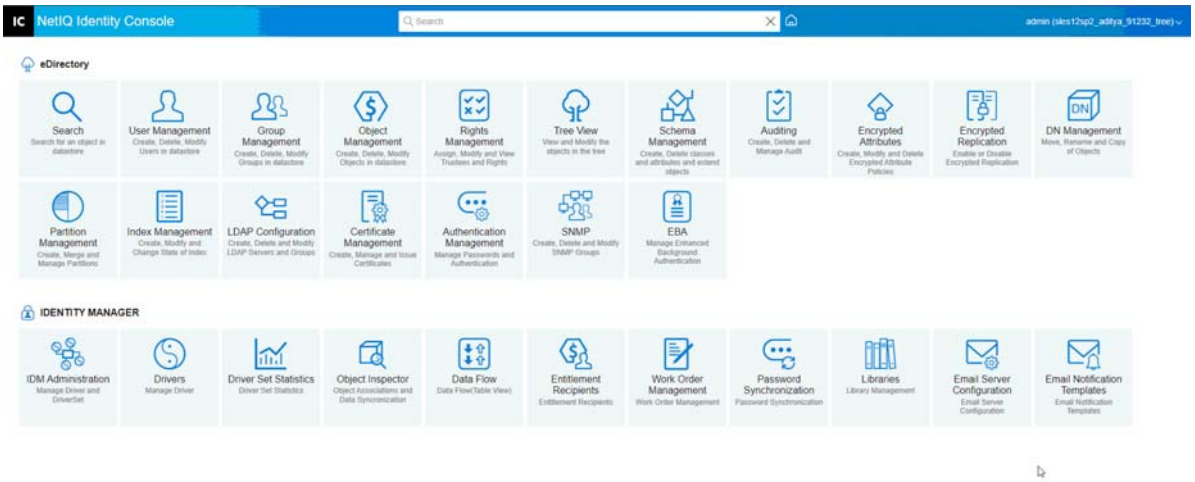
例如，您可使用在此指定的驗證資訊，傳送「忘記密碼」電子郵件通知。但 Identity Manager Password Synchronization 使用驅動程式規則傳送通知電子郵件。您也必須在該驅動程式規則中提供驗證資訊。

若要對伺服器進行驗證，請執行以下步驟：

1. 選取 **「使用身分證明驗證伺服器」**選項。
2. 指定 **「使用者名稱」**與 **「密碼」**。
3. 按一下 **「測試伺服器連線」**以驗證連接性。
4. 按一下 **「儲存」**。

附註：儲存身分證明詳細資料後，**「測試伺服器連線」**將會停用。

圖 31-1 電子郵件伺服器組態



32 管理電子郵件範本

此清單顯示可用的通知範本。您可使用這些範本，傳送電子郵件訊息給此網路樹中的使用者。您可以使用自己的文字自定這些範本。

某些應用程式會提供自己的範本。這些「範本」物件位於「保全性」容器中，通常可在您網路樹的根部找到。

您可依名稱、日期或標題排序清單。

標題

使用者在電子郵件「標題」所看到的文字。若要編輯範本，請按一下範本的「標題」的標頭。透過使用「編輯電子郵件通知範本」介面，您可以修改範本及其詳細資料。

範本名稱

各範本都有唯一名稱。應用程式寄送的電子郵件會提到此名稱。

上次修改

上次修改範本的日期與時間。

新增

可讓您建立新電子郵件範本。

1. 按一下 ＋ 圖示。
2. 輸入新範本的名稱 (例如，「核准」)，再按一下 **「確定」**。

若您已停用快顯，會回到「編輯電子郵件通知範本」快顯。「名稱」欄會呈現新範本名稱，但「標題」標頭欄會出現 [無標題]。若這樣的話，請按一下 [無標題]，提供新範本中的詳細資料。

編輯電子郵件通知範本

「編輯電子郵件通知範本」頁面可讓您修改電子郵件範本。您可以使用自己的文字自定範本。

範本名稱

顯示範本的名稱。

標題

使用者在電子郵件「標題」所看到的文字。您可變更「標題」行的文字。範本的實際名稱仍保持相同。

傳送為

SMTP 伺服器用來傳送電子郵件的格式：文字或 HTML。

記號或替代標記

這些替代標記可協助您針對使用者製作個人化訊息。您可從可用標記清單中複製替代標記，並將標記貼上至訊息中。

每個範本都包含預設記號或替代標記，也就是使用者自定電子郵件所需的變數。例如，要傳送密碼給使用者的「忘記密碼」電子郵件範本，就包含名為 'CurrentPassword' 的預設記號或替代標記。

新增：您可定義其他替代標記，用於訊息本文。

若要新增記號或替代標記，請執行以下步驟：

1. 按一下  圖示。
2. 在 **「新增替代標記」**視窗中指定 **「名稱」**和 **「描述」**。
3. 按一下 **「確定」**。
4. 新記號或替代標記列在「替代標記」欄中。

複製標記：按下  以將所選標記複製到系統緩衝區，然後您可以按下滑鼠將其黏貼，並在訊息的標題行或本文中使用。

刪除：在清單中選取記號或替代標記，然後按下  以從清單中刪除標記。請確認您不會移除訊息本文所需的標記。

訊息本文

電子郵件訊息的文字。

在指定所有電子郵件通知範本修改後，按一下 **「更新」**。

刪除

(從 Identity Vault) 移除您建立的範本。您無法刪除 Identity Manager 等應用程式附帶的預設範本。

1. 選取您要刪除的範本。

   若您按一下範本「標題」標頭，Identity Console 會提供「編輯電子郵件範本」對話方塊。
2. 按一下「刪除」圖示。
3. 按一下**確定**。

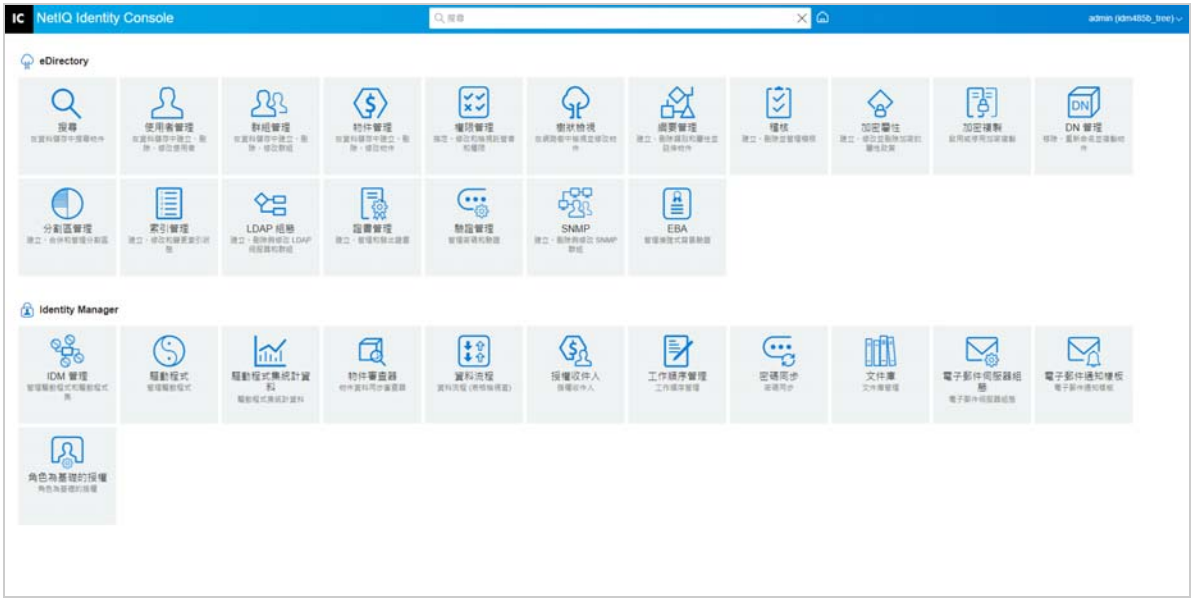
篩選範本

使您能夠篩選要顯示的電子郵件範本。僅顯示選取的範本。「篩選全部」選項會顯示所有的範本。

重新整理範本

按一下 圖示可重新整理並移除任何套用的篩選器範本。

圖 32-1 *電子郵件通知範本*



33 管理角色型授權

RBE 可讓您將已連結系統上的授權授予一組「NetIQ® 身分主控台」使用者。使用 RBE 規則，您可以對企業規則進行有效管理，並減少設定 Identity Manager 驅動程式的必要。

「角色型授權」模組具有下列功能：

- 「角色型授權」(第 195 頁)
- 「重新評估成員資格」(第 203 頁)

角色型授權

RBE 規則是「身分主控台」動態群組物件，加入了額外的功能，可讓您授予所連結系統上的 RBE。當您建立 RBE 規則時，您會定義規則和授權的成員資格，這兩者應授予給 RBE 規則的成員。每個 RBE 規則皆與指定給特定伺服器的單一「驅動程式集」物件相關聯。與 Identity Manager 驅動程式類似，每個「授權」規則只能管理其指定伺服器上主複製本或讀 / 寫複製本中的物件。

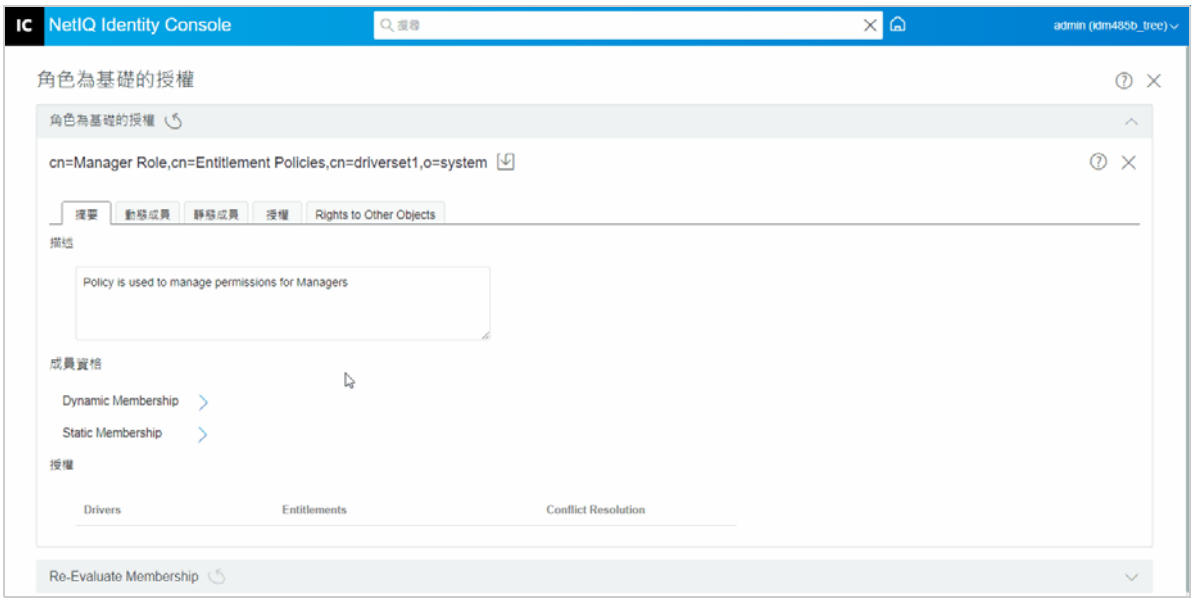
以下各節詳細說明角色為基礎的授權：

- 「總結」(第 195 頁)
- 「動態成員」(第 197 頁)
- 「靜態成員」(第 199 頁)
- 「授權」(第 199 頁)
- 「其他物件的權限」(第 200 頁)
- 「設定 RBE 規則的優先順序」(第 202 頁)

總結

此頁面摘要「授權」規則的成員資格準則與授權高階層檢視。

圖 33-1 摘要頁



成員：

以 LDAP 過濾器的語法顯示動態成員資格的指定準則。搜尋 「身份」指示查詢動態成員資格時使用何物件權限，「基礎 DN」和 「範圍」指示查詢要包含網路樹的哪個部份。

您可選取核取方塊，檢視包含與排除的靜態成員資格。

所有成員的合併清單不會顯示於 「摘要」頁面，因為此清單應該很長。若要檢視 「授權」規則中，包括動態與靜態的所有成員的合併清單，請使用 「成員資格」 >「檢視成員資格」索引標籤。

授權：

授予 「授權」規則成員的已連接系統上授權。請記住，「角色授權」與已連接系統之間的一致性並不是十分健全。這表示已連接系統上的授權狀態並不會顯示於 「授權規則」介面中。若您將授權授予 「授權規則」，稍後無法在已連接系統上使用該授權，但授權仍會列於 「授權規則」清單中，直到您手動從清單移除為止。

衝突解決：

對於具有值的 RBE，若有兩個或更多 RBE 規則將不同值授予使用者時，可使用這些方法判斷使用者被授予哪個值。具有值的授權範例為，電子郵件配送清單中的成員，其中配送清單名稱即為值。

各驅動程式物件上的個別授權，會分別設定衝突解決方法。若某授權用於多個 RBE 規則，則所有 RBE 規則會使用相同的衝突解決方法。若要變更某授權的衝突解決方法，請在驅動程式的驅動程式資訊清單中變更授權設定。

- **無法辨識：**未於精靈中完成 RBE 規規，或驅動程式資訊清單中的設定輸入錯誤。
- **合併：**預設設定為 「合併」 (在驅動程式資訊清單中為結合)。這表示使用者會被授予其所屬所有 RBE 規則中，此授權的所有值。

  使用 「合併」預設值時，規則清單優先程度順序對此特定授權而言並不重要。

例如，使用者被 「管理員」規則與 「小組成員」規則這兩個不同的 RBE 規則，授予 GroupWise® 驅動程式 A 的電子郵件配送清單成員資格。在 「規則 1」中，使用者被授予 「管理員」電子郵件配送清單的成員資格，而在 「規則 2」中，使用者被授予 「小組成員」電子郵件配送清單的成員資格。透過 「合併」設定，使用者會同時被授予兩個電子郵件配送清單的成員資格。

- **優先順序：**此設定表示若有多個 RBE 規則對某使用者授予相同驅動程式物件中、相同授權的不同值，則使用者只會被授予清單中最高優先順序之的 RBE 規則所指定的值。

  使用 「優先程度」設定時，規則清單優先程度順序對此特定授權而言就很重要。

  例如，使用者被 「管理員」規則與 「小組成員」規則這兩個不同的 RBE 規則，授予 GroupWise 驅動程式 A 的電子郵件配送清單成員資格。在 「管理員」規則中，使用者被授予 「管理員」電子郵件配送清單的成員資格，而在 「小組成員」規則中，使用者被授予 「小組成員」電子郵件配送清單的成員資格。「管理員」規則在規則清單中的位置高於 「小組成員」規則。透過 「優先程度」設定，使用者僅會被授予 「管理員」電子郵件配送清單的成員資格。

  舉例來說，當已連接系統上的屬性只允許單一值時，使用優先程度進行衝突解決便十分有用。若兩個不同的 RBE 規則將該屬性的值授予相同使用者，則該使用者會收到清單中位置最高之 RBE 規則所授予的值。

附註：沒有值的授權，如帳戶，並不會提供衝突解決設定。無論規則在清單中的優先順序為何，不具有值的授權一律授予 RBE 規則的成員。

動態成員

以 LDAP 過濾器的語法顯示動態成員資格的指定準則。搜尋 「身份」指示查詢動態成員資格時使用何物件權限，「基礎 DN」和 「範圍」指示查詢要包含網路樹的哪個部份。

成員資格篩選器

您可定義成員資格的準則，例如在網路樹中的位置和物件屬性。例如，成員資格可取決於使用者是否為使用中容器，或取決於工作標題是否包含 「管理員」字眼。符合該準則的使用者會自動成為 RBE 規則的成員，而無需特別將每個使用者新增至規則。動態成員資格與 「動態群組」物件相同。

若物件有所變更，而無法符合動態成員資格的任何準則，則下次重新評估使用者時，授權會自動撤銷。

設定搜尋參數

指定您要「授權」規則管理的使用者位置。選擇保有使用者的容器 (基本 DN)，以及您要容器搜尋到多遠的位置 (搜尋範圍)。如需「授權」規則管理您所指定容器中的使用者，使用者必須在伺服器的讀 / 寫複製本或主複製本中。

提供以下用於「搜尋範圍」的選項：

- 此容器和此子容器：在網路樹中，位於此容器以下的使用者如果符合為動態成員資格指定的準則，則均為「授權」規則的成員。子容器中的使用者如果符合準則，也會是成員。
- 此容器僅適用於：此容器中的使用者只有在符合動態成員資格特定的準則下，才為「授權」規則的成員。在此容器之下子容器中的使用者，即使符合準則，仍不是成員。

定義過濾器準則

指定決定哪些使用者是「授權」規則之成員的特性。

在「授權」規則的「摘要」頁面中，您所指定的動態成員資格準則會以 LDAP 過濾器的語法顯示。

依照預設，動態成員資格會設定為將所有使用者類別物件 (和自使用者類別衍生的類別物件) 包含在搜尋範圍內，作為「授權」規則的成員。

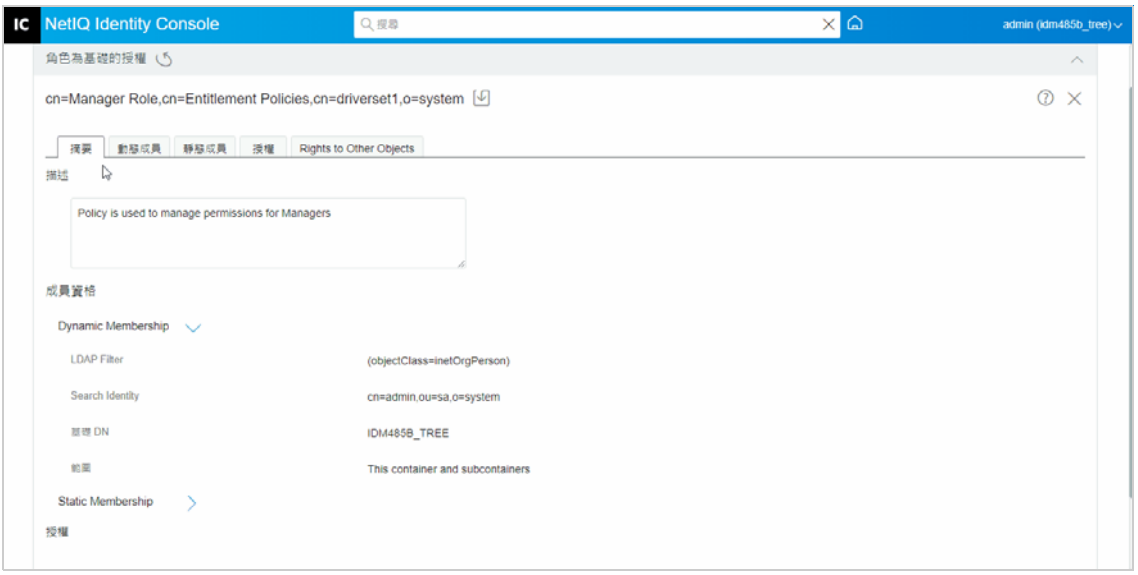
附註：如果您建立衍生自使用者的新物件類別，則現有「授權」規則不會察覺到該類別，直到您修改「授權」規則。這可防止不小心將授權授予新類別的使用者。在對「授權」規則進行任何修改後，會更新該規則的使用者衍生類別清單。

建立動態成員資格

在「動態成員」索引標籤上，執行下列作業：

1. 按一下 **「動態成員」**索引標籤。
2. 根據需要使用 **「搜尋身分」**、**「開始搜尋位置」**和 **「搜尋範圍」**篩選器。
3. 按下特定的 **「建立群組」**以建立新條件或列，然後提供所需的搜尋準則或條件。

圖 33-2 動態成員



搜尋範圍：「搜尋範圍」指出位於搜尋基本 DN 或之下的項目集，這些項目可能會視為搜尋作業的潛在相符項目。

搜尋準則：您可限制某個搜尋，以協助您從大量記錄中找出特定記錄或記錄群組。

基本 DN：基本 DN 是伺服器搜尋使用者的點。

LDAP 群組：這是個 「使用者」、「群組」和 「組織單位」的階層式組織，其為使用者和群組的容器。

附註：使用者可以建立具條件的單一或多個群組。條件包含屬性、運算子和值。依預設，填入 「物件類別」 > 「等於」 > 「使用者」。

靜態成員

靜態成員是使用靜態關鍵字聲明的成員類別。靜態成員具有特定的有限存取權。

在 「靜態成員」索引標籤上，可以執行以下操作：

包括成員：

以靜態方式新增動態成員資格過濾器未包含的成員。

排除成員：

排除符合過濾器準則，但不應包含於授權規則中的成員。

授權

RBE 可讓您在連接的系統上授予授權，並在 Identity Manager 中授予權限。「授權」可為下列任一：

- 已連接系統上的帳戶 .

- 已連接系統上電子郵件通訊群組清單的成員資格 .
- 已連接系統上的群組成員資格 .
- 已連接系統中相對應物件的屬性，已對其填入您指定的值 .

附註：「授權」功能是 Identity Manager 的一部分，所以您必須先安裝 Identity Manager 驅動程式，並將其組態設定為支援「授權」，之後您才能在連接的系統上授予授權。

建立授權

在「授權」索引標籤上，執行下列作業：

1 按一下「**授權**」索引標籤。

2 按一下 ＋ 以 **新增驅動程式**，並在已連結系統上提供授權。

「新增驅動程式」畫面隨即顯示。

3 從下拉式選單中選取驅動程式。

4 按一下**新增**。

「新增授權」畫面隨即顯示。

5 從下拉式選單**選取您要新增的授權**群組。

6 選取 **「查詢類型」**：

- **已快取**：當先前執行查詢時。
- **外部查詢**：當查詢是新的時。

「新增群組授權」畫面隨即顯示。

7 從下拉式選單中選取群組授權，然後按一下 **「選取」**。

其他物件的權限

使用此頁面，將「授權」規則託管者權限賦予 eDirectory 物件。「授權」規則的各成員都會成為物件的託管者。

除了指定對所有屬性的權限之外，您也可按一下「新增內容」，指定對特定內容的權限。

「承襲」核取方塊可決定權限是否會在網路樹中向下承襲。例如，若您指定了對某容器物件的權限，而您希望「授權」規則對該容器下的物件及子容器皆具有相同權限，請選取「承襲」核取方塊。

在您完成此頁面的變更之後，就會將對 eDirectory 中物件的權限授予「授權」規則中的成員。相對地，下次修改某成員對某動態成員資格屬性、移動或重新命名該使用者時，會將已連接系統中的授權授予「授權」規則中所有成員。(當撤銷權利和授權時，相同情況各自適用)。使用「重新評估成員資格」任務以強制更新。

建立對其他物件的權限

如要建立權限：

1 按一下 **「其他物件的權限」**索引標籤

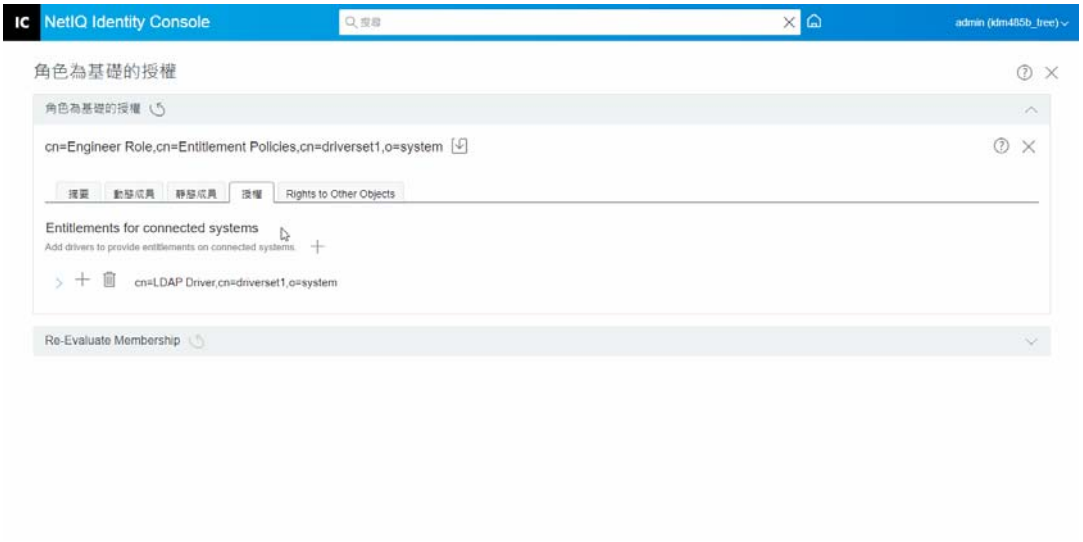
您可在此新增一個新物件，並瀏覽希望此 「授權規則」成為託管者的物件。

1a 若要新增物件，請按一下 ＋ 按鈕。

「內容瀏覽器」頁面隨即顯示。該頁面包含 「物件」。

1b 展開 「物件」，然後根據您的要求選取 「群組」或 「個別使用者」，並為其指派權限。

圖 33-3 *其他物件的權限*

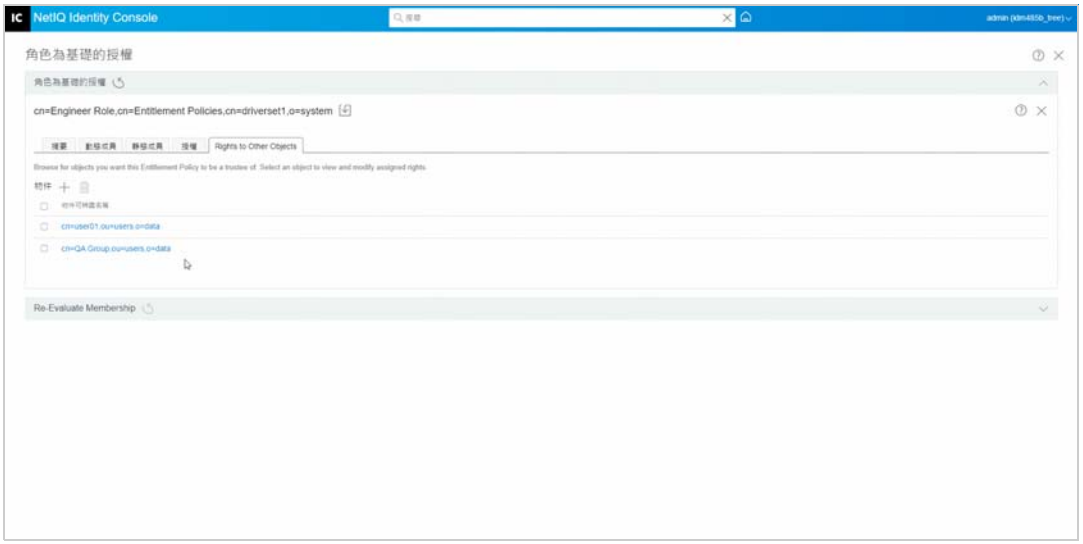


1c 如要新增更多屬性，請按一下 ＋。

「選取屬性」頁面隨即顯示。此頁面包含 「物件」可具有的 「屬性」清單。

1d 按一下 「完成」。

圖 33-4 *選擇屬性*



2 (選用) 透過使用 「向上」和 「向下」箭頭，來設定 RBE 規則的優先順序。

設定規則的優先順序是為了解決多個規則之間的授權衝突。最上層的規則具有最高優先順序。詳細相關資訊請參閱：「設定 RBE 規則的優先順序」 (第 202 頁)

設定 RBE 規則的優先順序

建立 RBE 規則後，影響某個使用者的規則可能會有衝突。

清單中的 RBE 規則順序代表優先順序。您可以使用向上箭頭和向下箭頭來變更清單的順序。

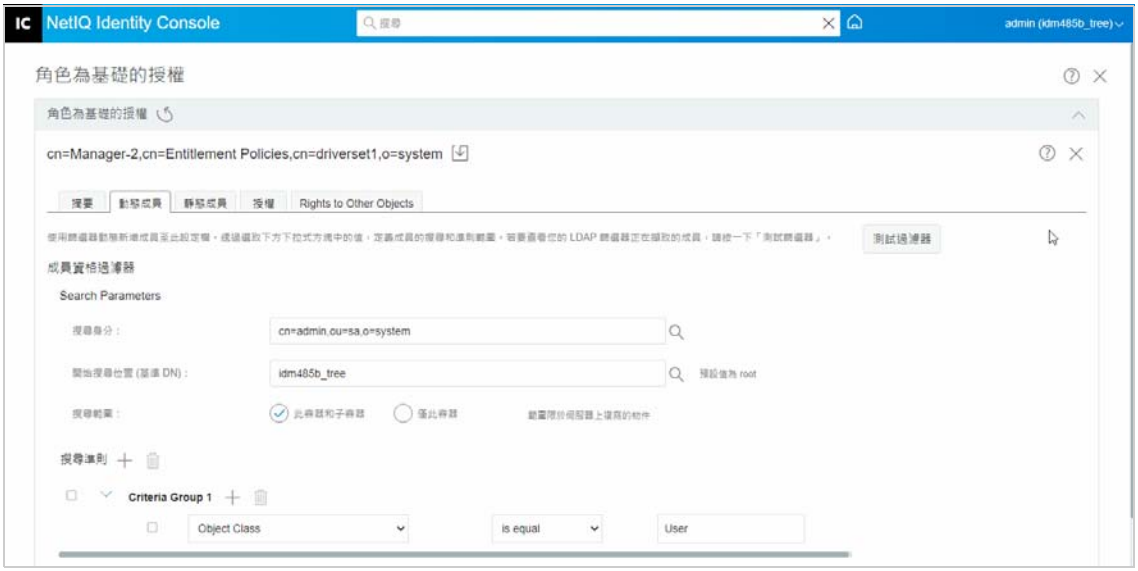
- 舉例來說，當已連接系統上的屬性只允許單一值時，此設定可能就很有用。若兩個不同的 RBE 規則將該屬性的值授予相同使用者，則該使用者會收到清單中位置最高之 RBE 規則所授予的值。另舉一例，您或許將環境組態設定為使用 「授權」，以將使用者放置於另一個系統的階層結構中。您可能想要將使用者置於其中一個位置，而非同時置於兩個位置中。
- 請記住，每個驅動程式提供的每個授權之設定都是獨立的。
- 作為規則，您應在清單中將管理員規則置於一般使用者或個別顧問規則之上。您應該將成員資格較為嚴格的群組，置於成員資格較為寬鬆的群組之上。

如要設定 RBE 規則的優先順序：

1 選取要升級或降級的 「授權規則」。

2 透過使用 「向上」或 「向下」箭頭，來設定 RBE 規則的優先順序。

圖 33-5 設定規則的優先順序

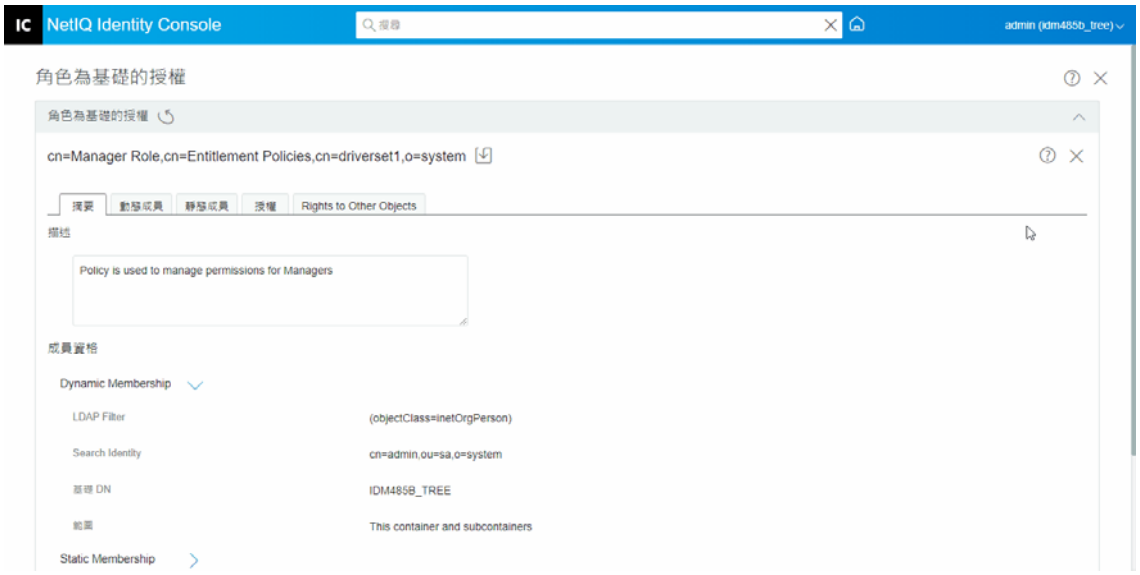


3 按一下儲存 按鈕。

規則成員資格詳細資訊的摘要顯會顯示於 「摘要」索引標籤中。

4 重新啟動驅動程式。

圖 33-6 關閉並重新啟動



附註：您必須重新啟動驅動程式才可使變更生效。

重新評估成員資格

「角色型授權」功能可讓您將已連結系統上的授權授予一組使用者。

當您建立或編輯 RBE 規則時，必須重新評估每個使用者的成員資格，以決定是否需要授予、變更或撤銷已連結系統上的授權。依照預設，重新評估只會一次對一位使用者進行，在下次有影響所有使用者成員資格的屬性遭到變更時，以及有使用者被移除或重新命名時，也會執行重新評估。此預設行為可將系統資源的使用降至最低，但這也表示 RBE 規則變更與對特定使用者授予、變更或撤銷授權之間，會有明顯的時間延遲。

您可使用 「重新評估 RBE 規則」（第 204 頁）任務，指定要立即重新評估的使用者，確認已一次更新所有使用者授權。建議您在每次建立或編輯 RBE 規則時，都要進行一次此動作。

在 Identity Manager 3.6 之前，成員資格的重新評估是在驅動程式集內針對所有 RBE 規則執行的，而不是針對個別的「授權」規則執行。但是，Identity Manager 3.6 可讓您 **「評估」**某個 RBE 規則並將其成員 **「新增」**至選取的 **「物件清單」**。若您已定義「授權」規則並且建立了會員清單，則可於選取的「物件」項目旁看到「評估授權規則並將其成員 **「新增」**至清單」標題。選取規則，然後按一下 ＋ 圖示，將規則的成員新增至選取的 **「物件清單」**。您可於選取的 **「物件清單」**中新增或移除成員或物件。

若要最有效的使用系統資源，您應於特定驅動程式集中進行所有 RBE 規則變更後，再使用「重新評估 RBE 規則」（第 204 頁）。

附註：只有已連接系統上的授權，才需要重新評估授權。當 RBE 規則的「身分主控台」權限有所變更時，變更會立即影響每一個使用者。您必須先執行「授權服務」驅動程式才能重新評估成員資格。

重新評估 RBE 規則

如要重新評估成員資格：

1 按一下「重新評估成員資格」>「選取驅動程式集」。

將會顯示已建立的規則清單。

2 選取需要評估的規則，然後按一下「評估」Evaluate。

在「物件」索引標籤上，將會顯示屬於該群組的使用者。

3 (選用) 如要新增特定使用者，請按一下 +。

當清單中缺少使用者，且您想要新增特定使用者時，僅如此才能使用此「新增」+ 功能。

4 (選用) 若要移除特定使用者，請按一下 🗑。

當需從清單中移除特定使用者時，僅如此才能使用「刪除」🗑功能。

5 按一下「重新評估成員資格」按鈕 ▷。

圖 33-7 重新評估成員資格