

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

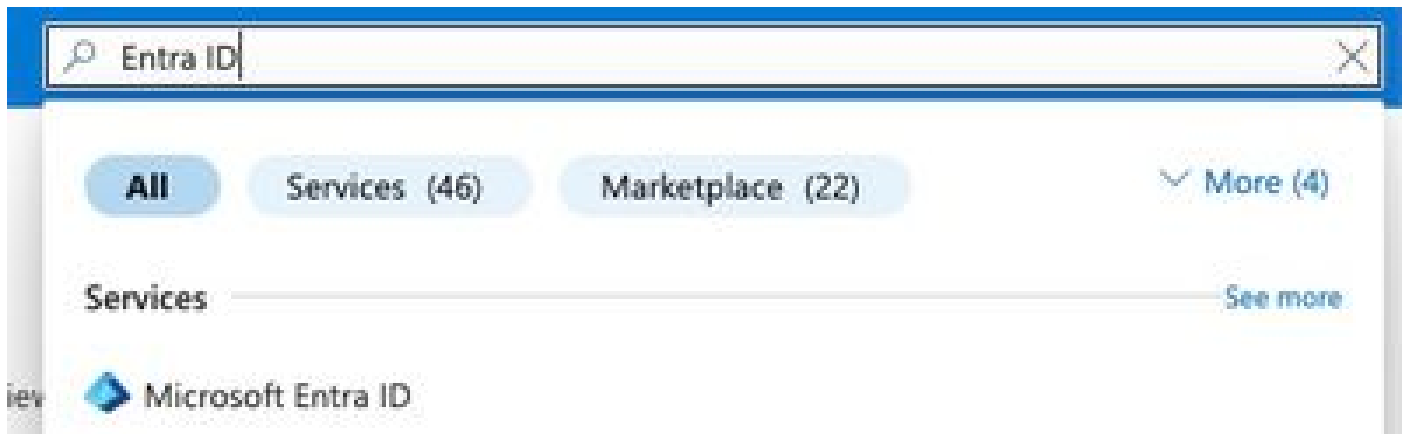
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定步驟

在Azure中配置企業應用程式

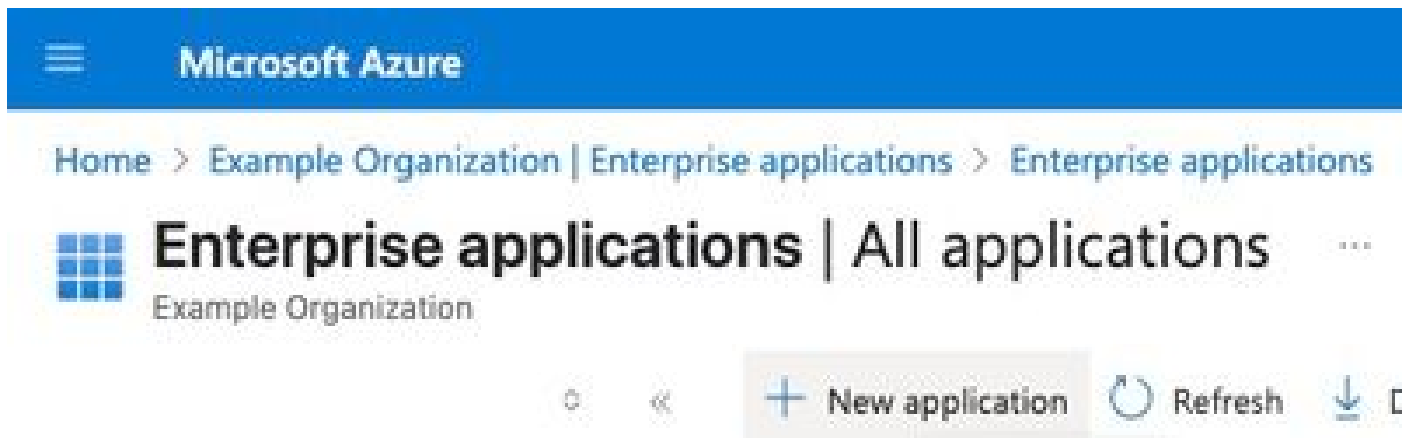
1. 登入到Azure [雲門戶](#)。

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」。



[Home](#) > [Enterprise applications](#) | [All applications](#) >

Browse Microsoft Entra Gallery



Create your own application



Got feedback?

The Microsoft Entra App Gallery is a catalog of thousands of applications. Browse or create your own application here. If you are want



Sir

Cloud platforms

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」。

Create your own application



Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

An Example SNA App Name



What are you looking to do with your application?

- ☐ Configure Application Proxy for secure remote access to an on-premises application
- ☐ Register an application to integrate with Microsoft Entra ID (App you're developing)
- ☒ Integrate any other application you don't find in the gallery (Non-gallery)

Create

8. 在新配置的應用程式控制面板上，按一下「設定單一登入」。



An Example SNA App Name | Overview

Enterprise Application

Overview

- Deployment Plan
- Diagnose and solve problems
- > Manage
- > Security
- > Activity
- > Troubleshooting + Support

Properties

AE

Name

An Example SNA App Name

Application ID

[Redacted]

Object ID

[Redacted]

Getting Started



1. Assign users and groups

Provide specific users and groups access to the applications

[Assign users and groups](#)



2. Set up single sign on

Enable users to sign into their application using their Microsoft Entra credentials

[Get started](#)

9.選擇SAML。

The screenshot shows the 'Single sign-on' configuration page in the Microsoft Entra ID portal. The left sidebar contains a navigation menu with options: Overview, Deployment Plan, Diagnose and solve problems, Manage (expanded), Properties, Owners, Roles and administrators, Users and groups, Single sign-on (selected), and Provisioning. The main content area has a header 'An Example SNA App Name | Single sign-on' and a sub-header 'Enterprise Application'. Below this, there's a description of Single sign-on (SSO) and a 'Select a single sign-on method' section. This section has two cards: 'Disabled' (with a red circle and slash icon) and 'SAML' (with a puzzle piece icon). The 'SAML' card is highlighted, indicating it's the selected method. The 'Disabled' card states: 'Single sign-on is not enabled. The user won't be able to launch the app from My Apps.' The 'SAML' card states: 'Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.'

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。

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating An Example SNA App Name.

The screenshot shows the 'Basic SAML Configuration' section in the Microsoft Entra ID portal. It has a numbered list item '1' on the left. The main content area is titled 'Basic SAML Configuration' and has an 'Edit' button in the top right corner. Below the title, there's a table with two columns: the configuration name and its requirement status.

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

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。

Basic SAML Configuration

 Save |  Got feedback?

Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default



[Add identifier](#)

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index

Default



[Add reply URL](#)

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

3

SAML Certificates

Token signing certificate

 Edit

Status	Active
Thumbprint	123456789abcdefghijklmnop
Expiration	6/3/2028, 8:39:10 AM
Notification Email	someuser@example.com
App Federation Metadata Url	https://login.microsoftonline.com/af42bac0-52aa- ...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

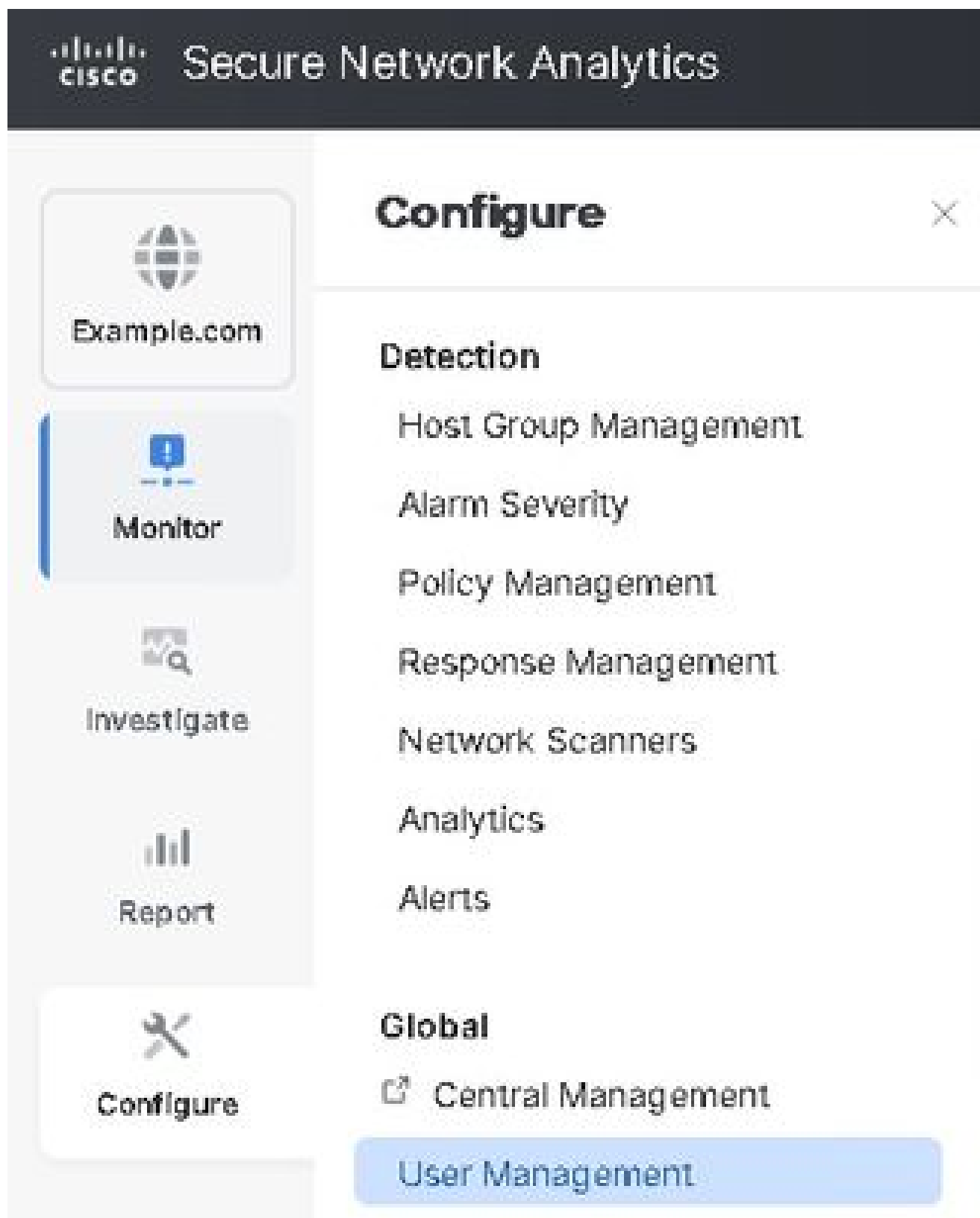
Verification certificates (optional)

 Edit

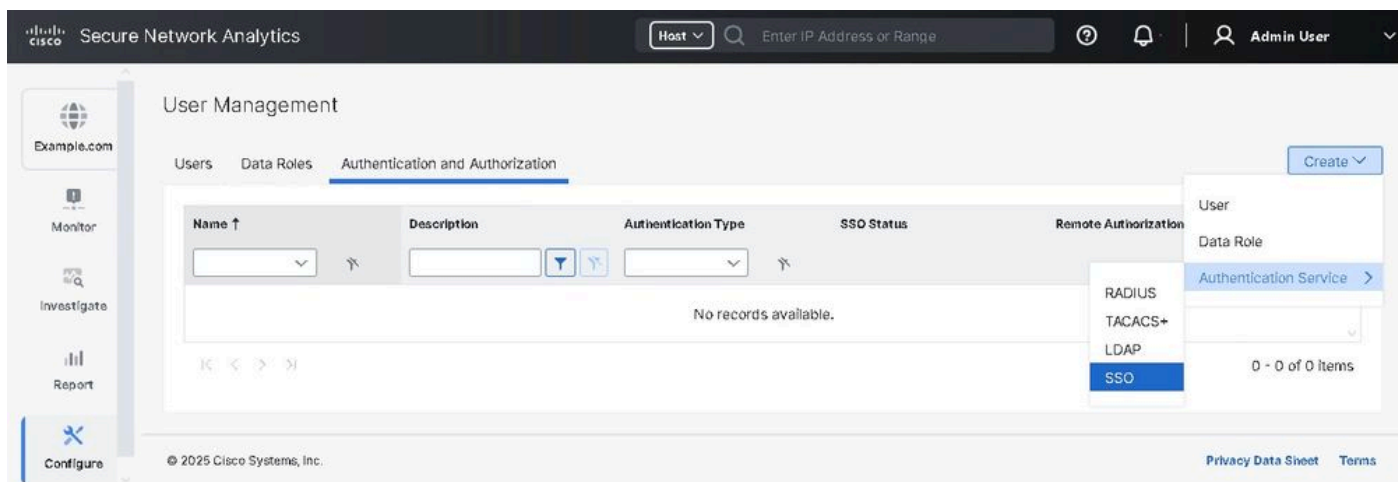
Required	No
Active	0
Expired	0

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。



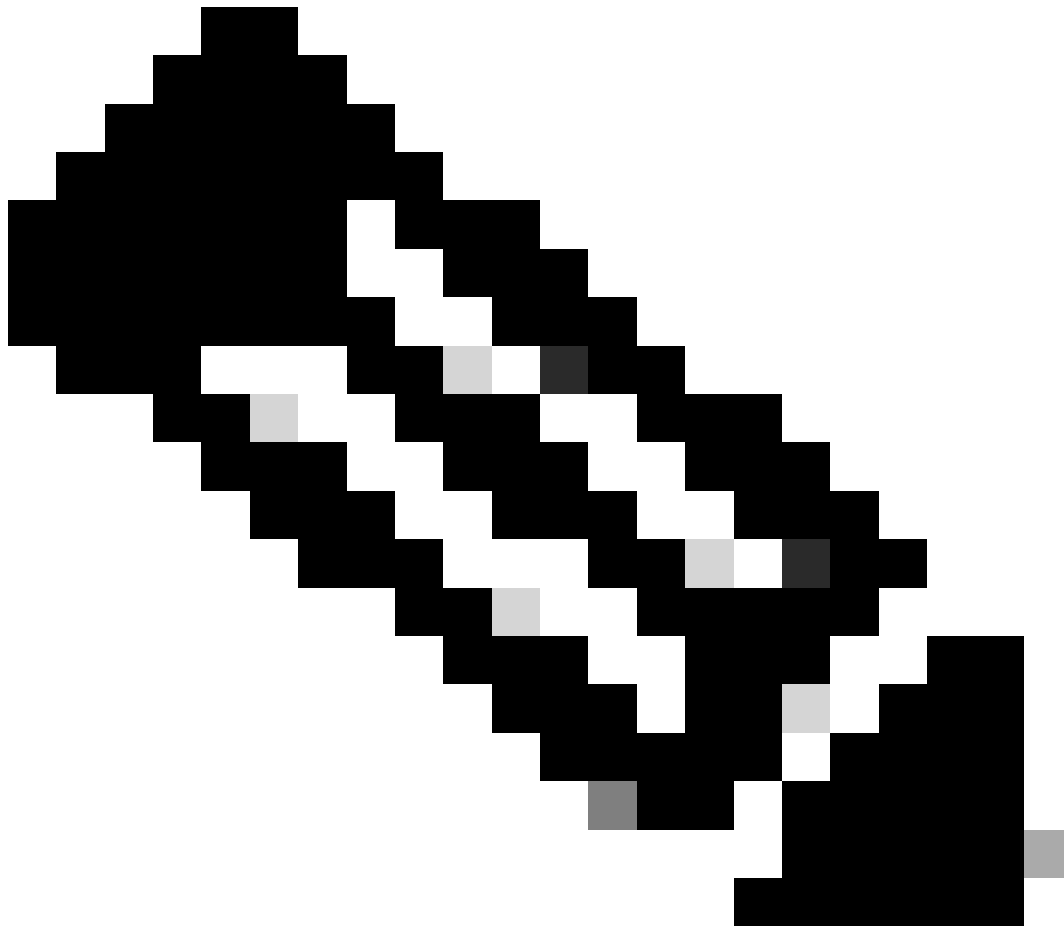
3. 在Authentication and Authorization頁籤下，按一下Create > Authentication Service > SSO。



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。

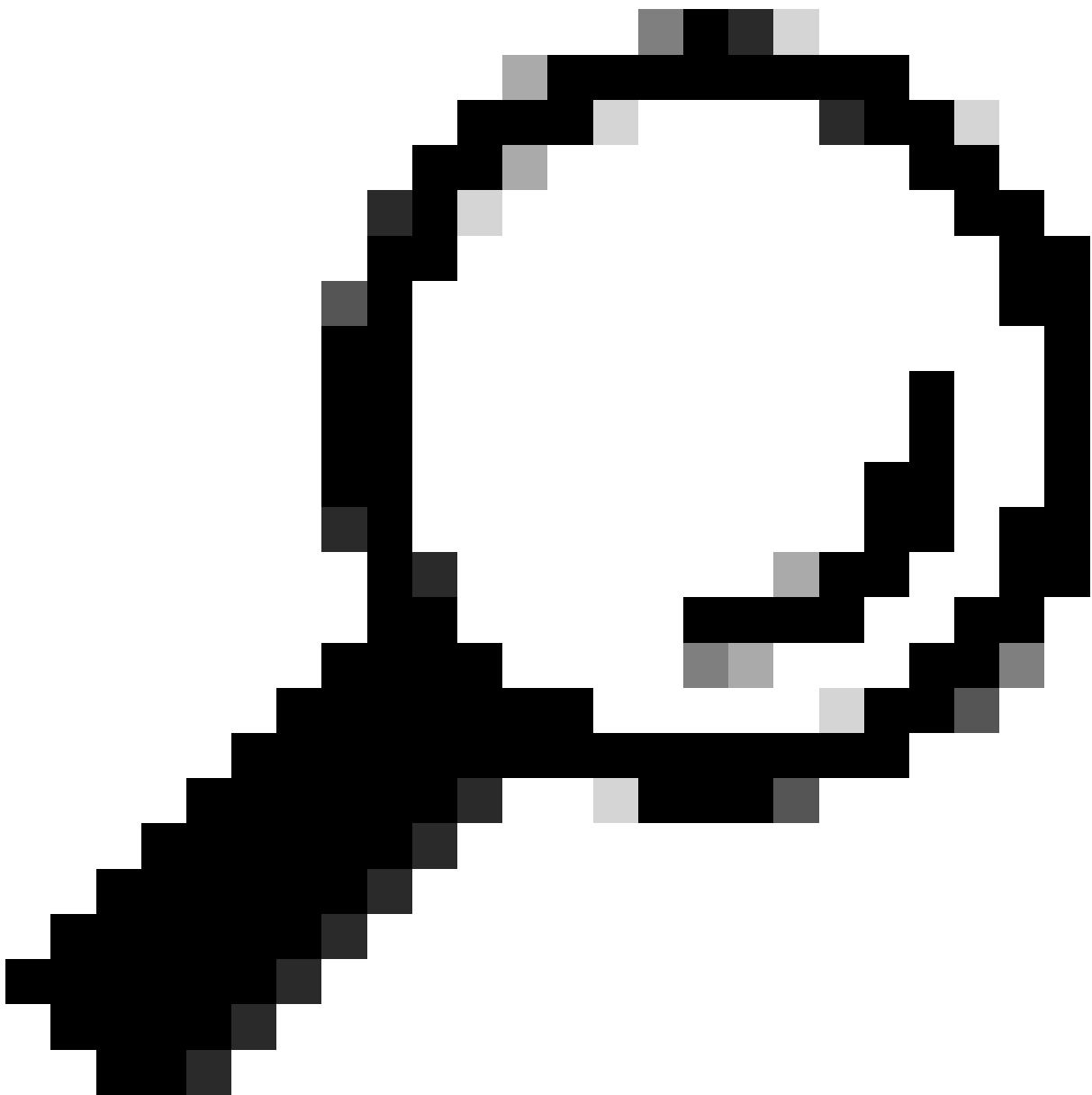
The screenshot shows the 'User Management | Authentication Service' configuration page. It includes a 'Cancel' and 'Save' button in the top right. The page is divided into three main sections:

- Authentication Service:** Contains fields for 'Authentication Service Type' (set to SSO), 'Name' (set to SSO), and 'Description'.
- Identity Provider:** Contains fields for 'Identity Provider Type' (set to Microsoft Entra ID), 'Status' (set to Ready), and two options for metadata: 'Identity Provider Metadata URL' (unselected) and 'Upload Identity Provider Metadata XML File' (selected). The XML upload option includes a note 'XML format required' and an 'Add File' button.
- General Configuration:** Contains fields for 'Name Identifier Format' (set to Persistent), 'Login Screen Label' (set to popup), and 'Custom Service Provider Address' (with an example: ex. sna-manager.example.com or 192.168.10.10).



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。

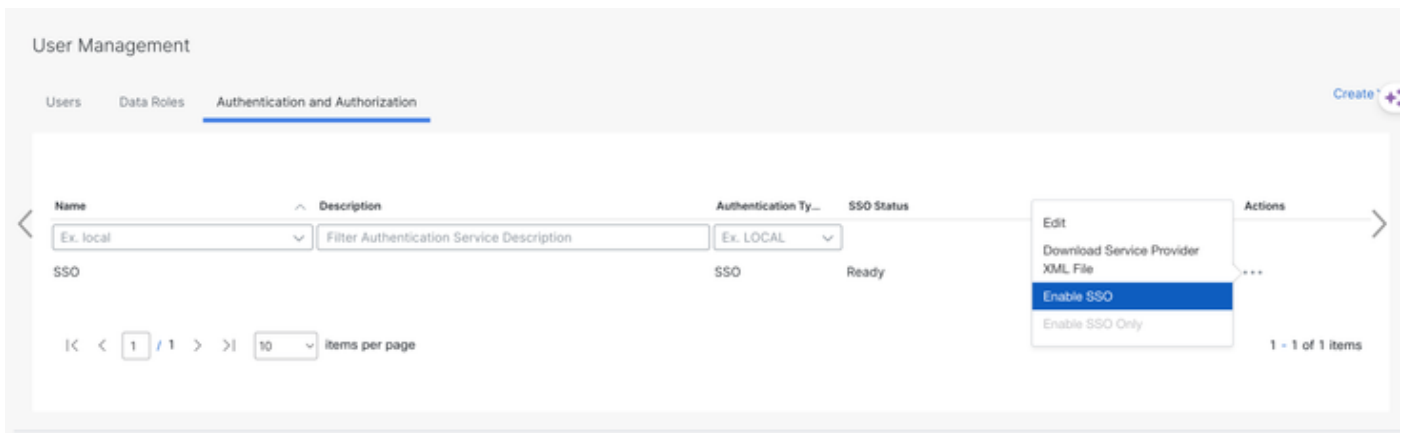
5.將「身份提供程式型別」字段配置為Microsoft Entra ID，將名稱識別符號格式配置為Persistent，鍵入Login Screen Label。



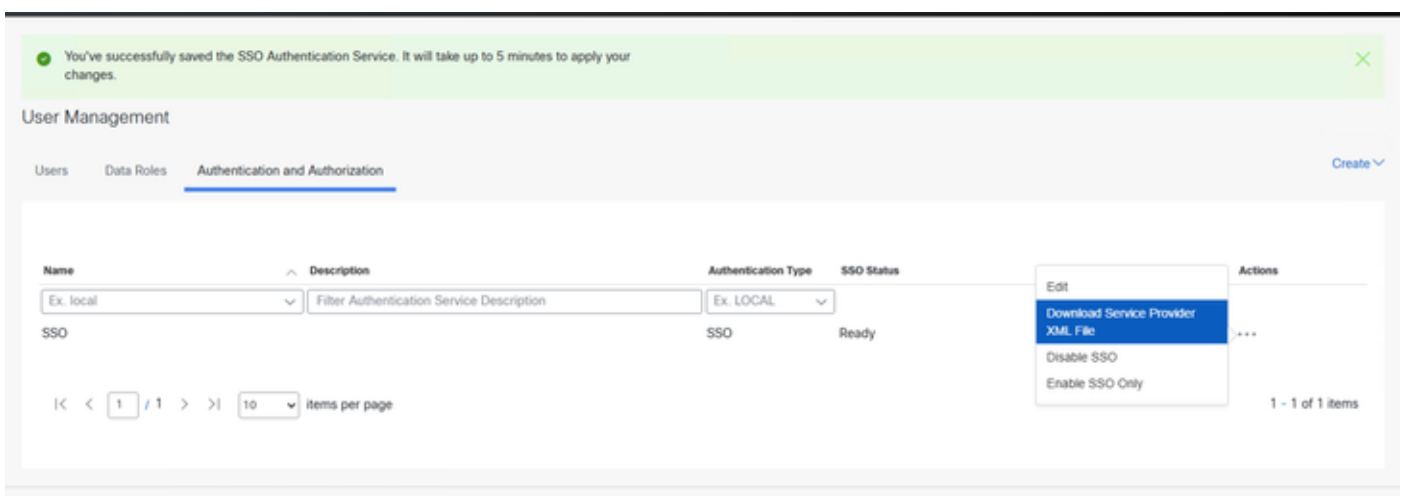
提示：已配置的登入螢幕標籤（名稱/文本）顯示在Login In with SSO按鈕上方，不應留空。

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。

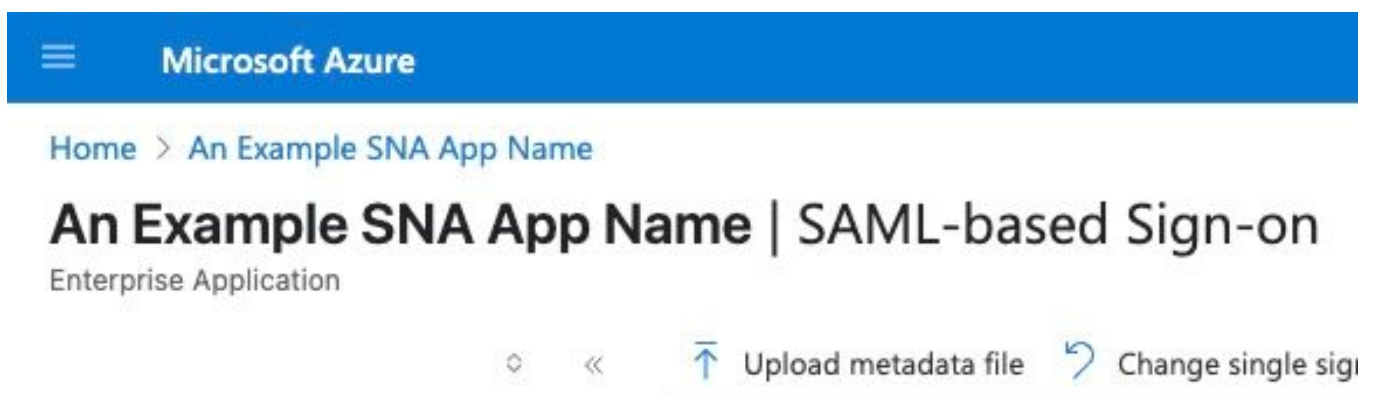


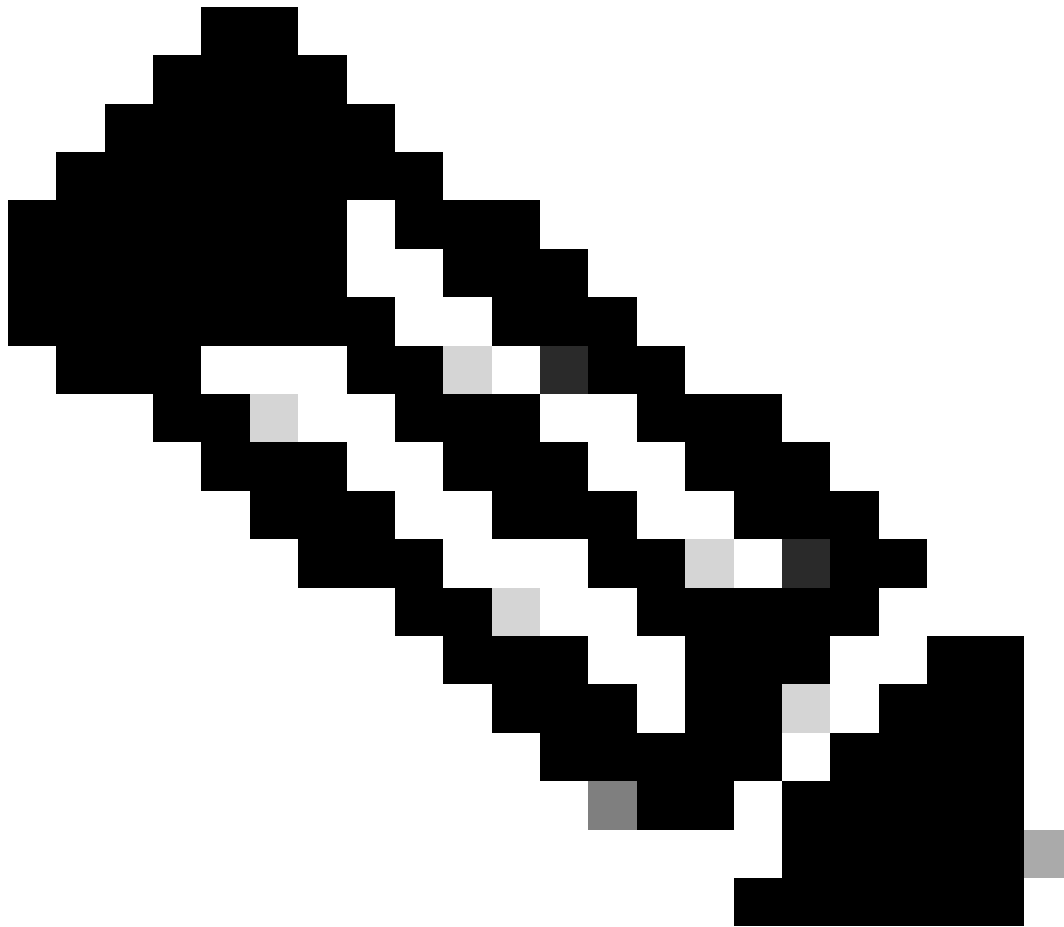
8.在「Authentication and Authorization」頁籤下，按一下「Actions」列中的三個點，然後按一下「Download Service Provider XML File」。



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。

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating An Example SNA App Name.

1

Basic SAML Configuration

Edit

Identifier (Entity ID)	https://example.com/fedlet
Reply URL (Assertion Consumer Service URL)	https://your-sna-manager-fqdn.com/fedlet/fedletapplication
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

2

Attributes & Claims

Edit

Edit u

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

6.按一下宣告名稱部分下的user.userprincipalname值。

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

Attributes & Claims ...

+ Add new claim + Add a group claim Columns | Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...] ...

7.在「管理索賠」頁下「驗證」選擇名稱識別符號格式。



Manage claim ...



Save



Discard changes



Got feedback?

Name

nameidentifier

Namespace

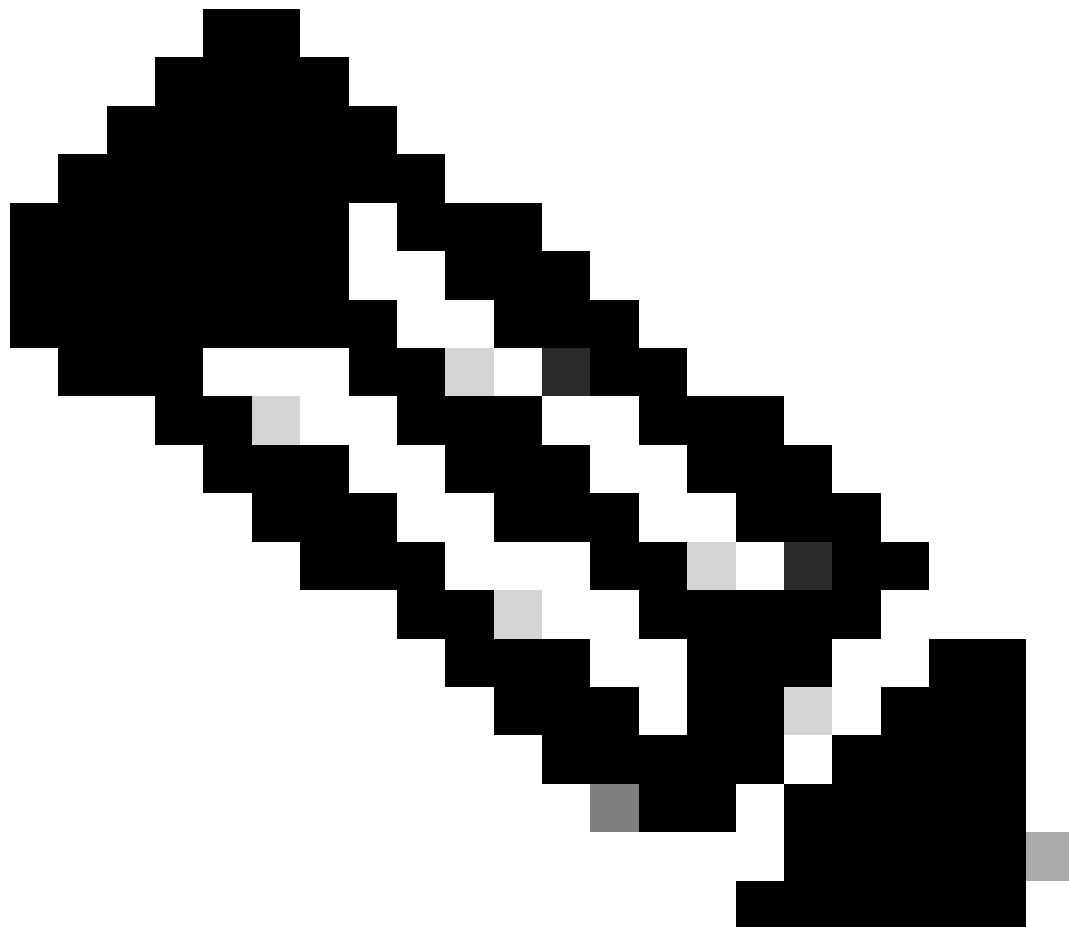
http://schemas.xmlsoap.org/ws/2005/05/identity/claims



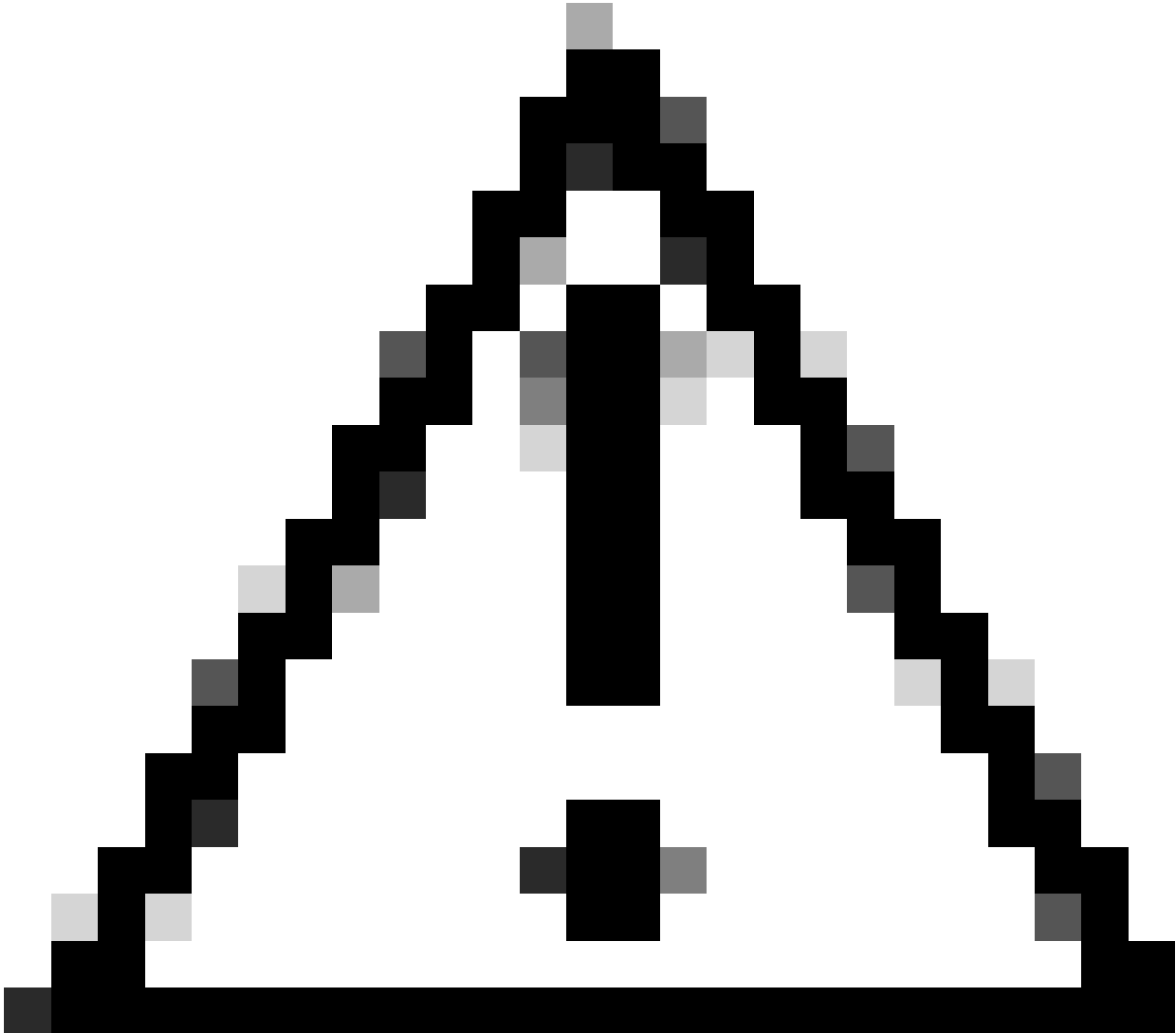
Choose name identifier format

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」。

Microsoft Azure

Home > An Example SNA App Name

An Example SNA App Name | Users and groups

Enterprise Application

◊ << + Add user/group ✎ Edit assignment 🗑 Remove as

Overview

Deployment Plan

Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups** ☆

📘 The application will appear for assigned users within My App

Assign users and groups to app-roles for your application here

🔍 First 200 shown, search all users & groups

Display name

No application assignments found

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。

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > An Example SNA App Name | Users and groups >

Add Assignment

Example Organization

Users and groups

None Selected

Select a role

User

Users and groups

Try changing or adding filters if you don't see what you're looking for.

Search

1 result found

All Users Groups

	Name	Type	Details
☒	 Example User	User	user@example.com

Selected (1)

Reset

 Example User
user@example.com

Assign

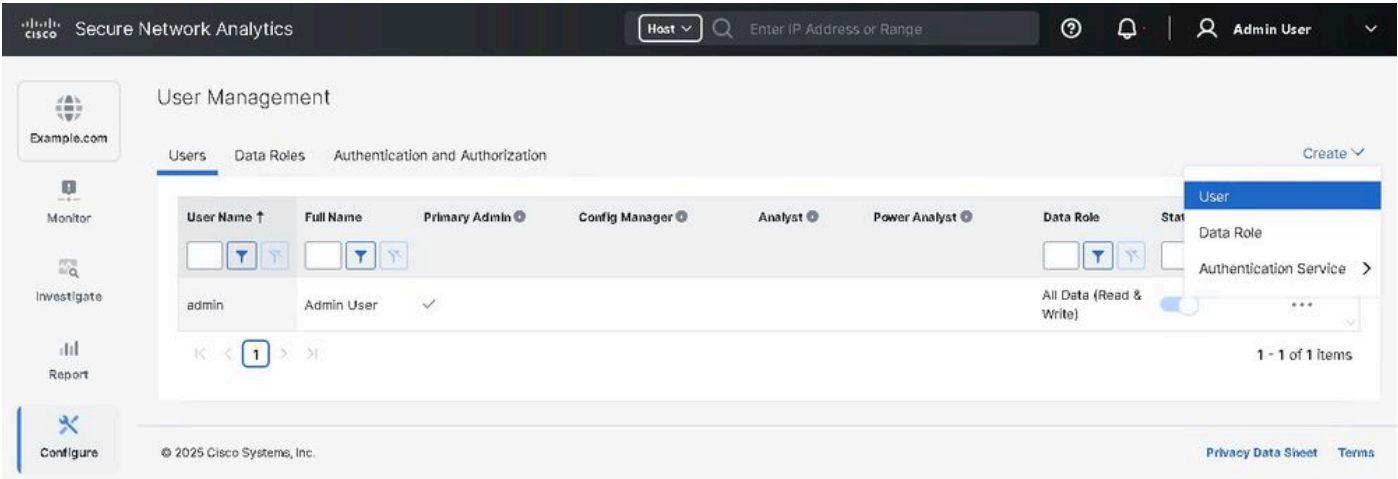
Select

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。

User Name *

Full Name

Email

SAML ID *

Authentication Service

SSO

Password

Generate Password

Confirm Password

Show Password

Role Settings

Primary Admin

Data Role

All Data (Read Only)

You must select a minimum of one web role and one desktop client role.

Web

Desktop

Web Roles * Compare

Configuration Manager

Analyst

Power Analyst

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）。