為Microsoft Entra ID SSO配置SNA管理器

目錄

[簡介](#)

[必要條件](#)

- [需求](#)
- [採用元件](#)

[設定步驟](#)

- [在Azure中配置企業應用程式](#)
- [在SNA中配置和下載服務提供商XML檔案](#)
- [在Azure中配置SSO](#)
- [在Entra ID中設定使用者。](#)
- [在SNA中配置SSO](#)

[疑難排解](#)

簡介

本檔案介紹如何將安全網路分析(SNA)設定為使用Microsoft Entra ID進行單一登入(SSO)。

必要條件

需求

思科建議您瞭解以下主題：

- Microsoft Azure
- 安全網路分析

採用元件

- SNA管理員v7.5.2
- Microsoft Entra ID

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定步驟

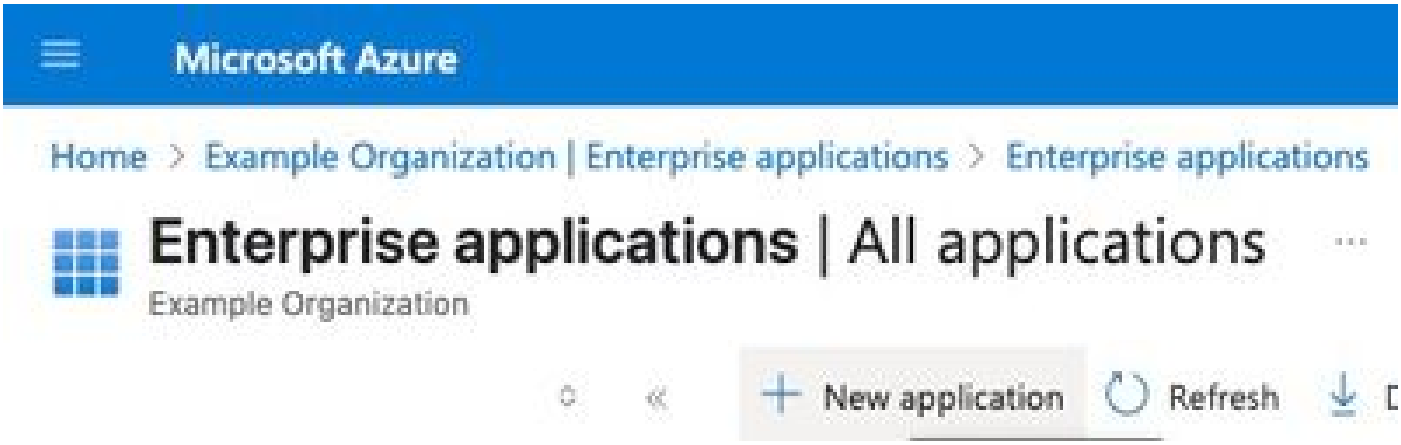
在Azure中配置企業應用程式

1.登入到Azure雲門戶。

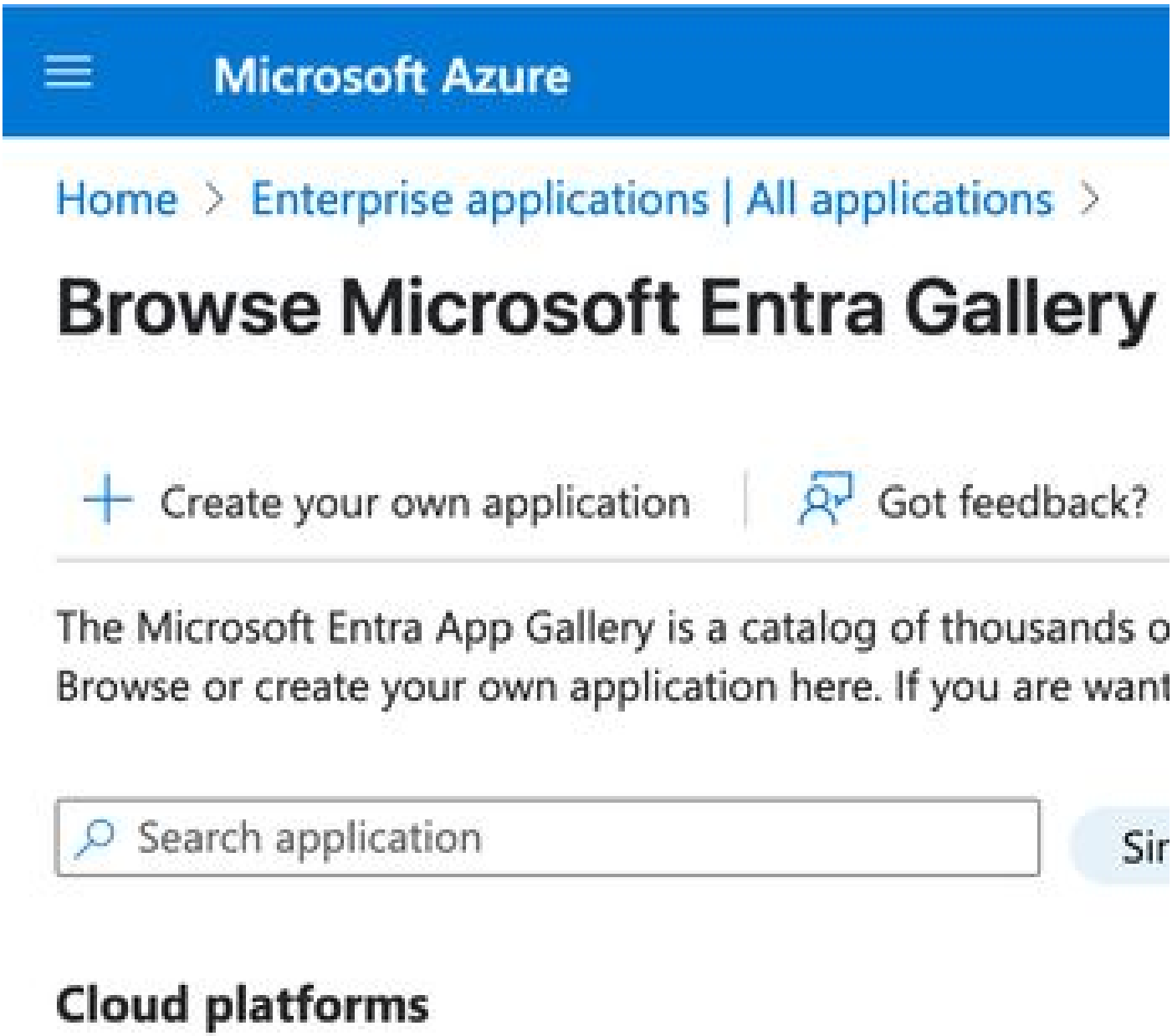
2.在搜索框中搜尋Entra ID服務，然後選擇Microsoft Entra ID。

3.在左窗格中，展開管理，然後選擇企業應用程式。

4.按一下New Application。



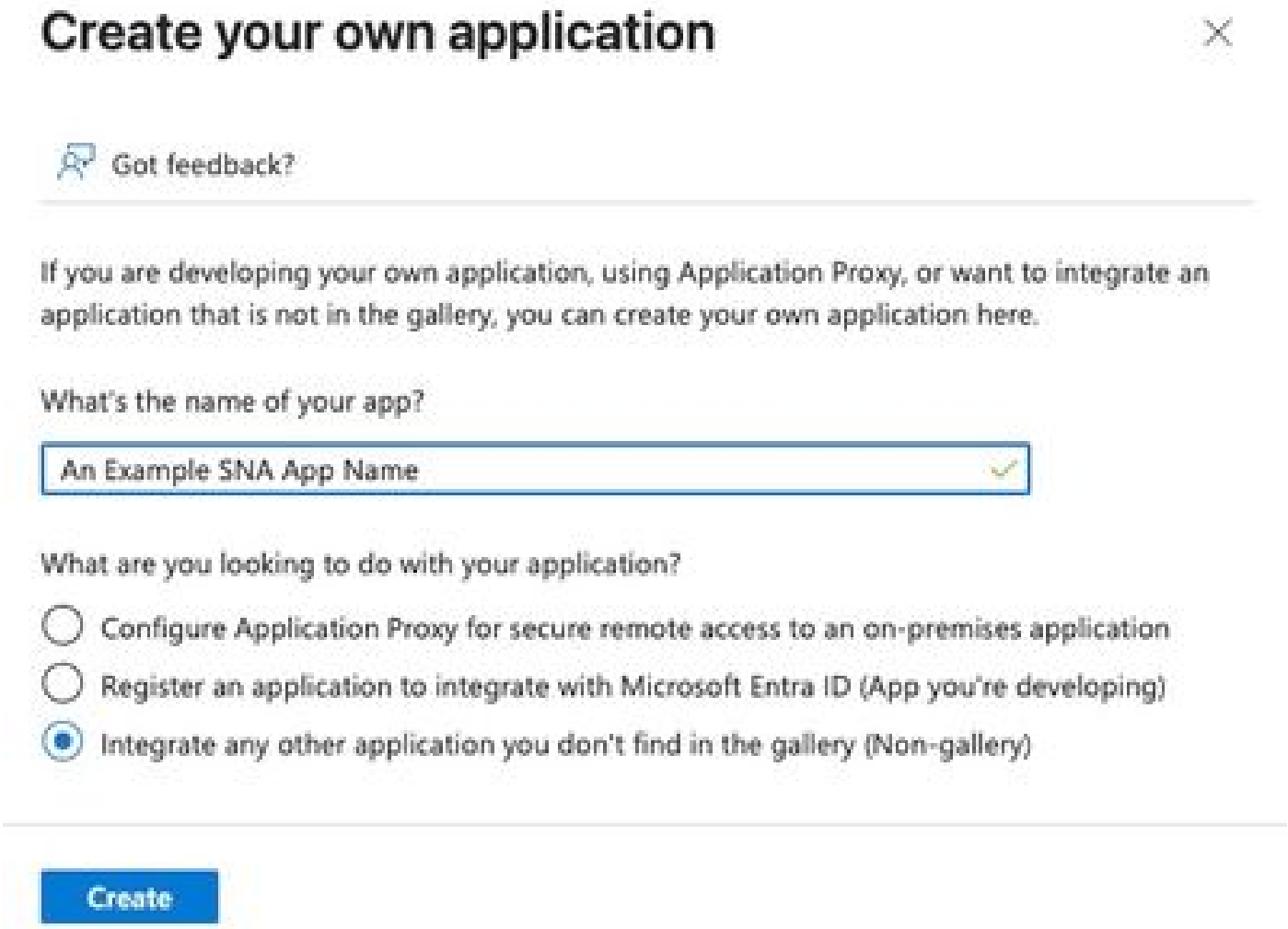
5.在載入的新頁面上，選擇「建立自己的應用程式」。



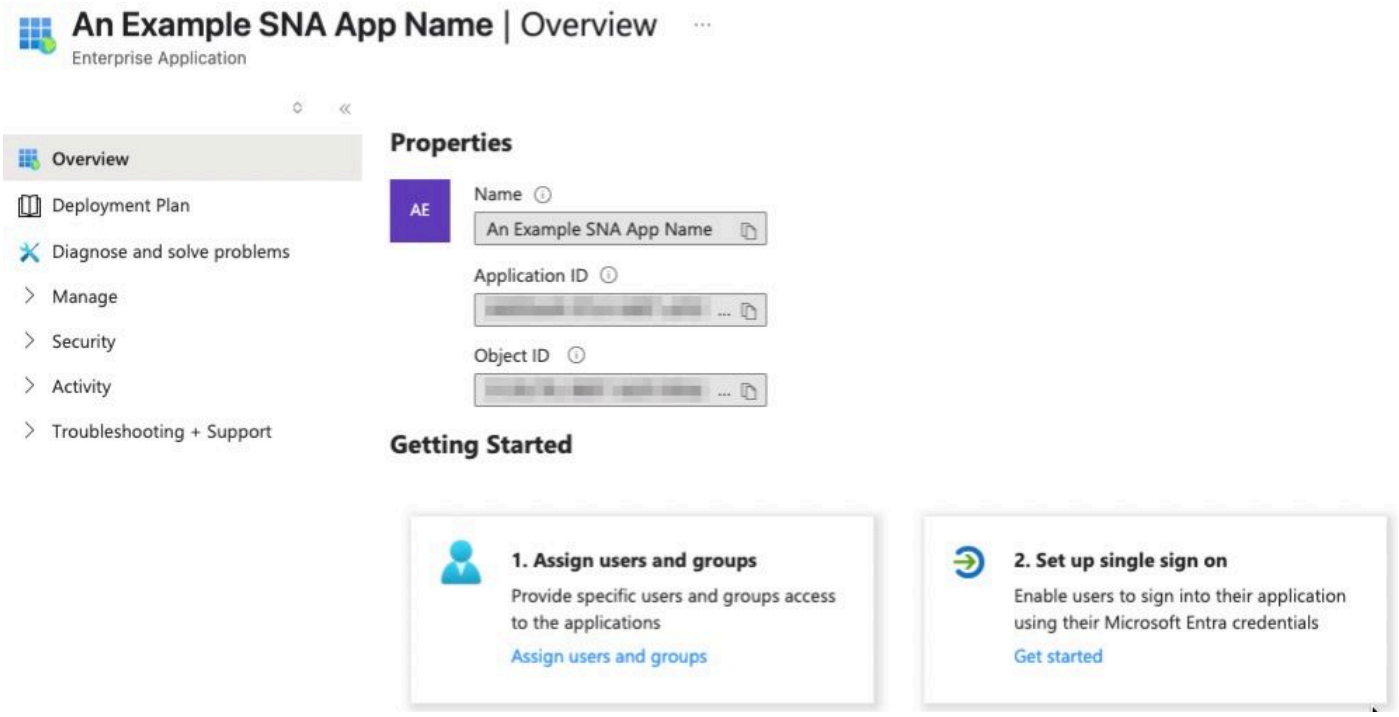
Azure-UI

6.在應用名稱是什麼？欄位.

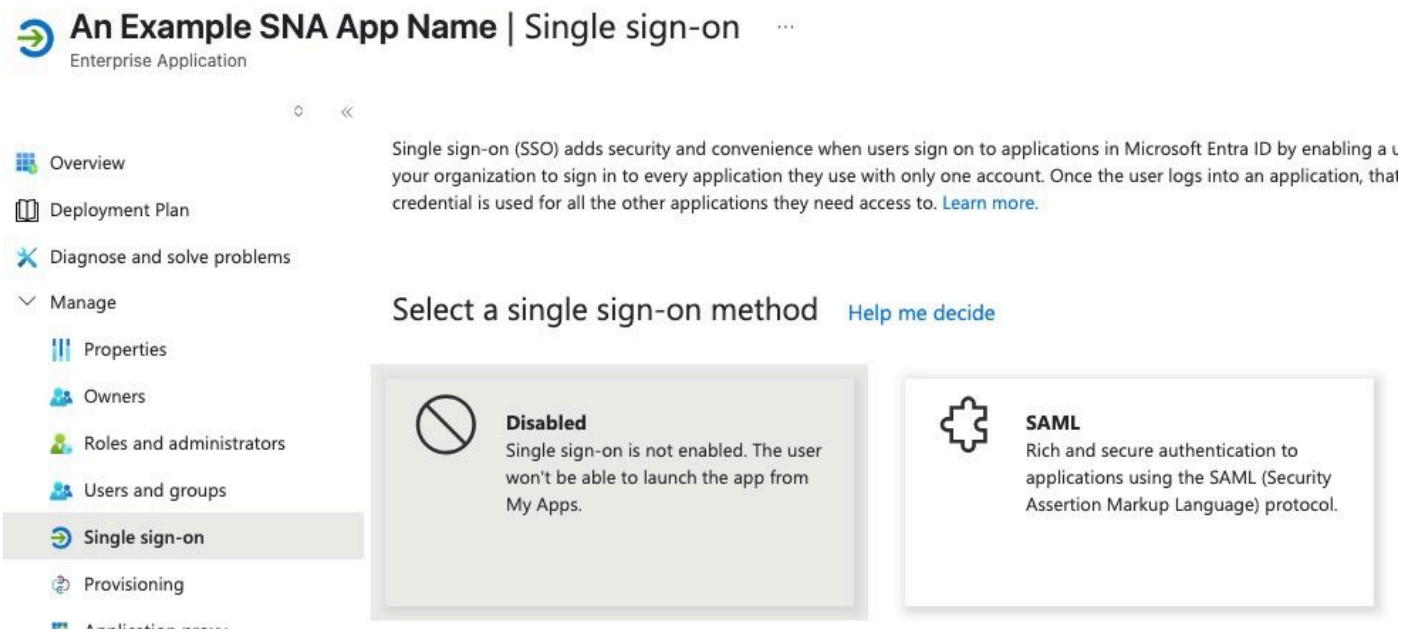
7.選擇單選按鈕「整合在相簿（非相簿）中找不到的所有其他應用程式」，然後按一下「建立」。



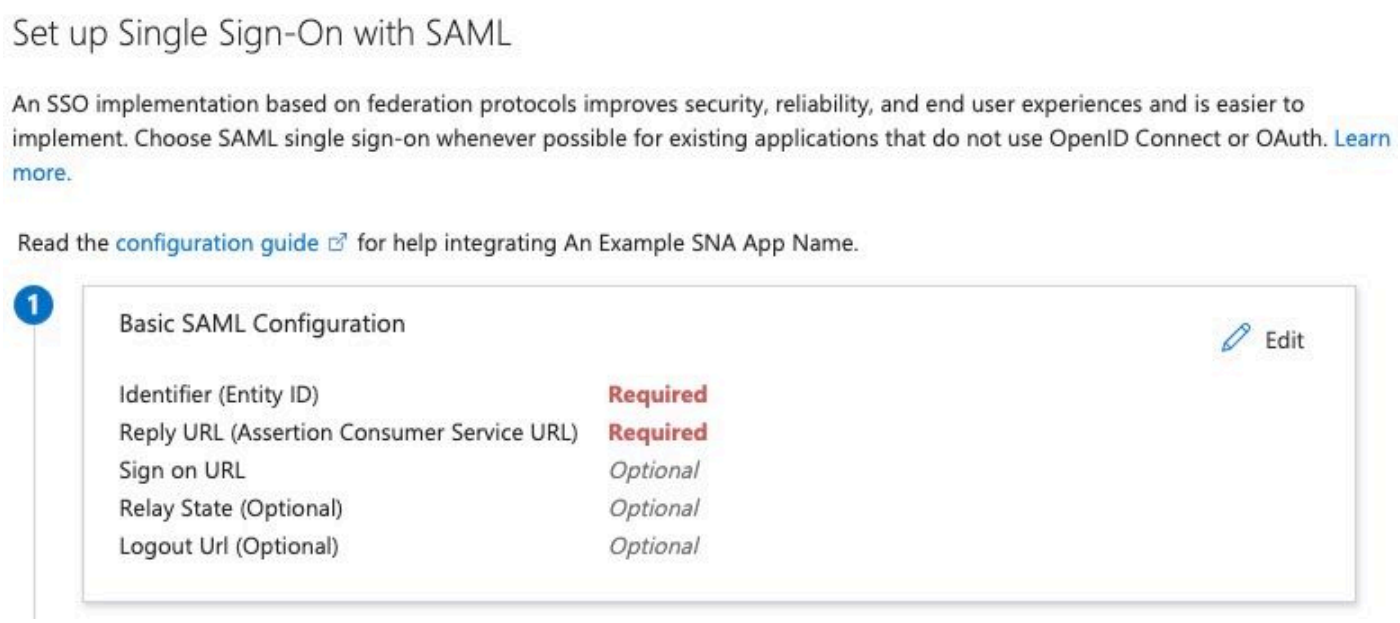
8.在新配置的應用程式控制面板上，按一下「設定單一登入」。



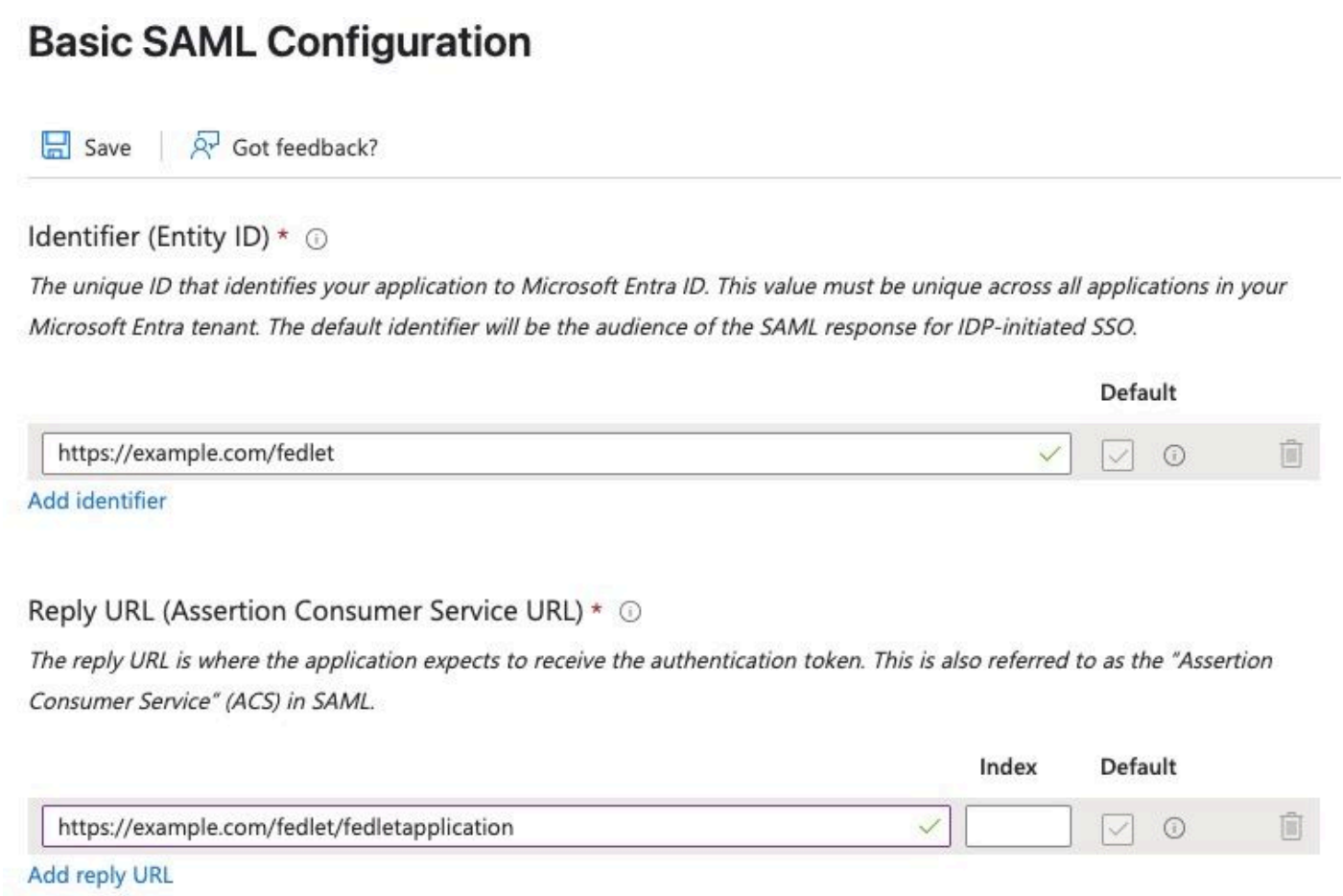
9.選擇SAML。



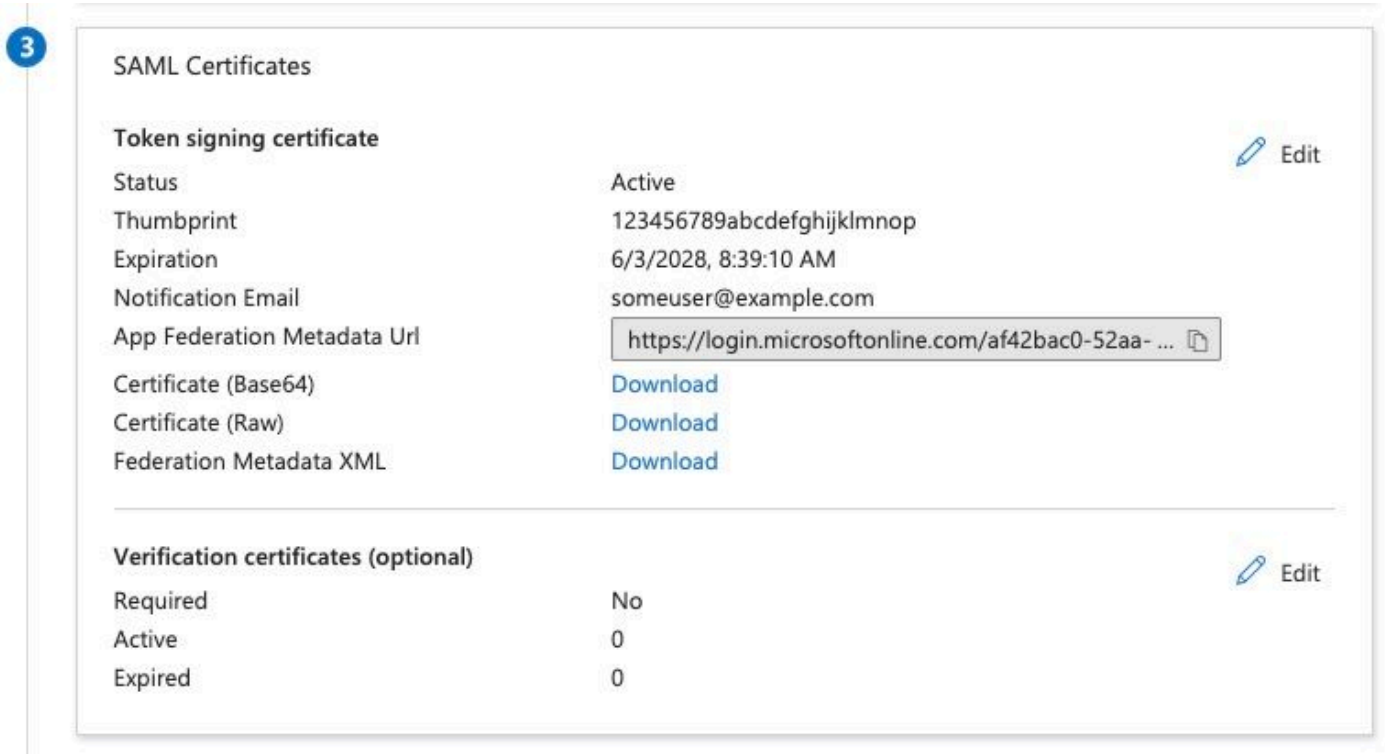
10.在「使用SAML設定單一登入」頁上，按一下「基本SAML配置」下的編輯。



11.在Basic SAML Configuration窗格下，將Add Reply URL配置到 https://example.com/fedlet/fedletapplication，用SNA Manager的FQDN替換example.com，然後按一下save。

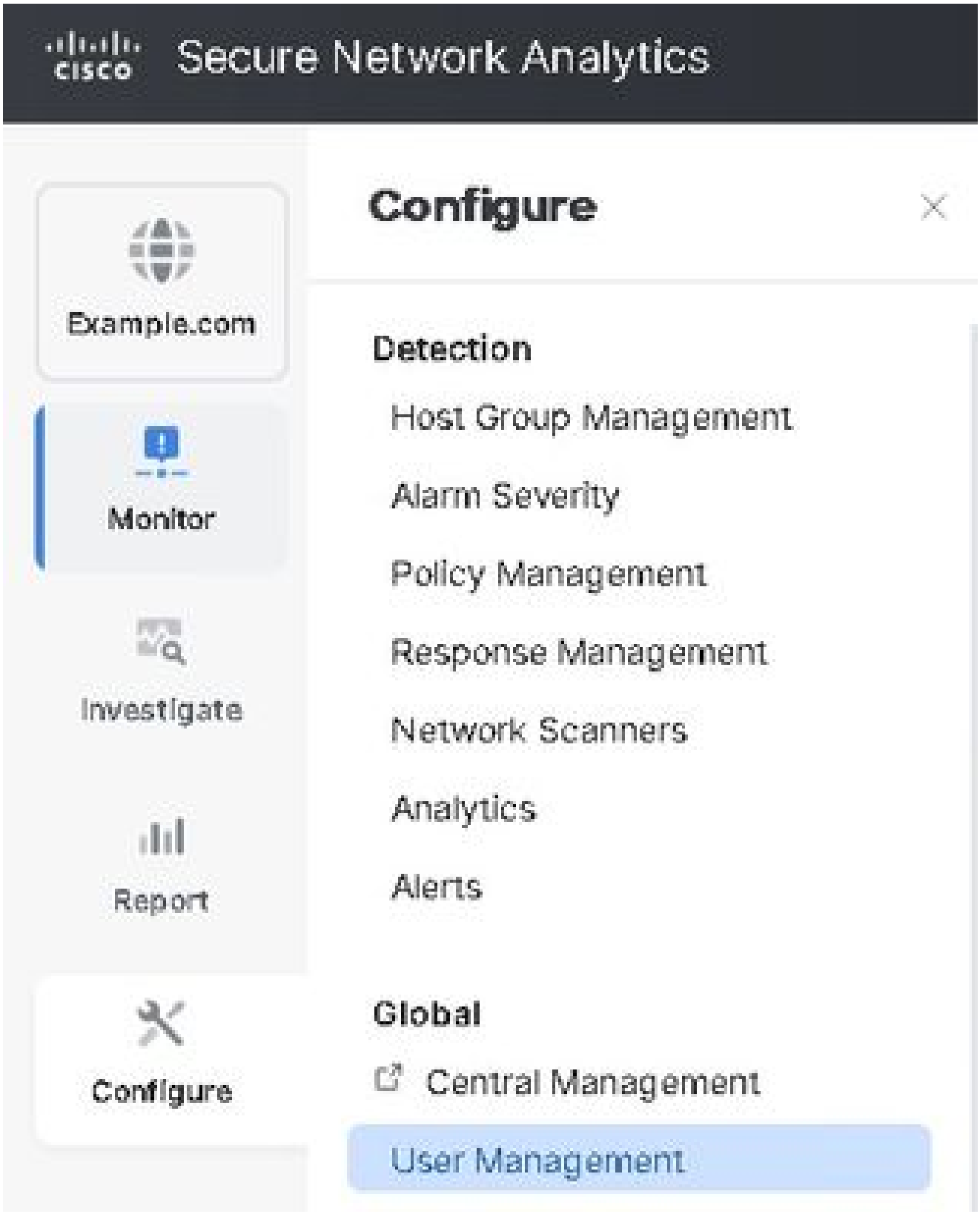


12.找到SAML Certificates卡並儲存App Federation Metadata URL欄位值，然後下載Federation Metadata XML。

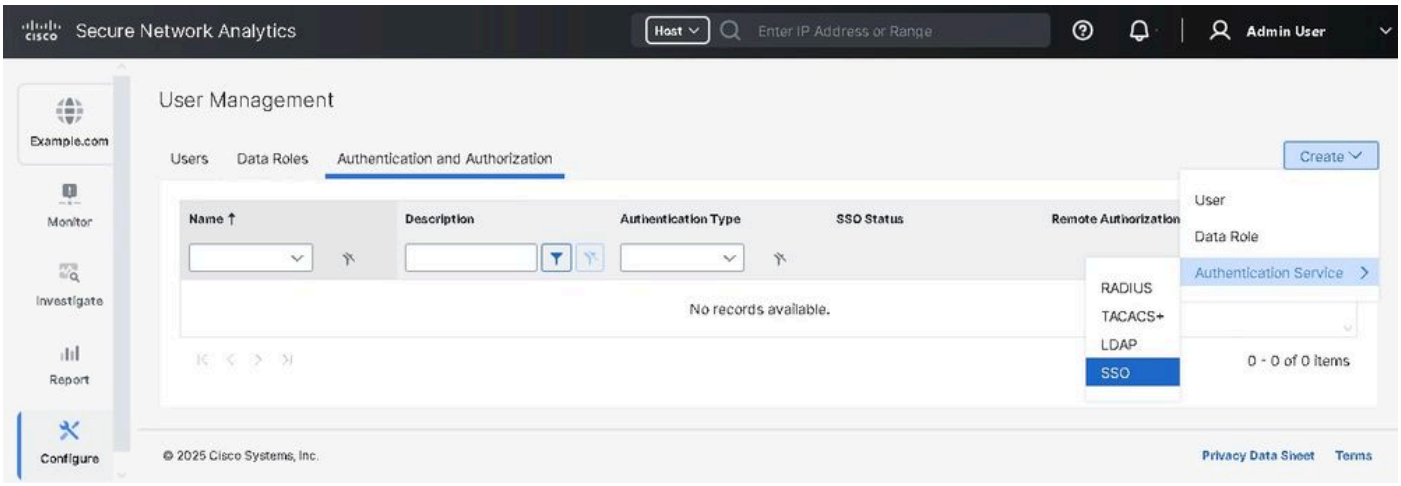


在SNA中配置和下載服務提供商XML檔案

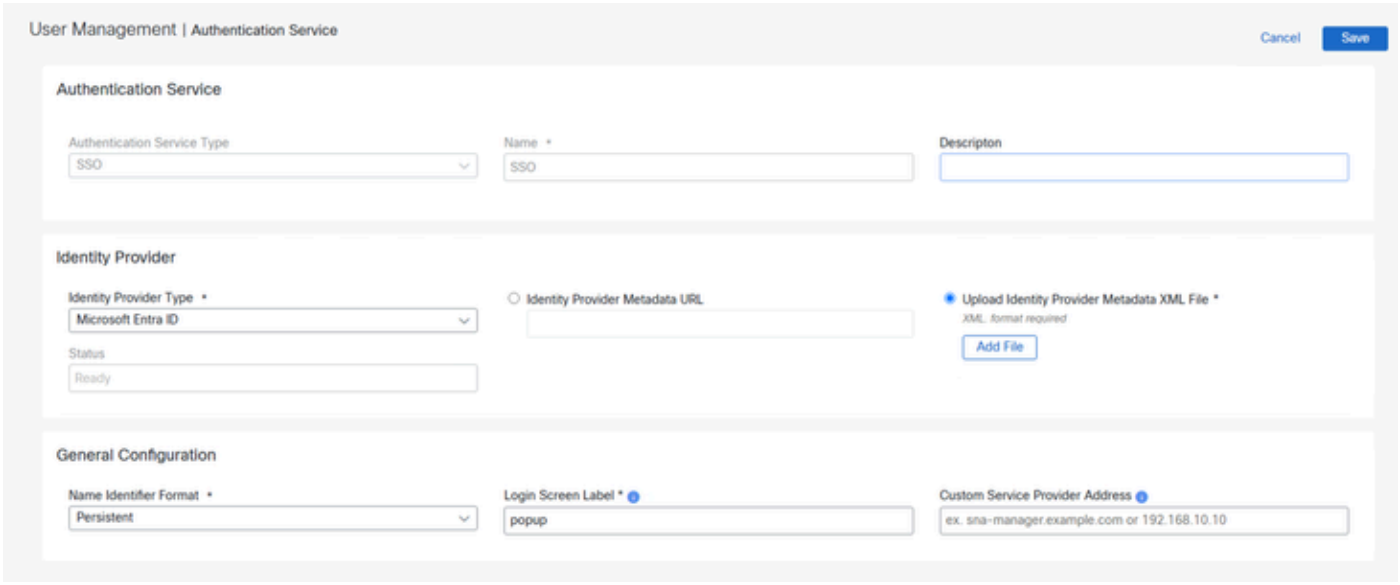
1. 登入到SNA管理器UI。
2. 導航到Configure > Global > User Management。

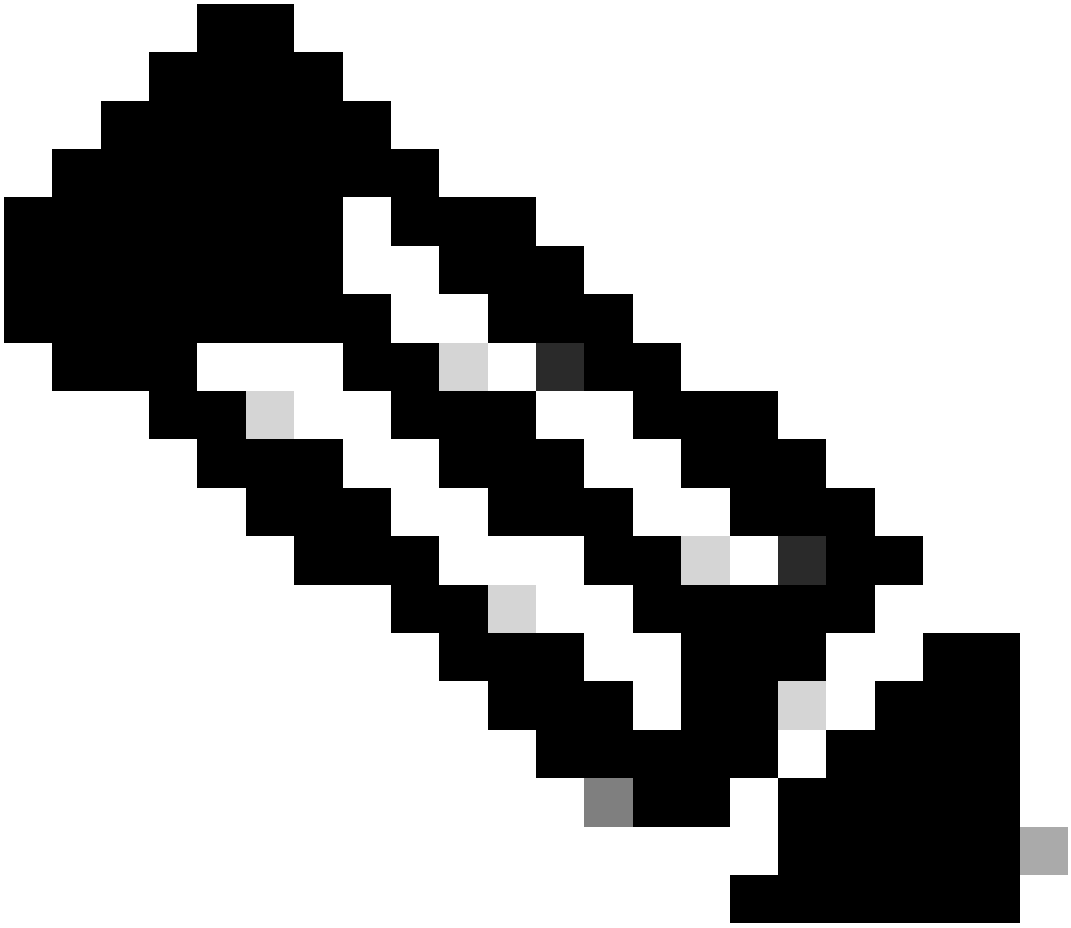


3. 在Authentication and Authorization頁籤下，按一下Create > Authentication Service > SSO。



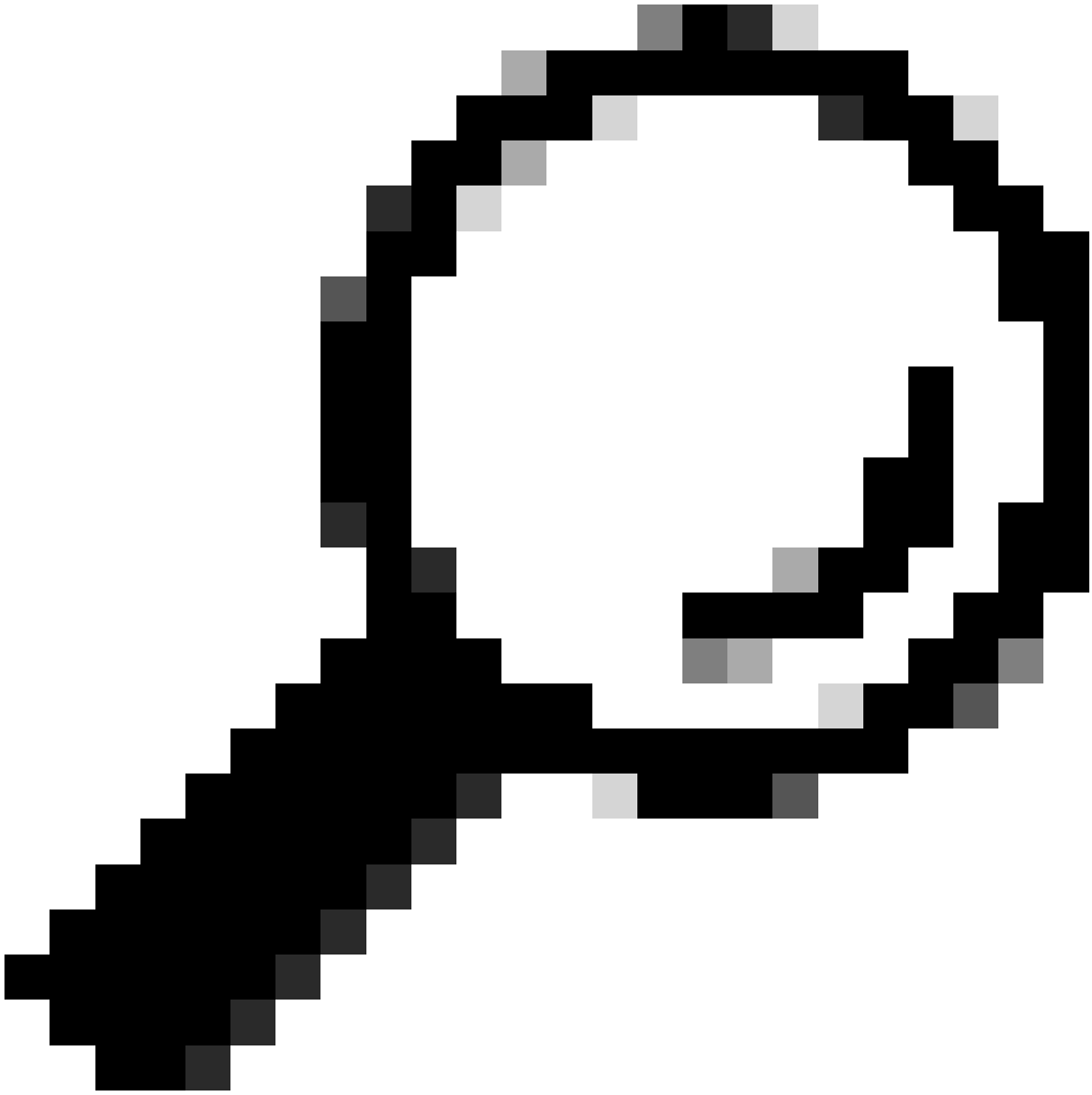
4.為身份提供程式後設資料URL或上傳身份提供程式後設資料XML檔案選擇適當的單選按鈕。





附註：在此演示中，已選擇上傳身份提供程式後設資料XML檔案。

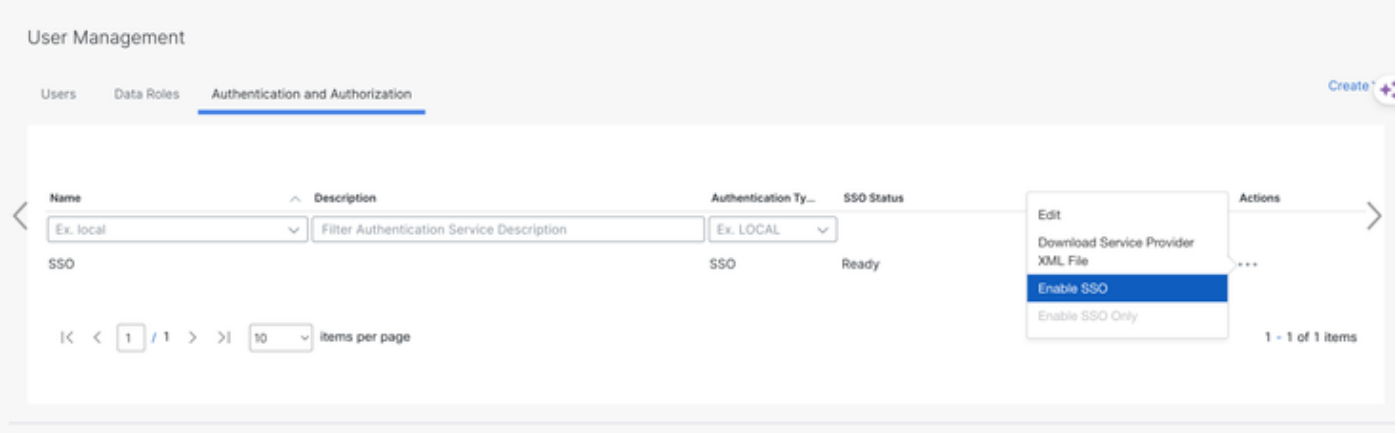
5.將「身份提供程式型別」字段配置為Microsoft Entra ID，將名稱識別符號格式配置為Persistent，鍵入Login Screen Label。



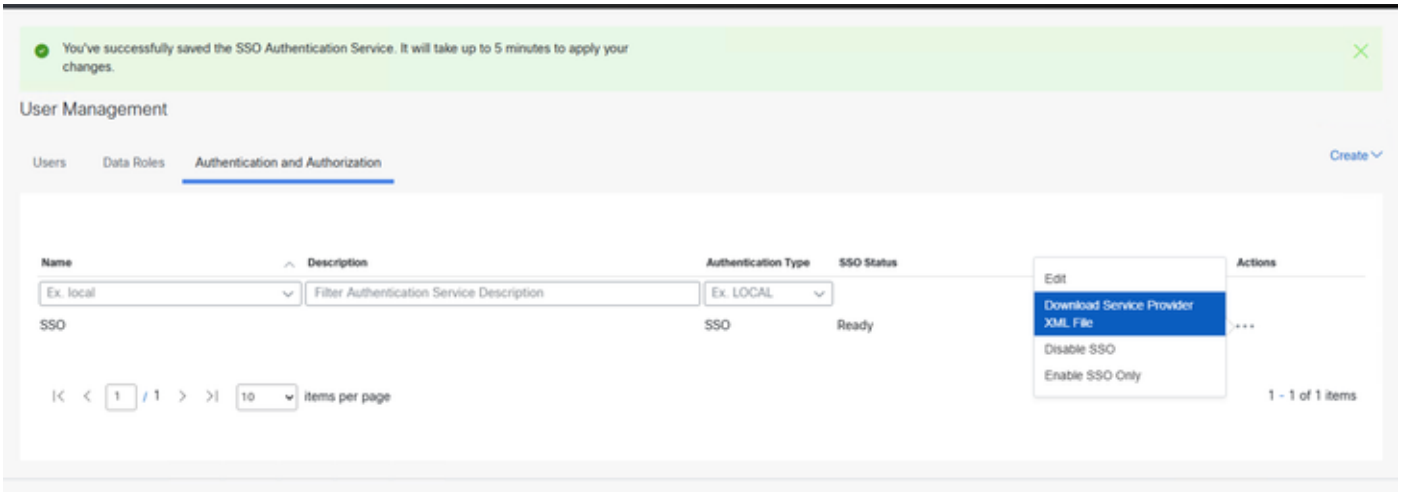
提示：已配置的登入螢幕標籤（名稱/文本）顯示在Login In with SSO按鈕上方，不應留空。

6.按一下Save，返回至Authentication and Authorization頁籤。

7.等待狀態變為READY，然後從操作選單中選擇Enable SSO。



8.在「Authentication and Authorization」頁籤下，按一下「Actions」列中的三個點，然後按一下「Download Service Provider XML File」。



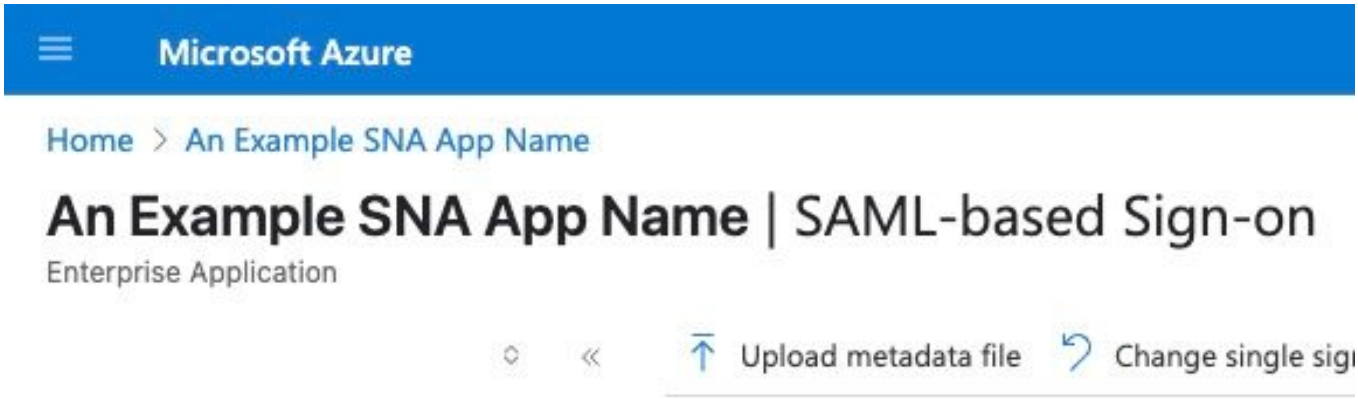
在Azure中配置SSO

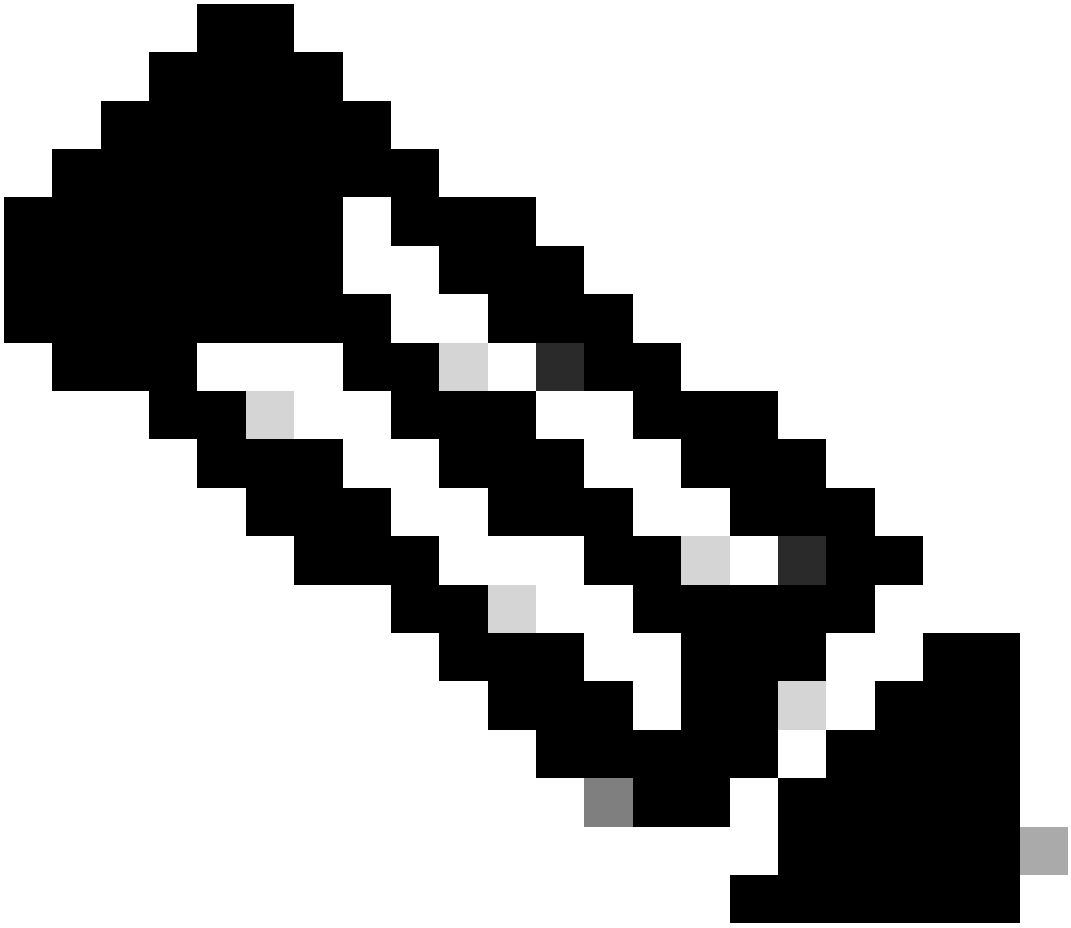
1.登入到Azure門戶。

2.從搜尋欄導航至「企業應用程式」>「選擇已配置企業應用程式」>「按一下設定單一登入」。

3.單擊頁面頂部的Upload metadata file並上傳從SNA Manager下載的sp.xml檔案。

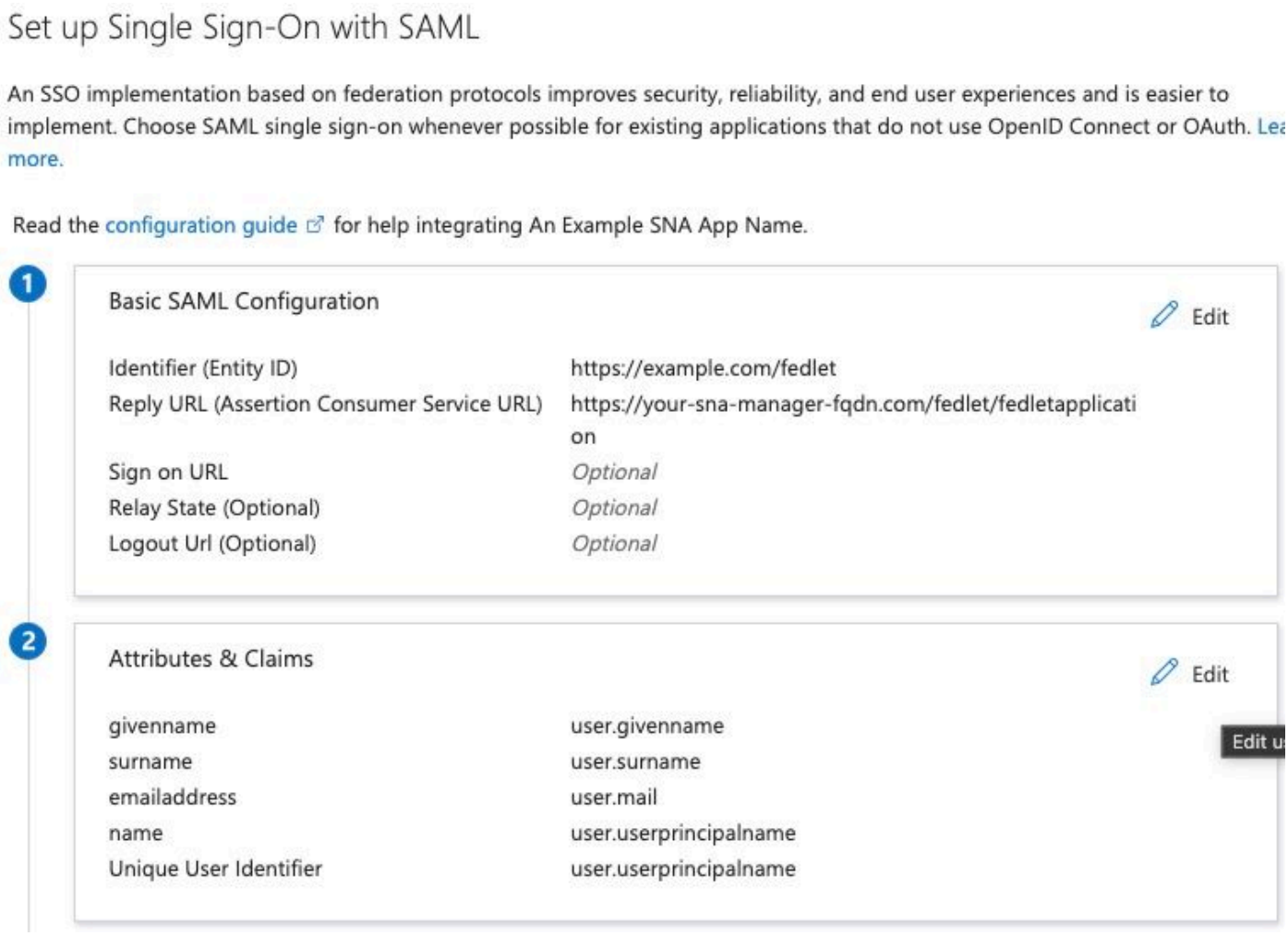
4.開啟「基本SAML配置」螢幕並將各種設定設定為正確的值，按一下「保存」。





附註：確保Entra ID中的「名稱ID 」格式正確。

5.找到Attributes & Claims部分，然後按一下Edit。



6.按一下宣告名稱部分下的user.userprincipalname值。

7.在「管理索賠」頁下「驗證」選擇名稱識別符號格式。

Microsoft Azure

Search

Home > An Example SNA App Name | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims >

Manage claim ...

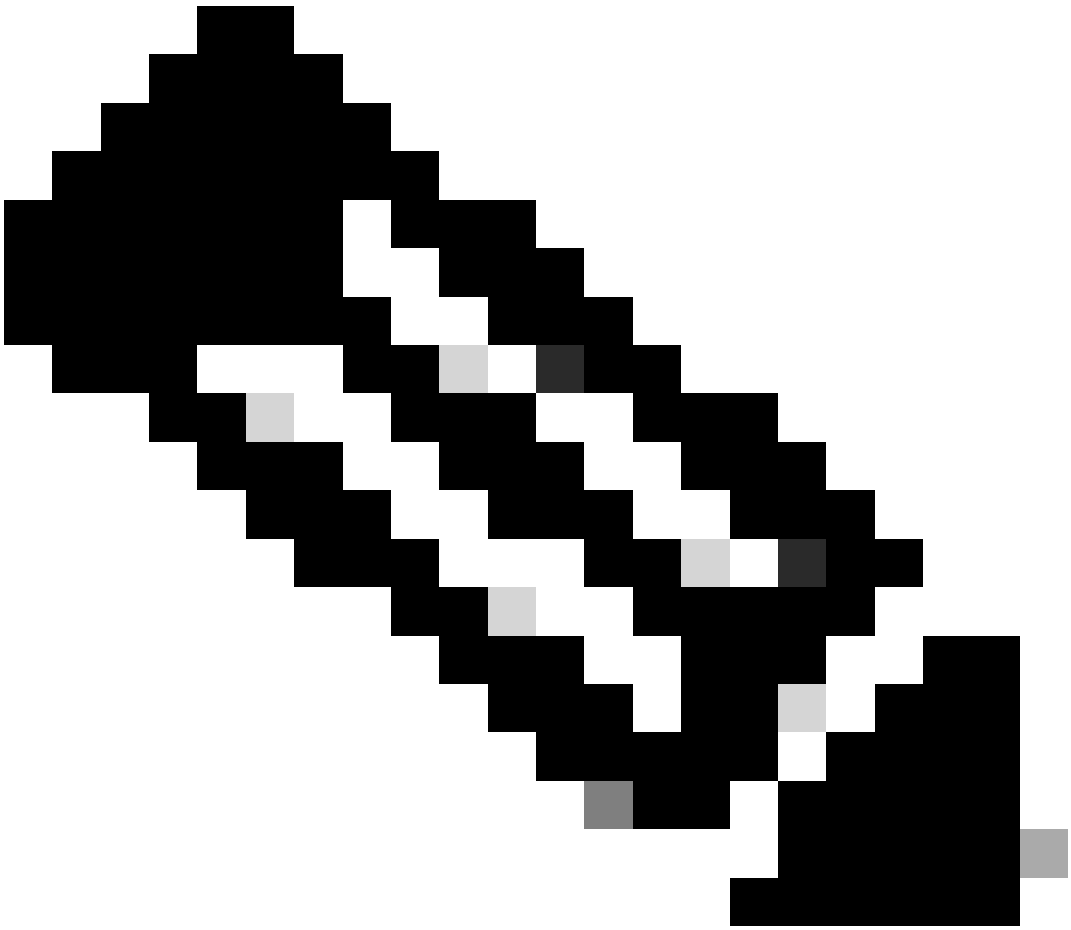
Save | Discard changes | Got feedback?

Name: nameidentifier

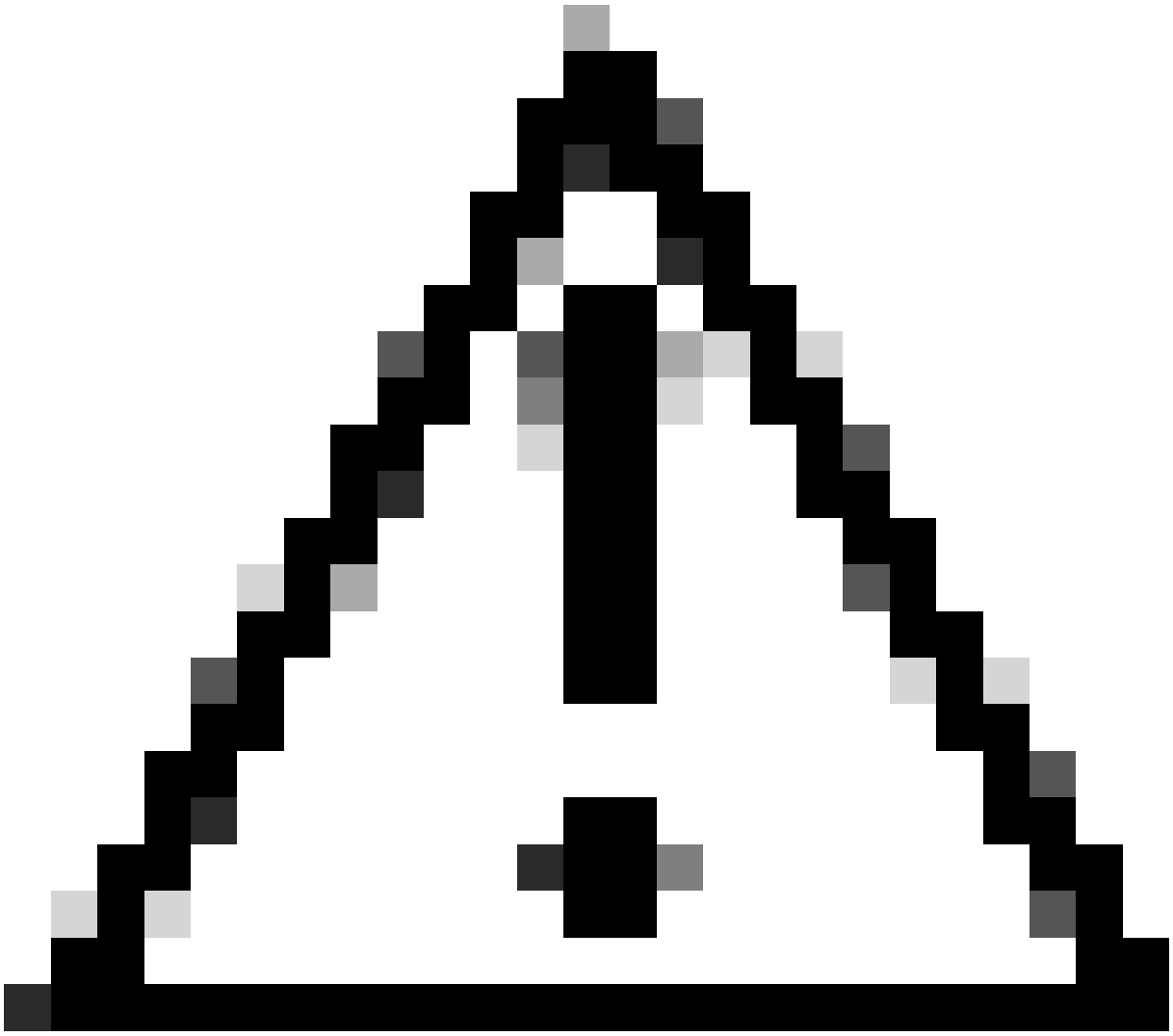
Namespace: http://schemas.xmlsoap.org/ws/2005/05/identity/claims

Choose name identifier format

Name identifier format *: Persistent



附註：名稱識別符號格式欄位設定為Persistent if not， then select it from the drop-down menu。如果進行了更改，請按一下「儲存」。

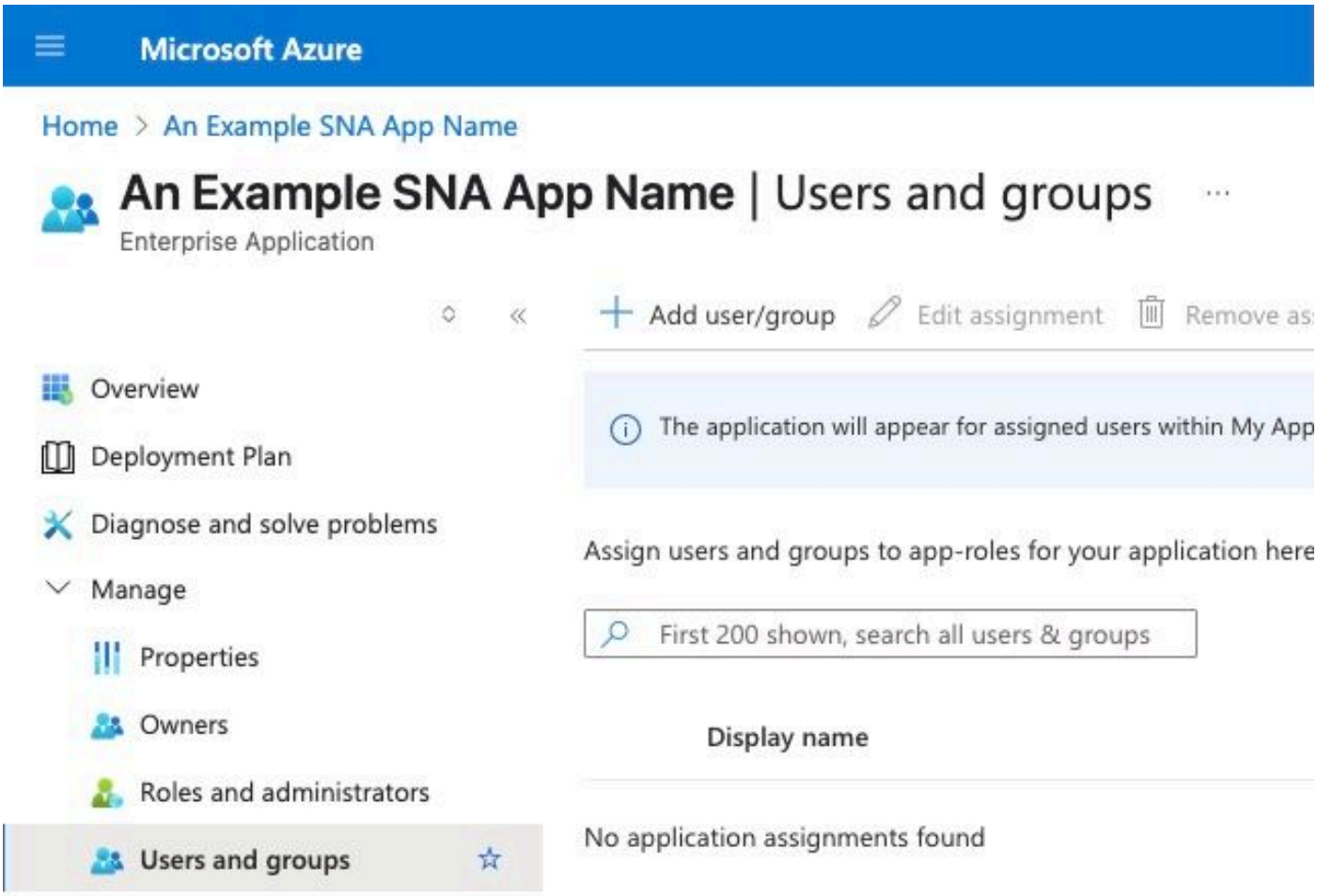


注意：這是最常見的遇到問題的地方。SNA Manager和Microsoft Azure上的設定必須匹配。如果您選擇在SNA中使用「emailAddress」格式，則此處的格式也必須是「Email Address」。

在Entra ID中設定使用者。

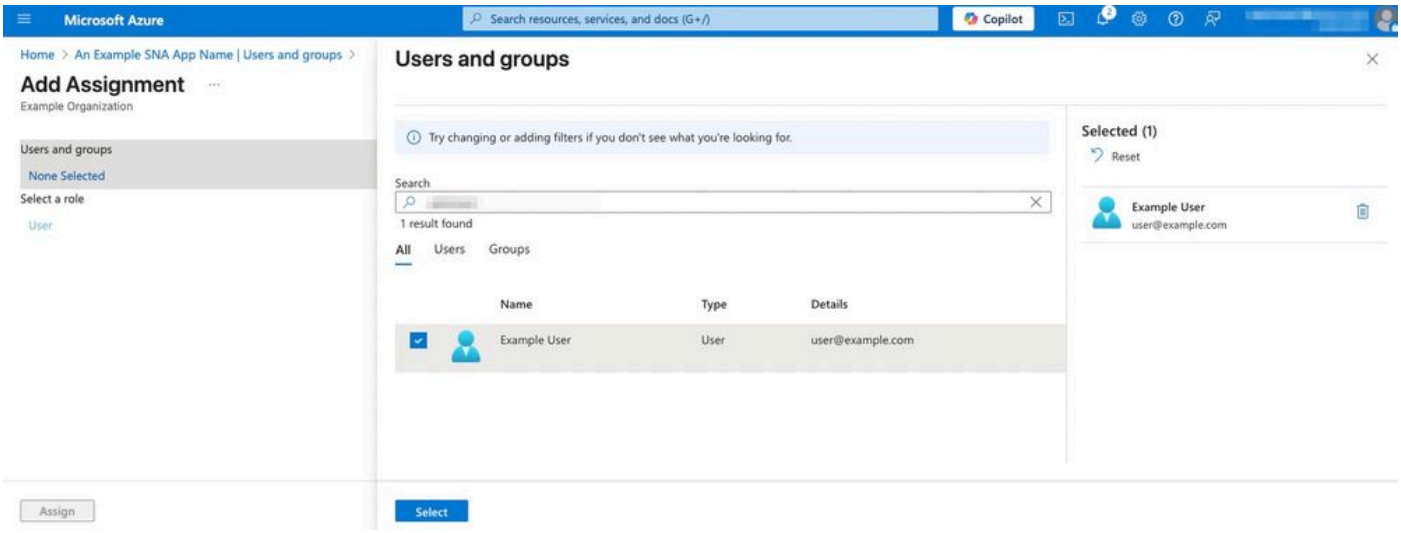
1.登入到Azure門戶。

2.從搜尋欄導航到「企業應用程式」>「選擇已配置企業應用程式」>選擇左側的「使用者和組」>按一下「新增使用者/組」。



3.在左窗格中，按一下None Selected。

4.搜尋所需的使用者並將其新增到應用程式中。

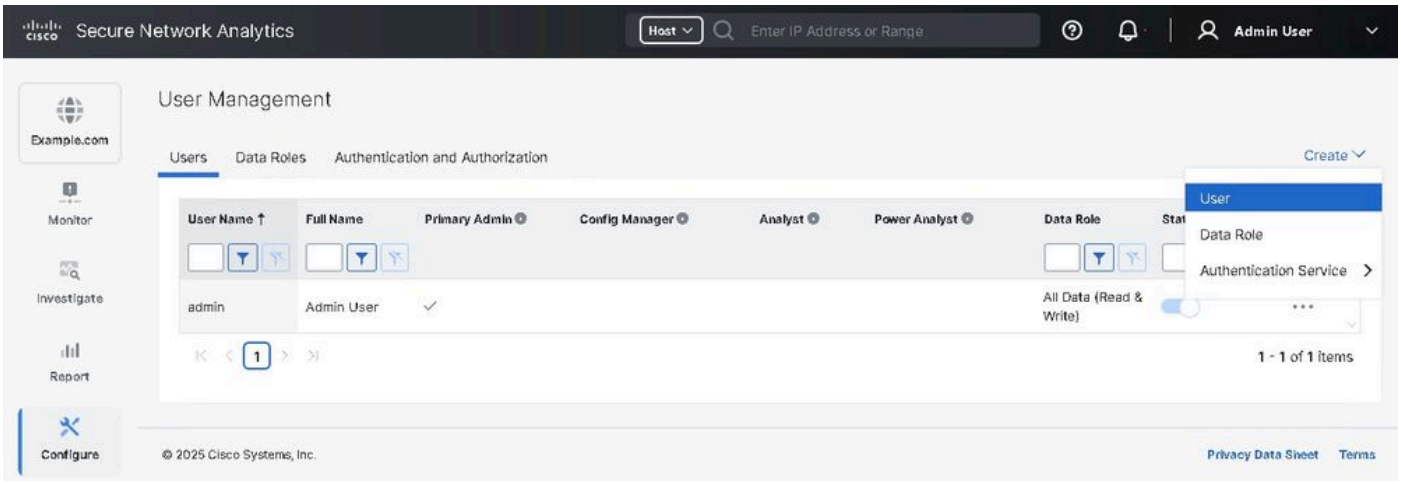


在SNA中配置SSO

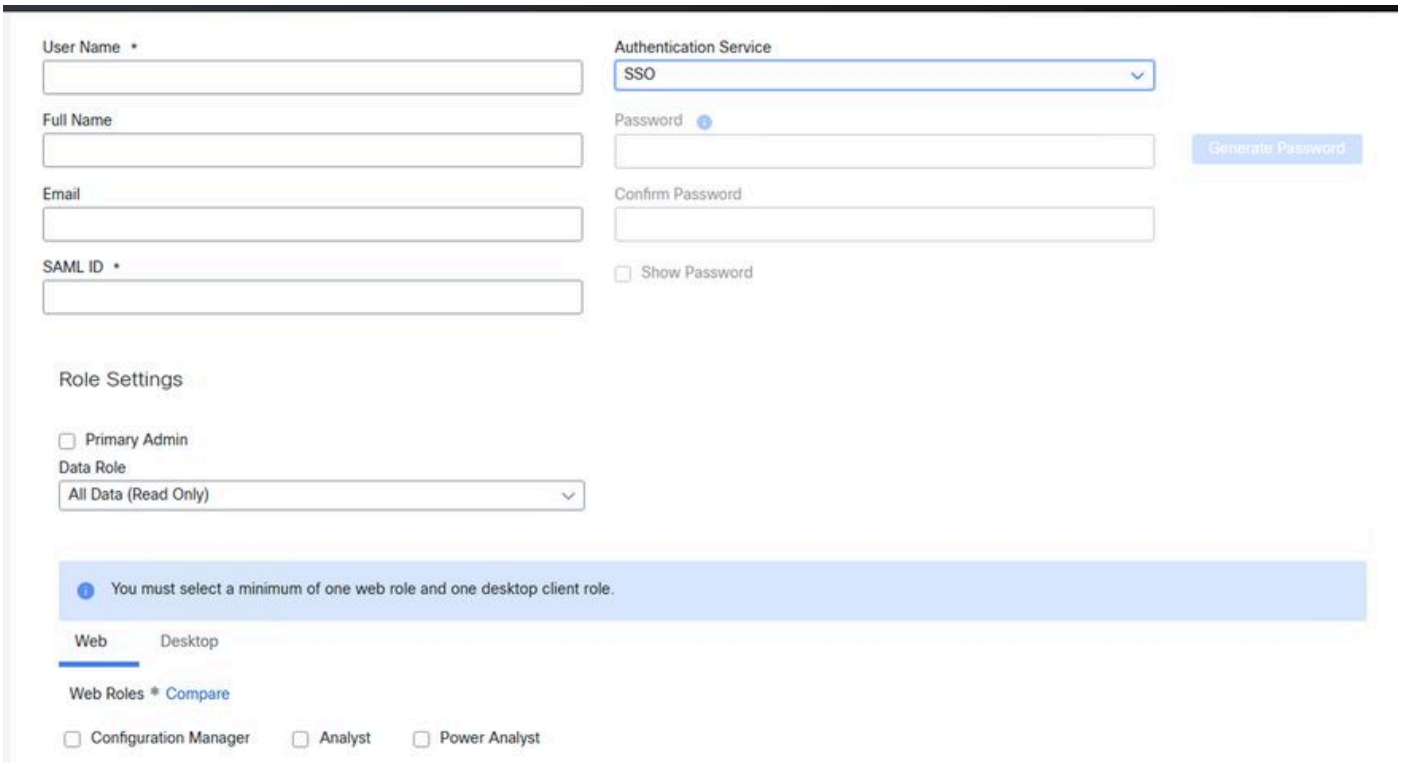
1.登入到SNA管理器UI。

2.定位至「配置」>「全域性」>「使用者管理」。

3.按一下建立>使用者。



4.通過提供與選定為SSO的身份驗證服務相關聯的詳細信息來配置使用者，然後按一下Save。



在SNA-UI中建立SAML — 使用者

疑難排解

如果使用者無法登入到SNA Manager，則可以使用SAML Tracer進行進一步調查。

如果調查SNA Manager需要進一步協助，則可以提出TAC案例。

https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。