將SWA外部身份驗證配置為ISE作為RADIUS伺服器

目錄

簡介

本文檔介紹將思科ISE作為RADIUS伺服器在安全Web訪問(SWA)上配置外部身份驗證的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Secure Web Appliance的基本知識。
- 瞭解ISE上的身份驗證和授權策略配置。
- 基本RADIUS知識。

思科建議您：

- SWA和ISE管理訪問。
- 相容的WSA和ISE版本。

採用元件

本檔案中的資訊是根據以下軟體版本：

- SWA 14.0.2-012
- ISE 3.0.0

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。

背景資訊

為SWA的管理使用者啟用外部身份驗證時，裝置會使用外部身份驗證配置中指定的輕型目錄訪問協定(LDAP)或RADIUS伺服器驗證使用者憑證。

網路拓撲

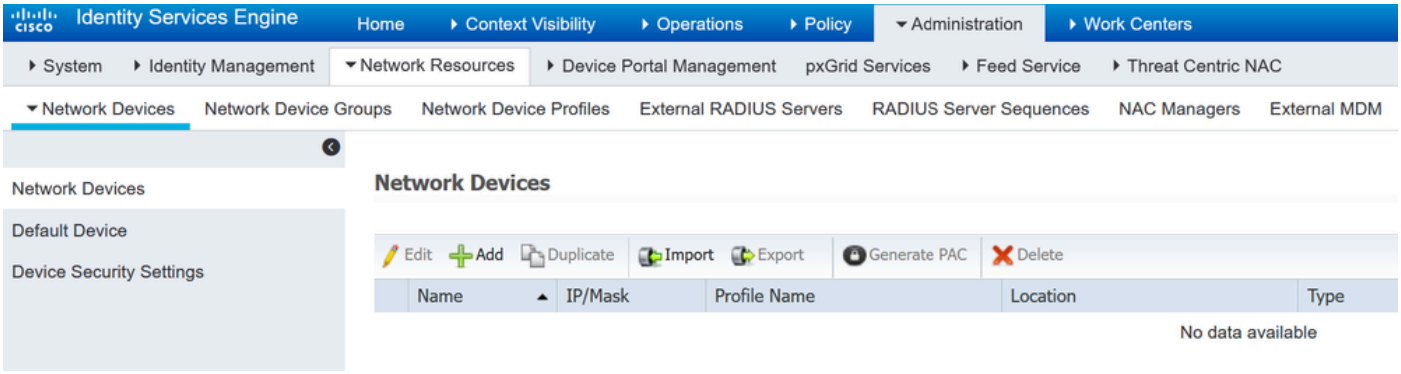
網路拓撲圖

管理使用者使用其憑據訪問埠443上的SWA。SWA使用RADIUS伺服器驗證憑證。

設定

ISE 組態

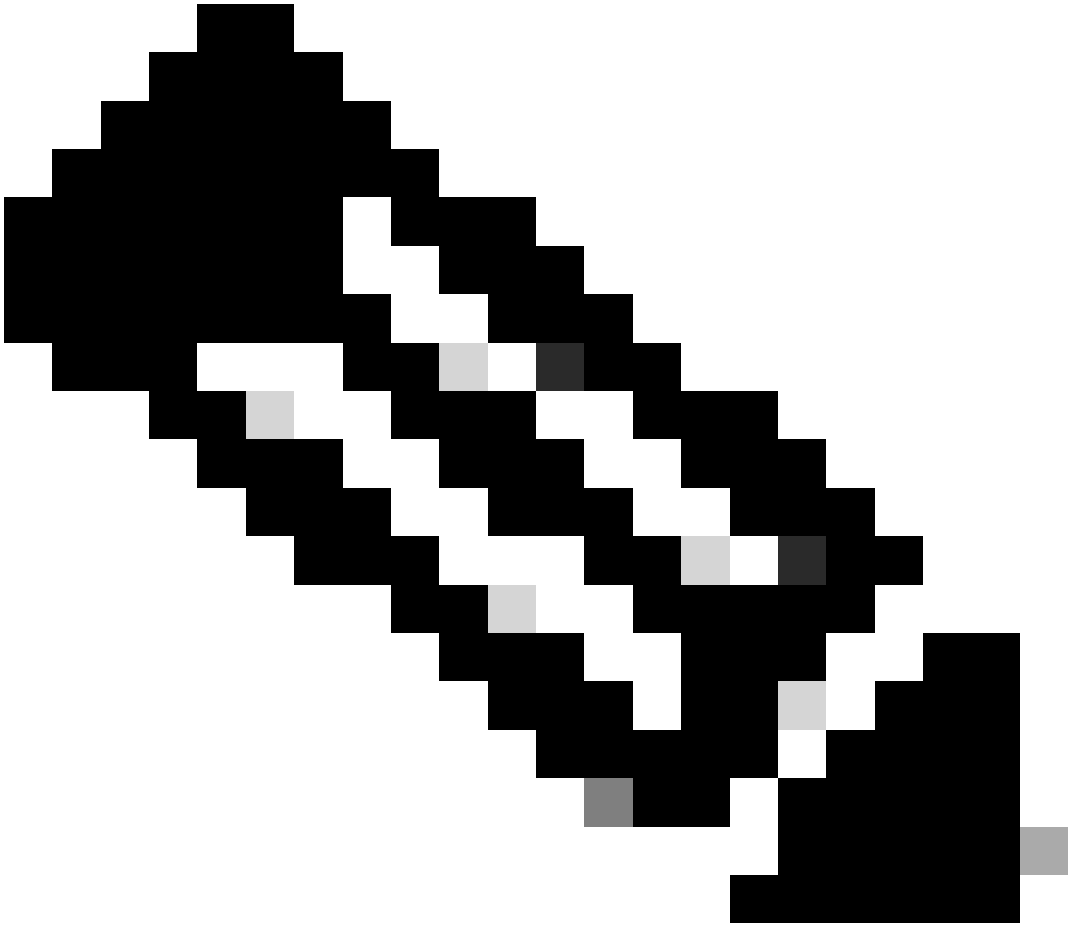
步驟 1. 新增網路裝置。導航到管理>網路資源>網路裝置> +增加。



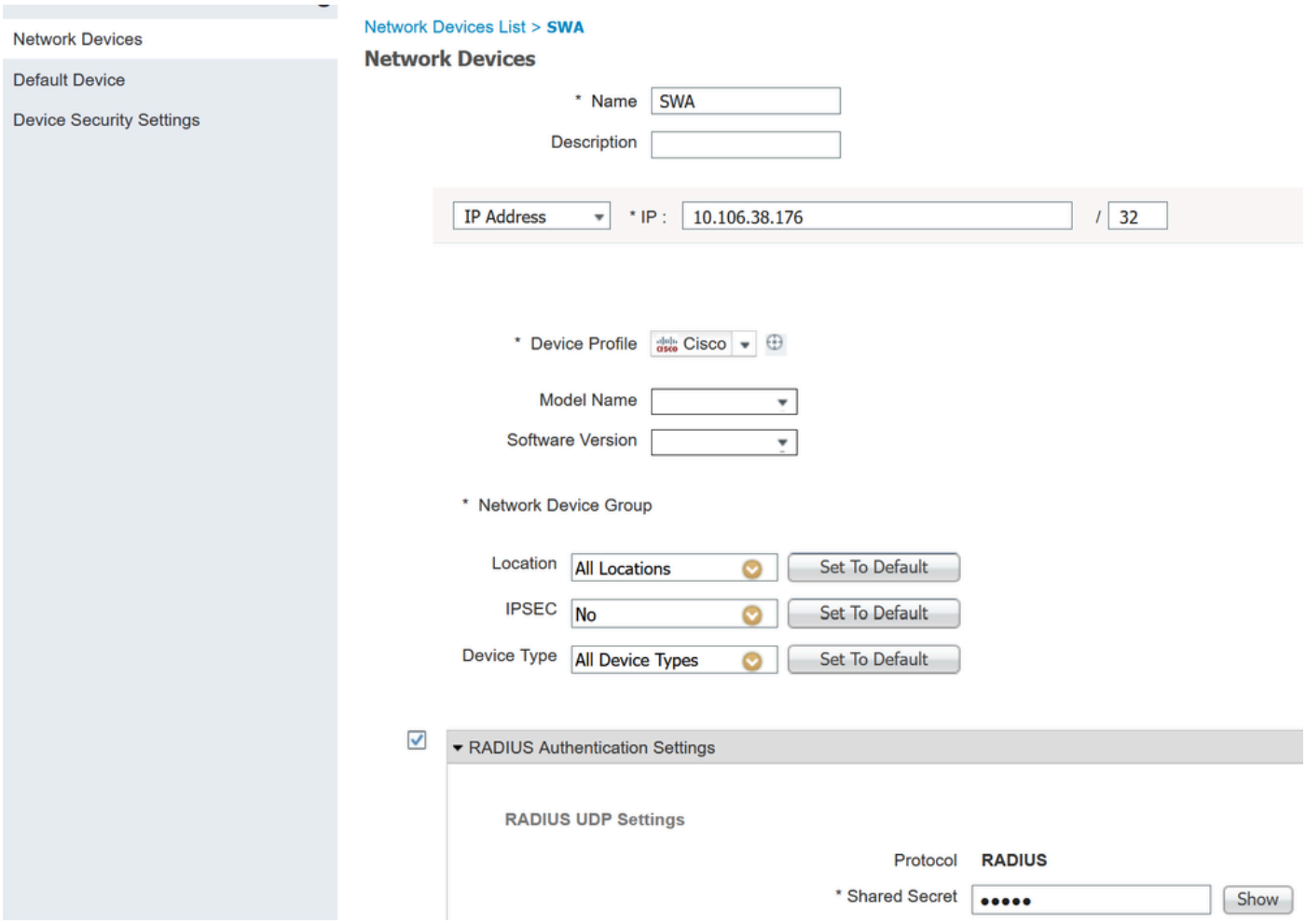
在ISE中增加SWA作為網路裝置

步驟 2. 為網路裝置對象分配名稱並插入SWA IP地址。

選中RADIUS 覈取方塊並定義共用金鑰。

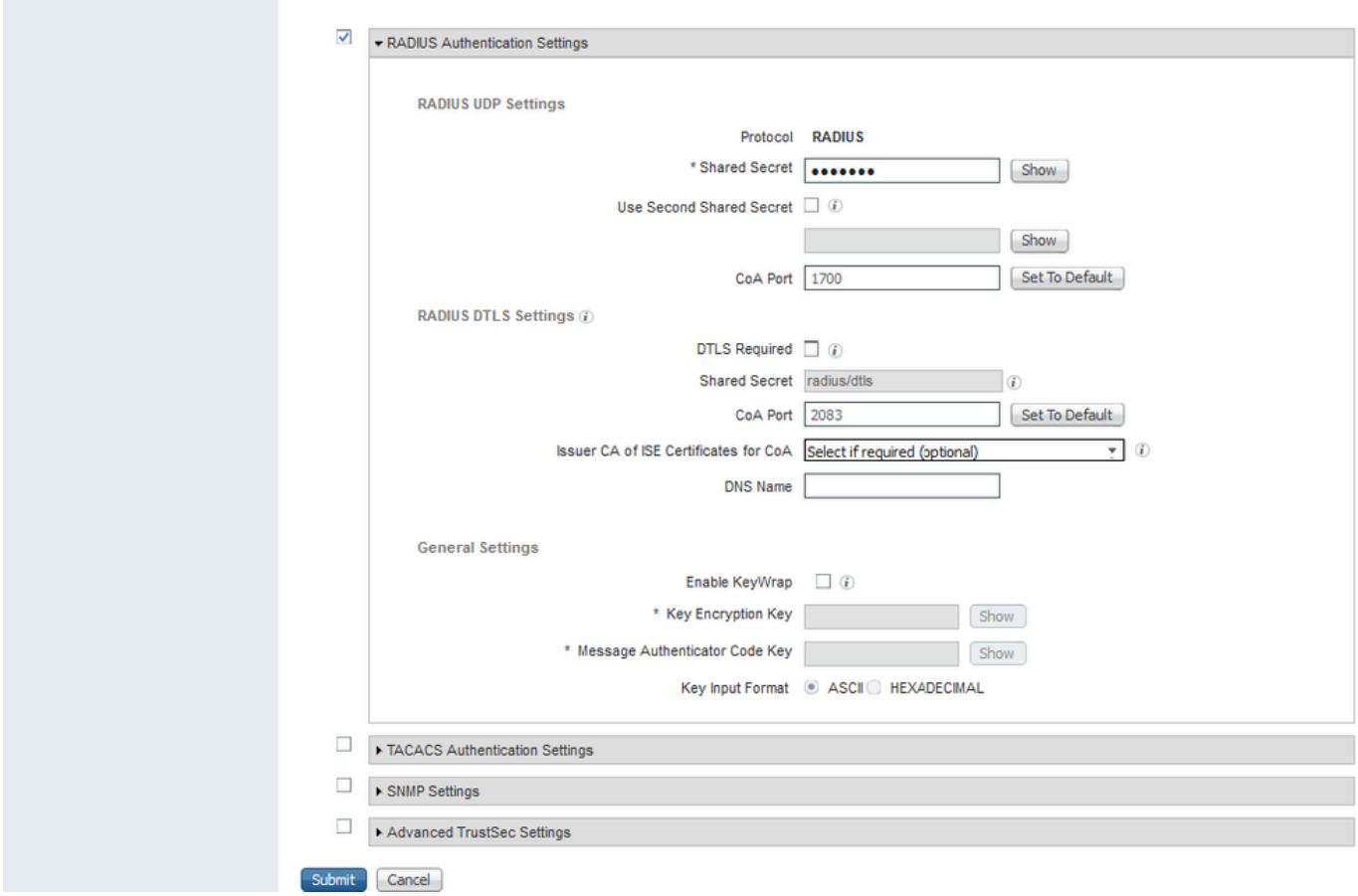


注意：稍後必須使用相同的金鑰在SWA中配置RADIUS伺服器。



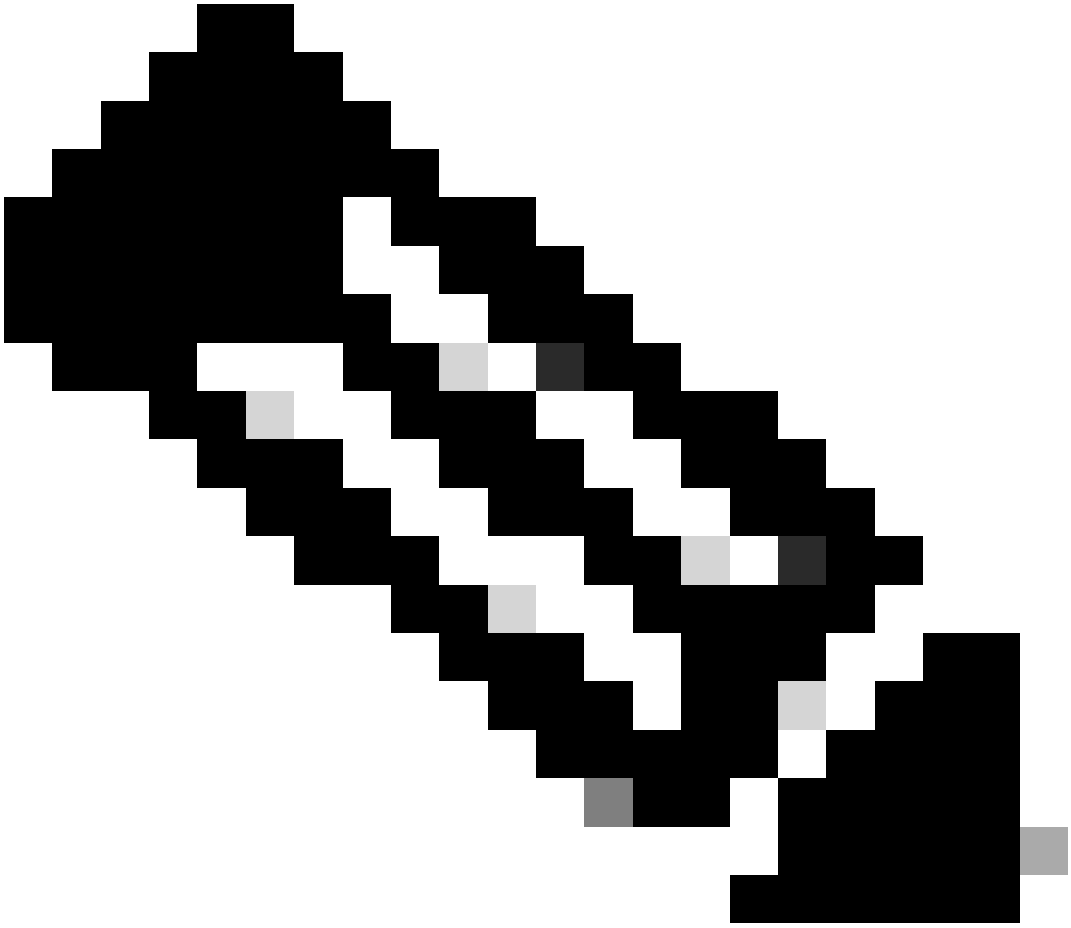
配置SWA網路裝置共用金鑰

步驟 2.1.按一下Submit。

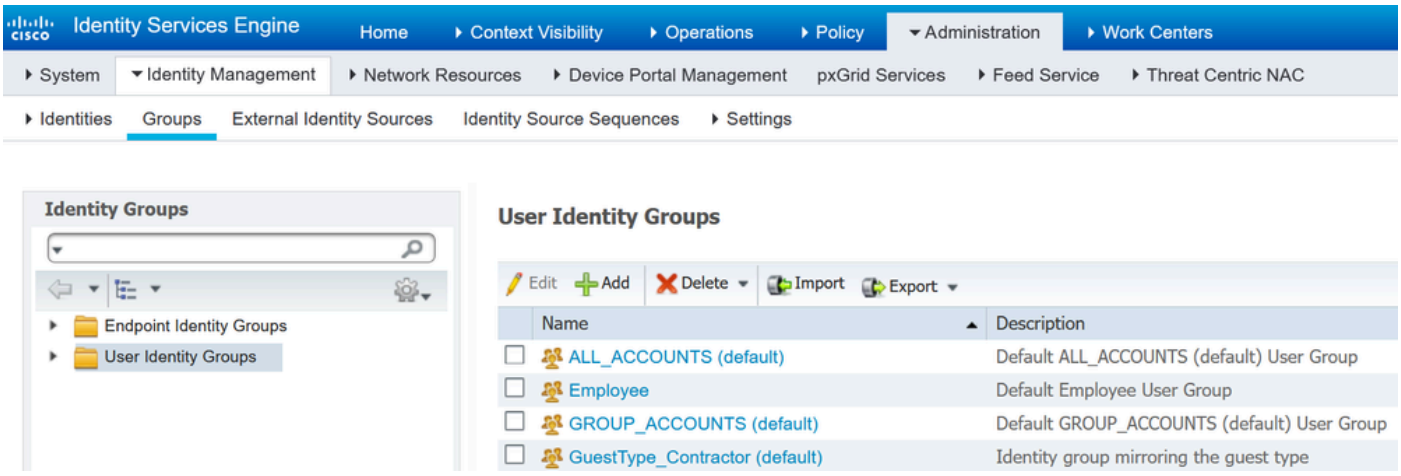


提交網路裝置配置

步驟 3. 建立所需的使用者身份組。導航到Administration > Identity Management > Groups > User Identity Groups > + Add。

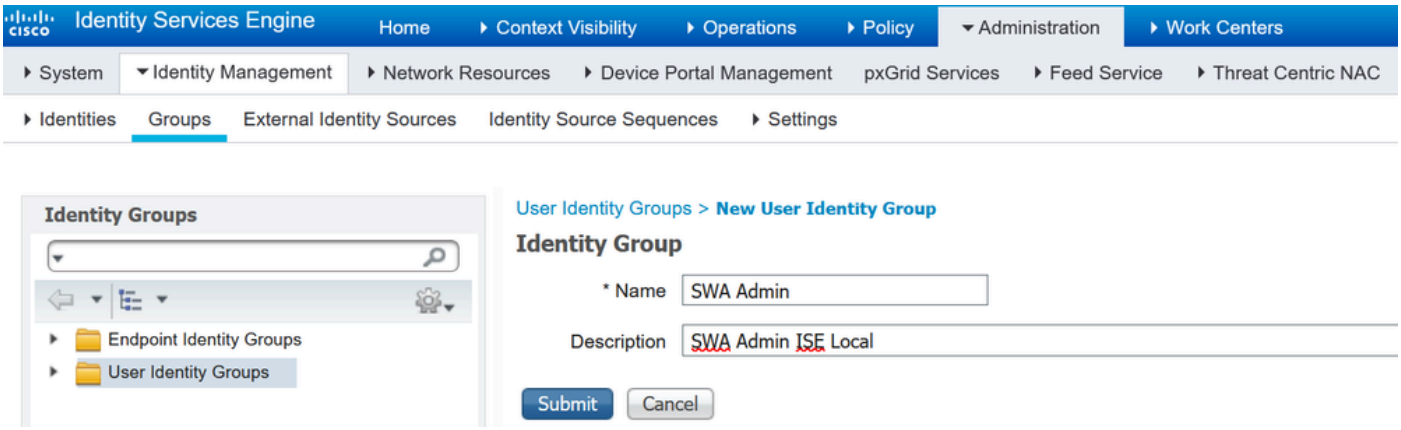


注意：您需要配置不同的使用者組以匹配不同型別的使用者。

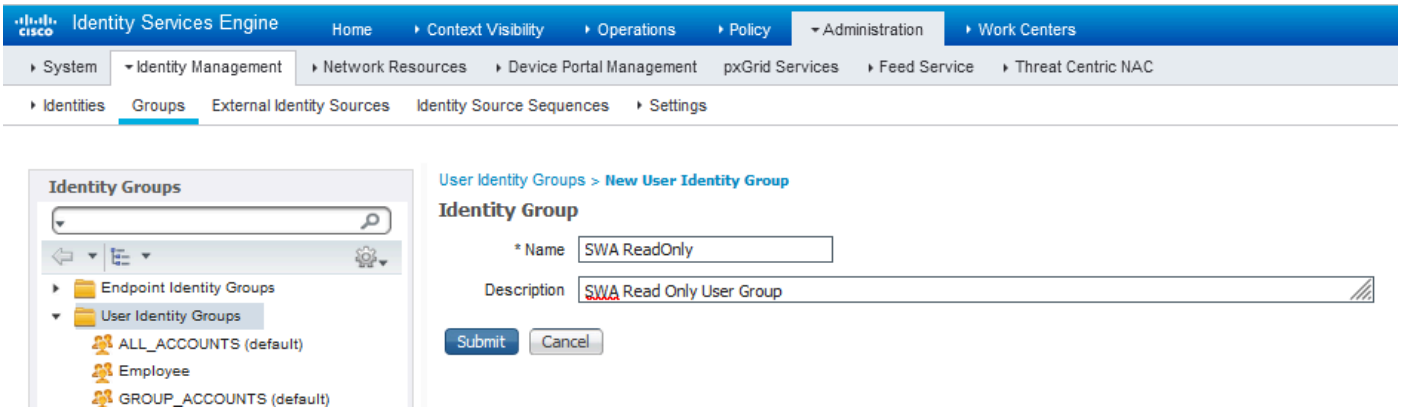


增加使用者身份組

步驟 4.輸入組名、說明（可選）和提交。對每個群組重複這些步驟。在本例中，您為管理員使用者建立一個組，為只讀使用者建立一個組。



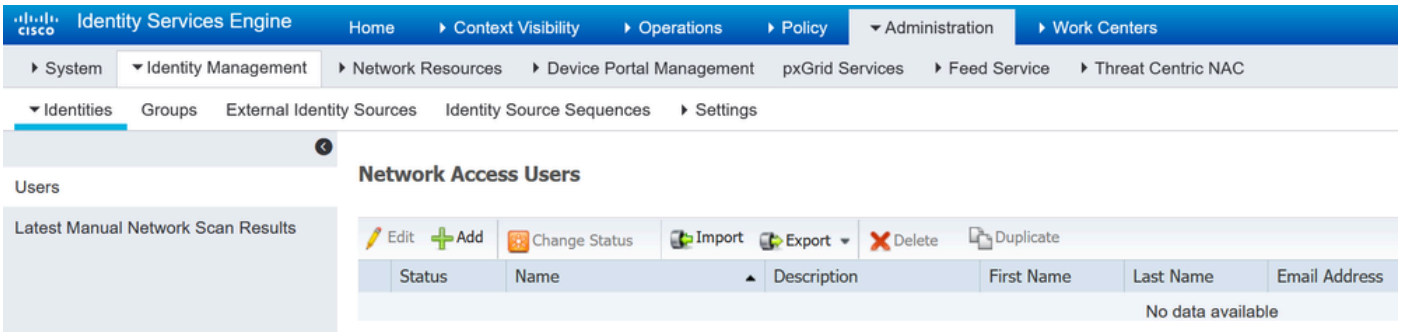
增加使用者身份



組為SWA只讀使用者增加使用者身份組

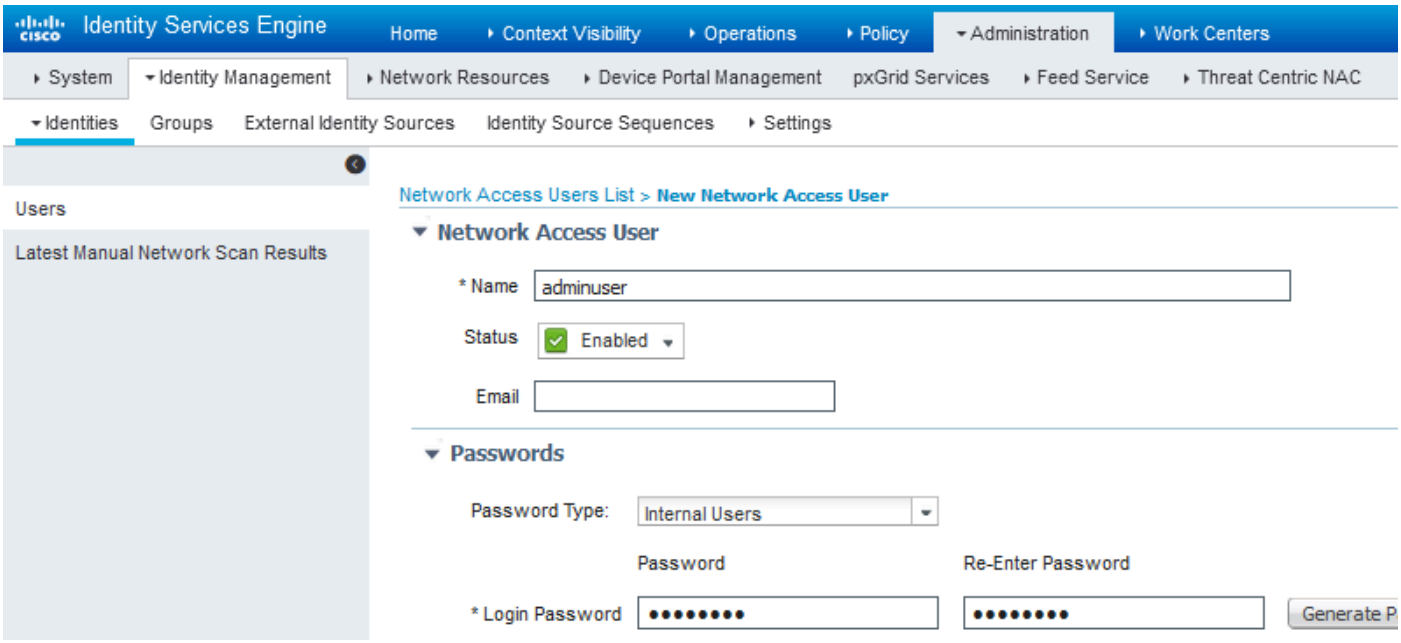
步驟 5.您需要建立與SWA中配置的使用者名稱匹配的網路訪問使用者。

建立網路訪問使用者並將他們增加到其對應組。導航到管理>身份管理>身份> + Add。



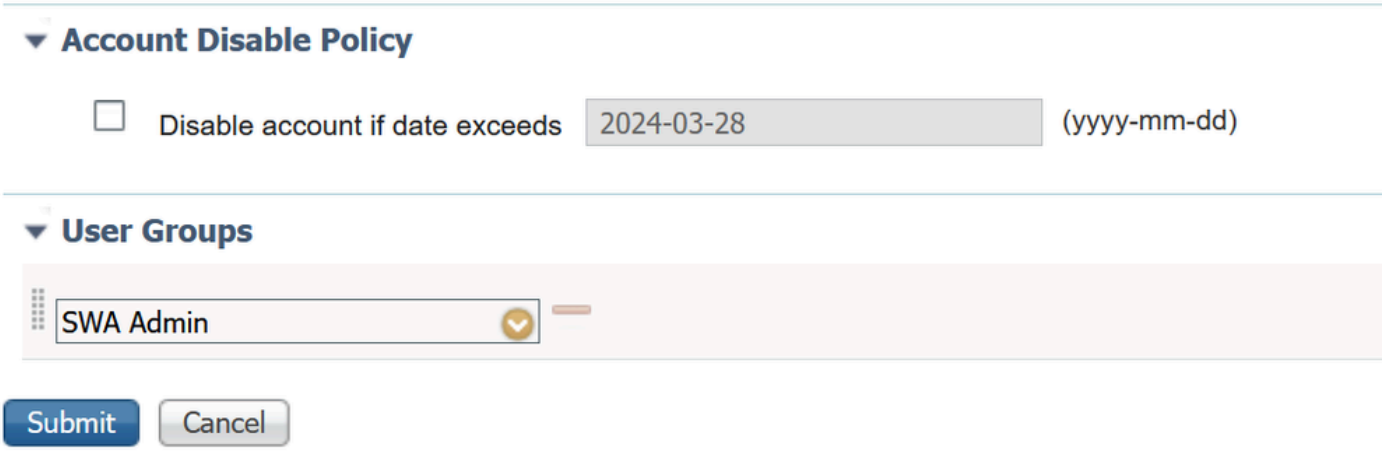
在ISE中增加本地使用者

步驟 5.1.您需要建立具有管理員許可權的網路訪問使用者。指定名稱和密碼。



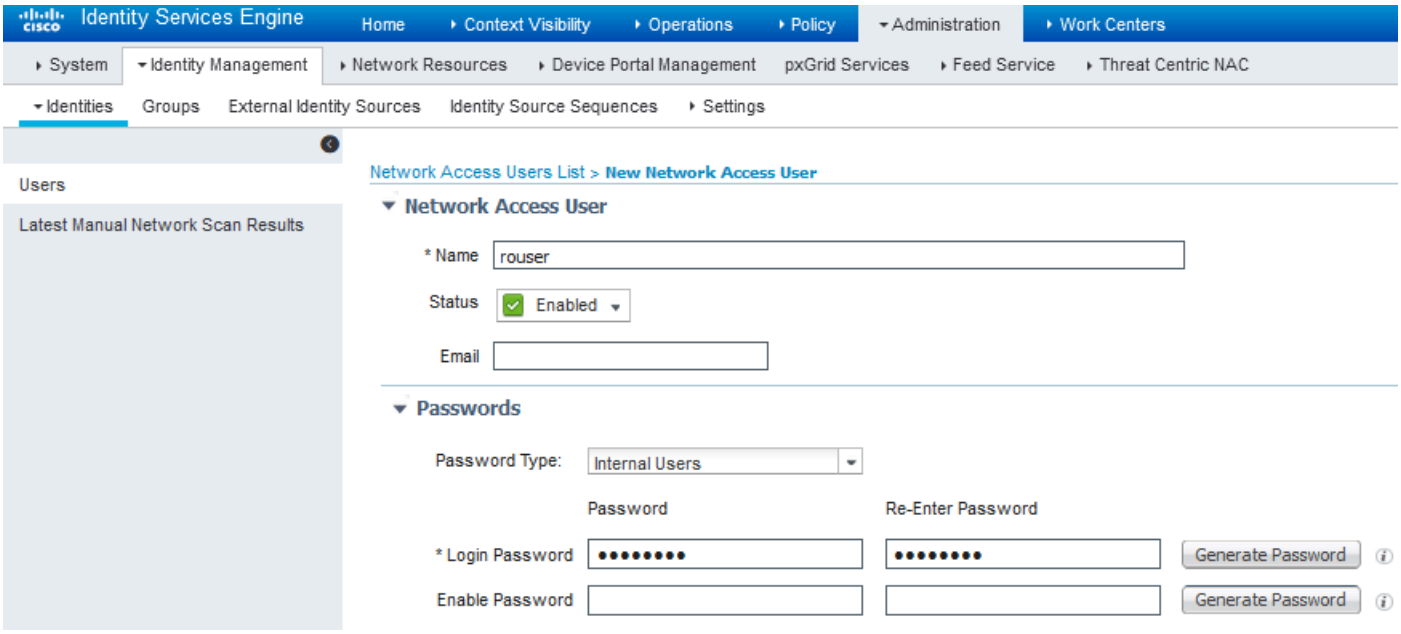
增加管理員使用者

步驟 5.2.在User Groups部分中選擇SWA Admin。



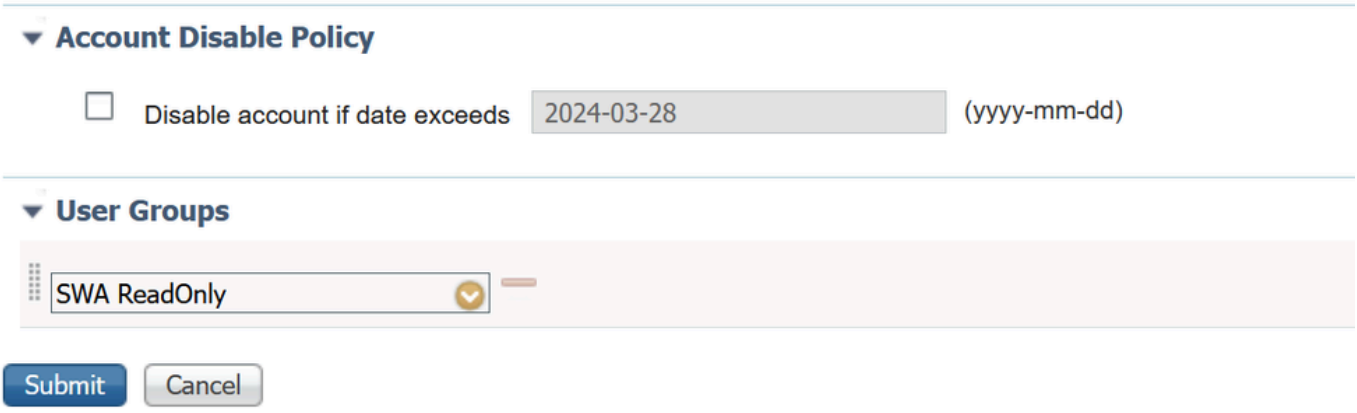
將Admin Group分配給Admin使用者

步驟 5.3.您需要建立具有唯讀許可權的使用者。指定名稱和密碼。



增加只讀使用者

步驟 5.4.在User Groups部分中選擇SWA ReadOnly。

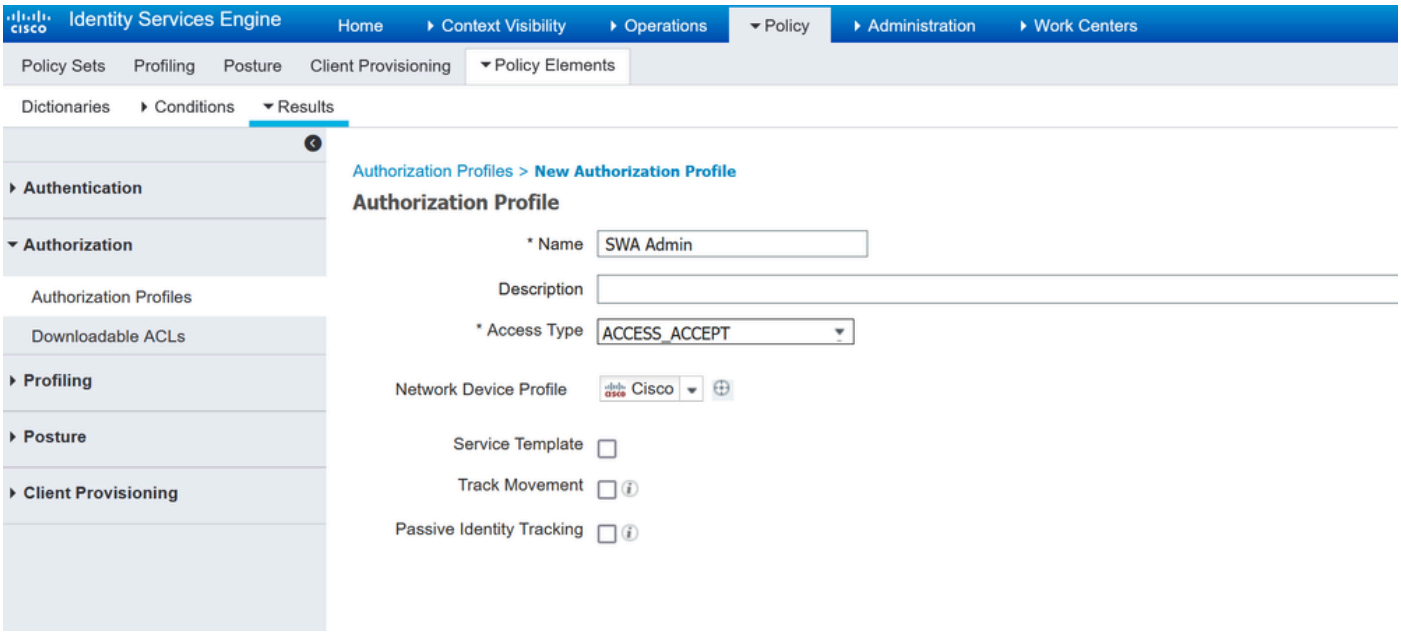


將只讀使用者組分配給只讀使用者

步驟 6. 為Admin使用者建立授權配置檔案。

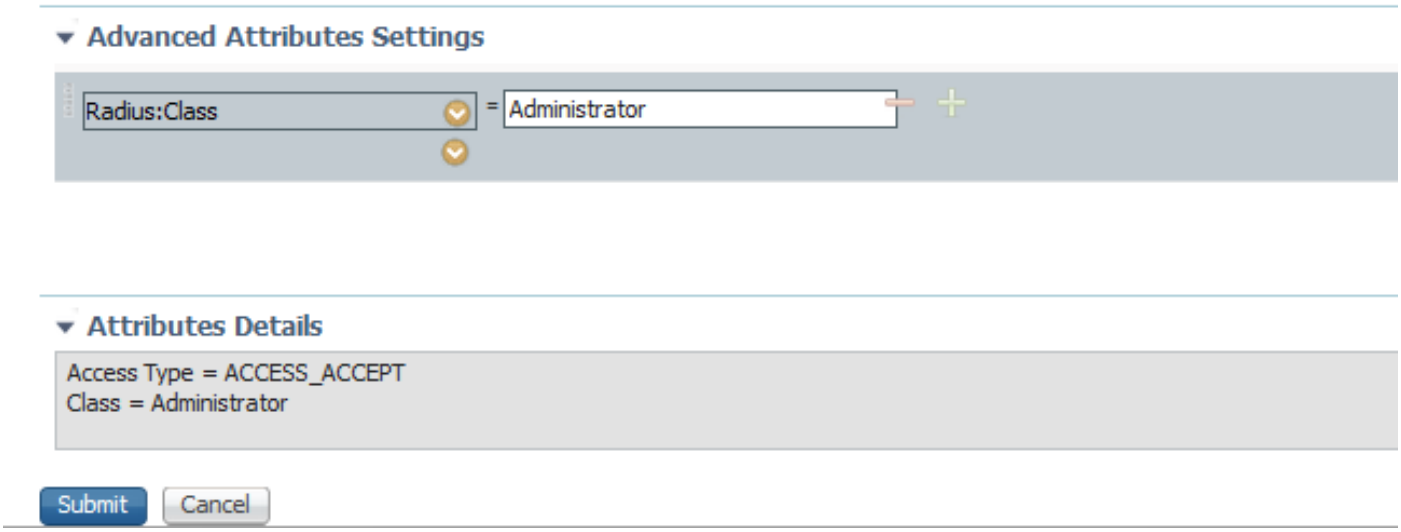
導航到策略>策略元素>結果>授權>授權配置檔案> +增加。

定義授權配置檔案的名稱，並確保訪問型別設定為ACCESS_ACCEPT。



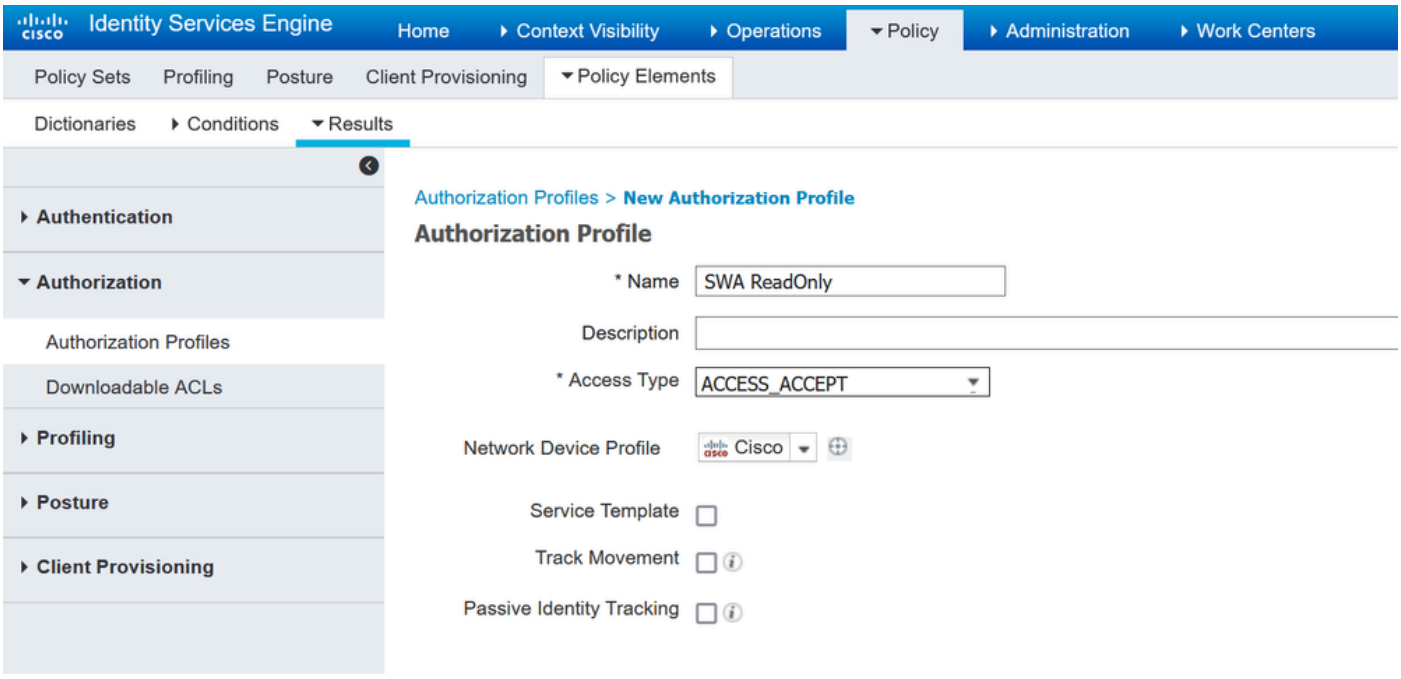
為管理員使用者增加授權配置檔案

步驟 6.1.在「高級屬性設定」中，導航到Radius > Class—[25]，輸入值Administrator，然後按一下Submit。



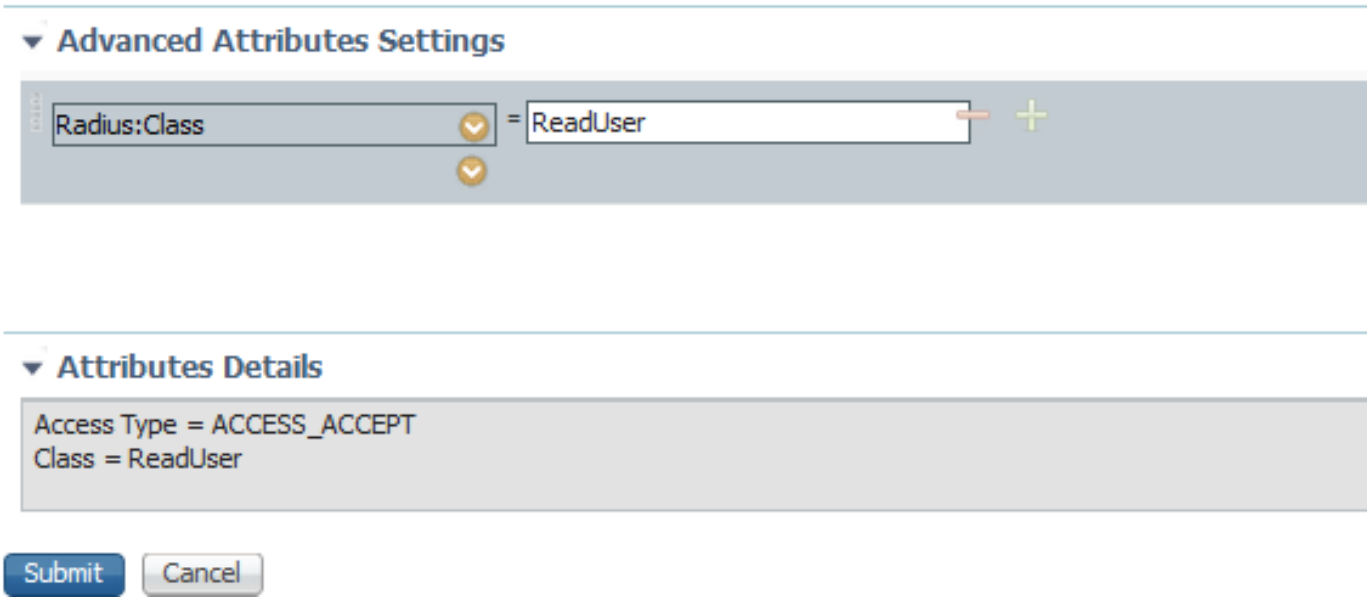
為管理員使用者增加授權配置檔案

步驟 7. 重複步驟6為只讀使用者建立授權配置檔案。



為只讀使用者增加授權配置檔案

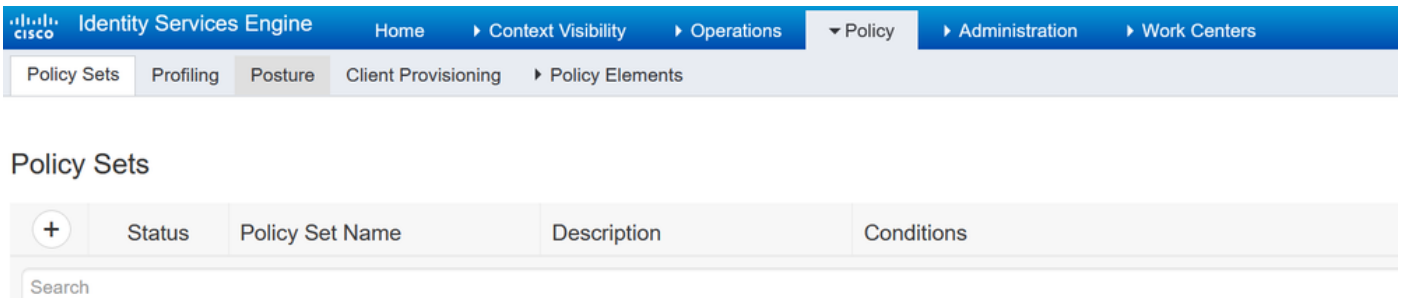
步驟 7.1.這次建立值為ReadUser的Radius：Class，而非Administrator。



為只讀使用者增加授權配置檔案

步驟 8. 建立與SWA IP地址匹配的策略集。這是為了防止使用這些使用者憑證訪問其他裝置。

導航到策略>策略集，點選位於左上角的+圖示。

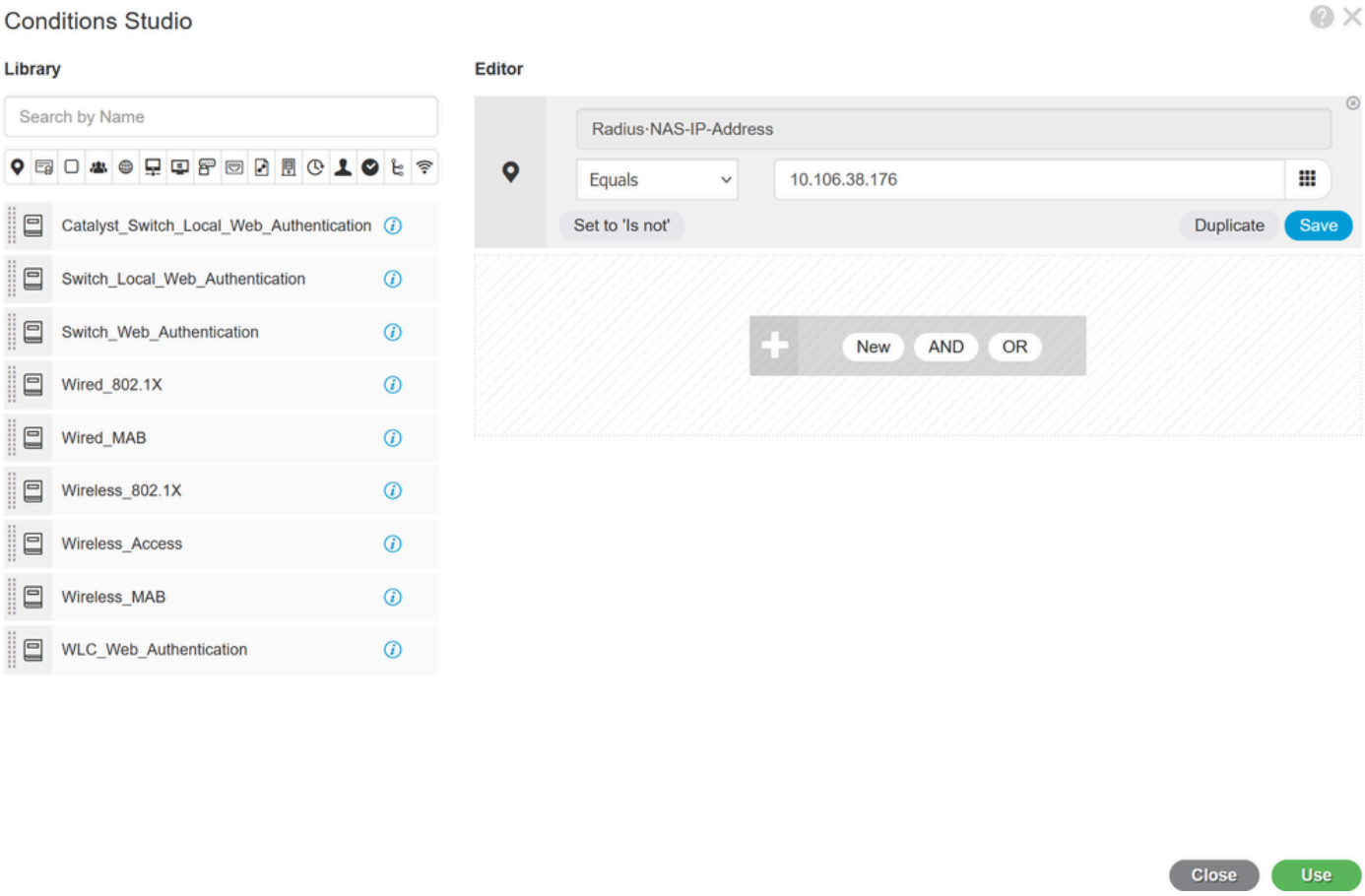


在ISE中增加策略集

步驟 8.1. 新行將放置在策略集的頂部。

為新策略命名，並為RADIUS NAS-IP-Address屬性增加一個條件以匹配SWA IP地址。

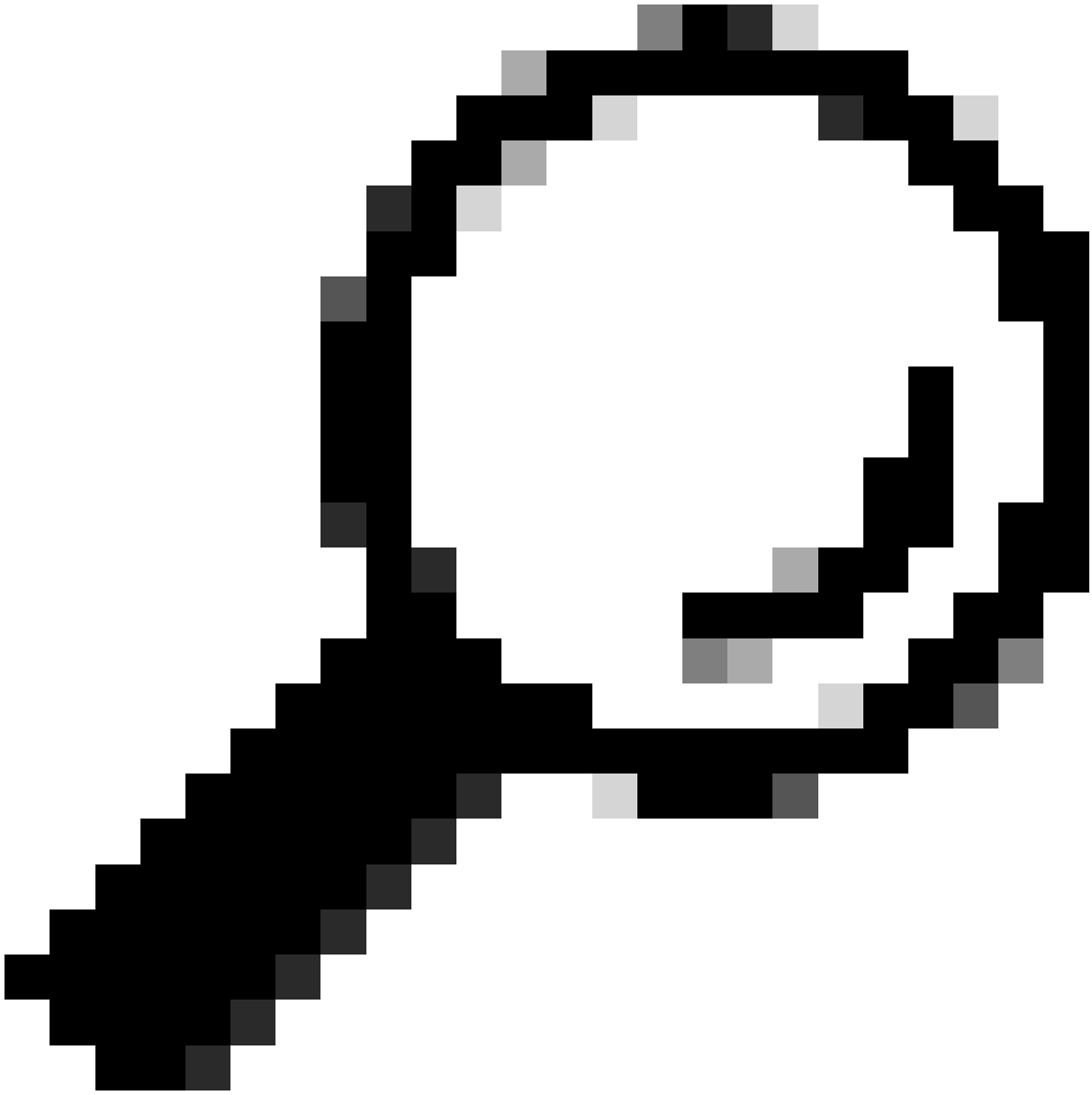
按一下Use以保留更改並退出編輯器。



增加策略以對映SWA網路裝置

步驟 8.2.按一下Save。

策略儲存

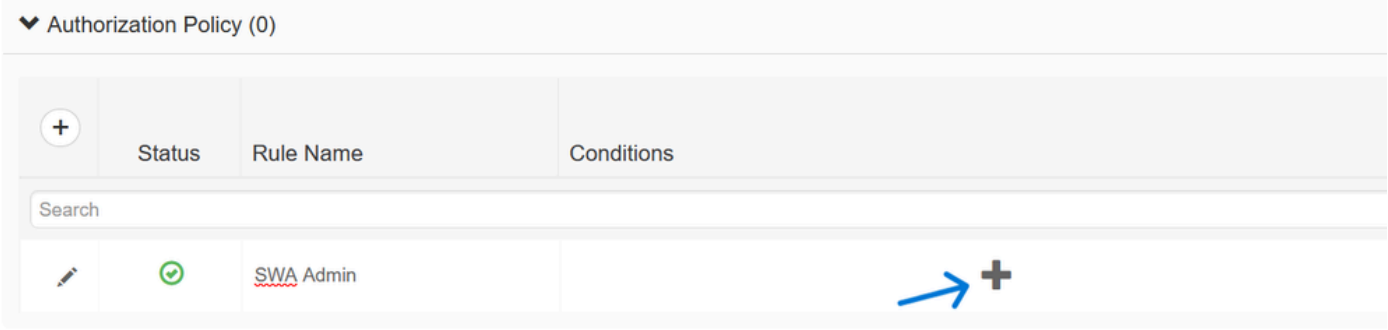


提示：在本文中，允許使用預設網路訪問協定清單。您可以建立新清單，並視需要縮小範圍。

步驟 9.要檢視新的策略集，請點選檢視列中的>圖示。展開Authorization Policy選單，然後按一下+圖示以增加新規則，以允許對具有管理員許可權的使用者進行訪問。

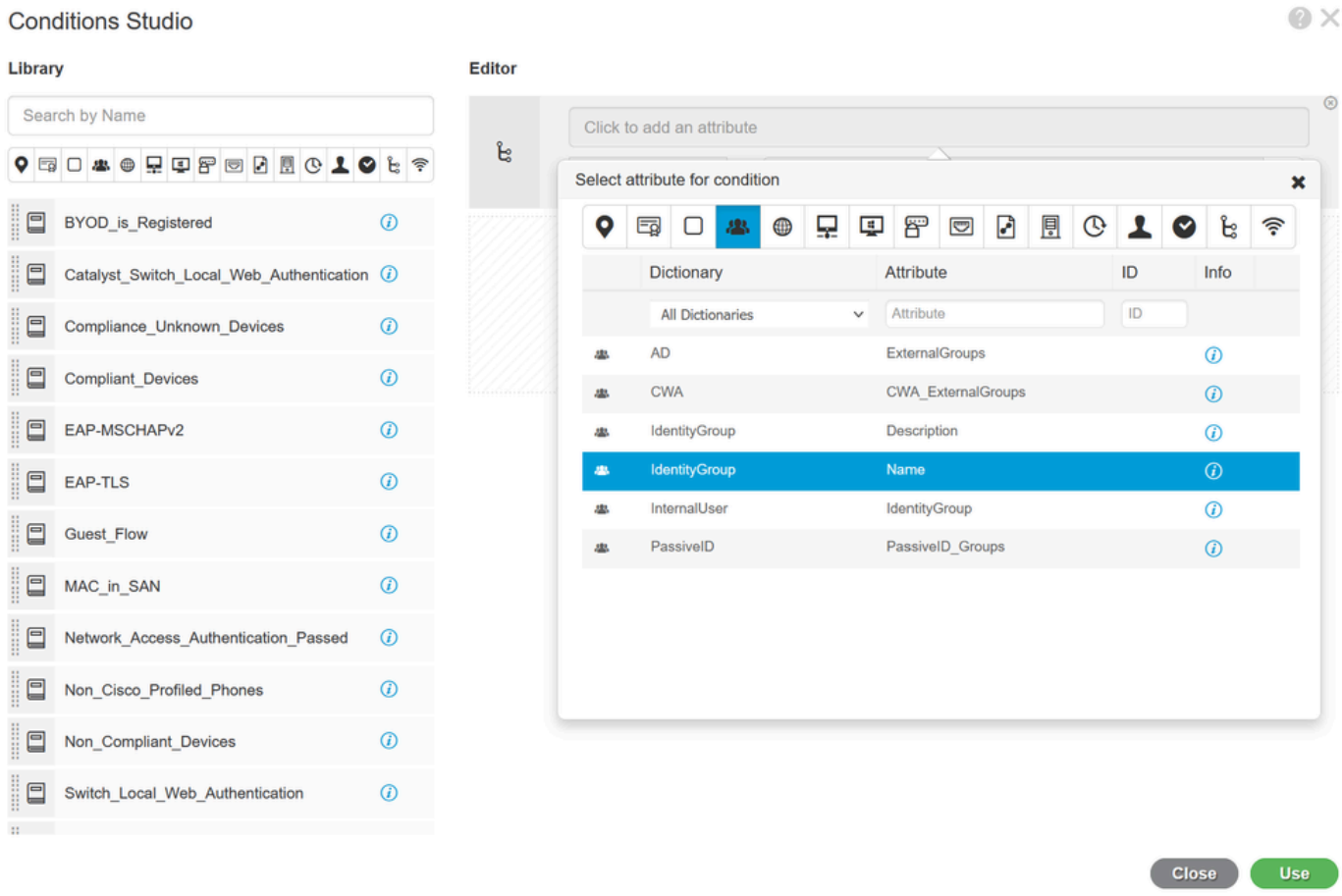
設定名稱。

步驟 9.1.要建立匹配管理員使用者組的條件，請點選+圖示。



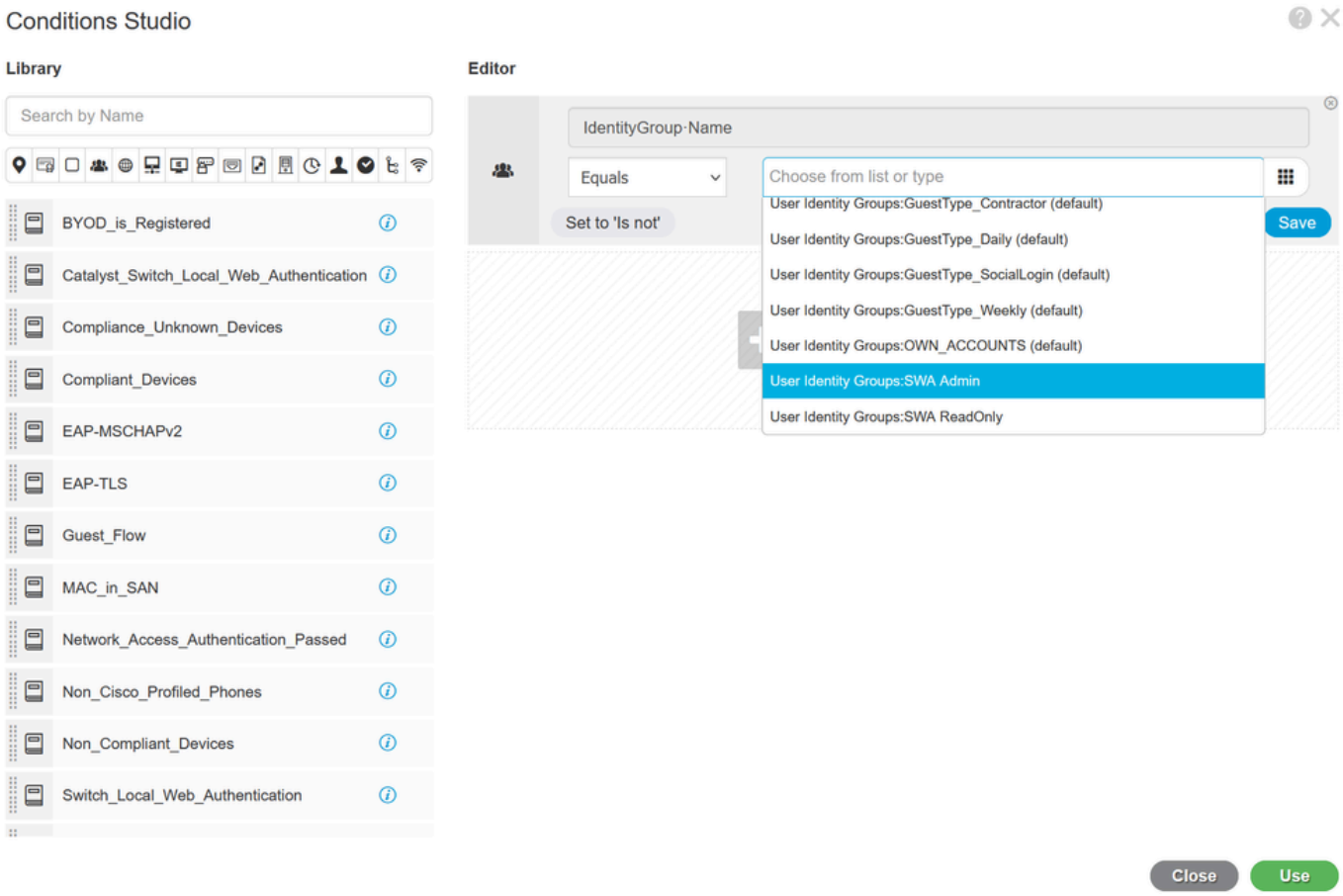
增加授權策略條件

步驟 9.2.設定條件以匹配屬性名稱等於使用者身份組的身份組SWA admin。選



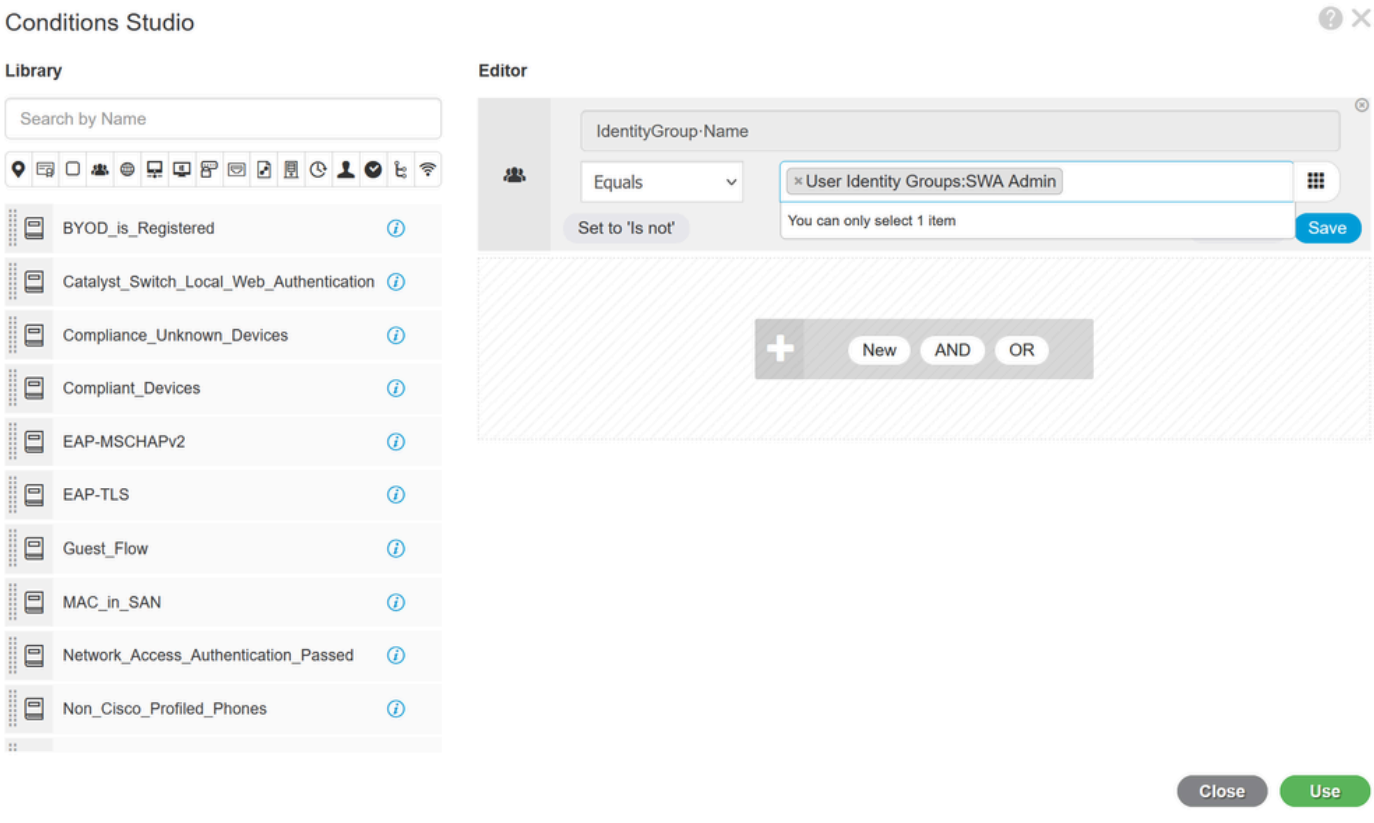
擇身份組作為條件

步驟 9.3.向下滾動並選擇User Identity Groups： SWA admin.



Scroll Down abd Select Identity Group Name

步驟 9.4.按一下Use。

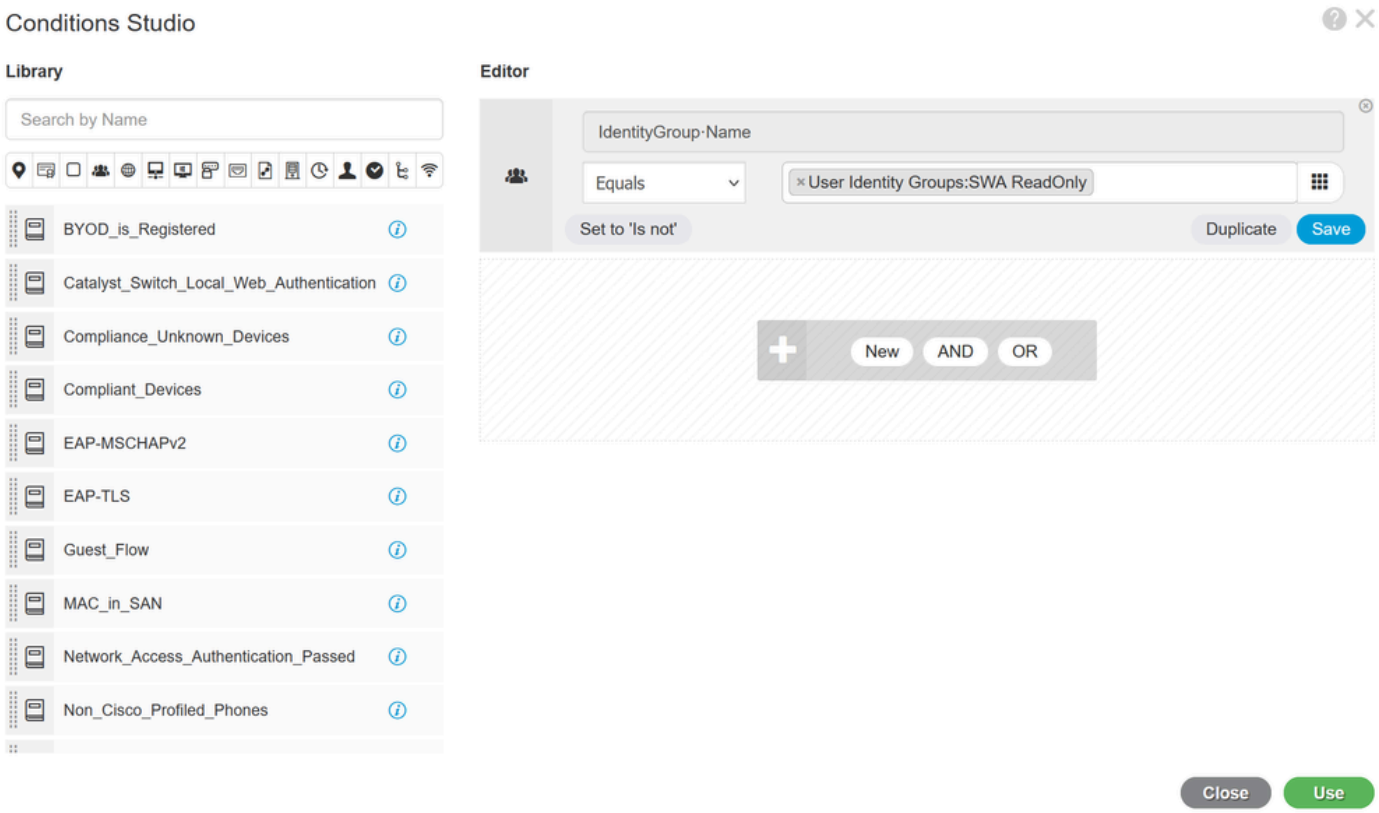


選擇SWA管理員使用者組的授權策略

步驟 10. 點選+圖示增加第二條規則，以允許訪問具有只讀許可權的使用者。

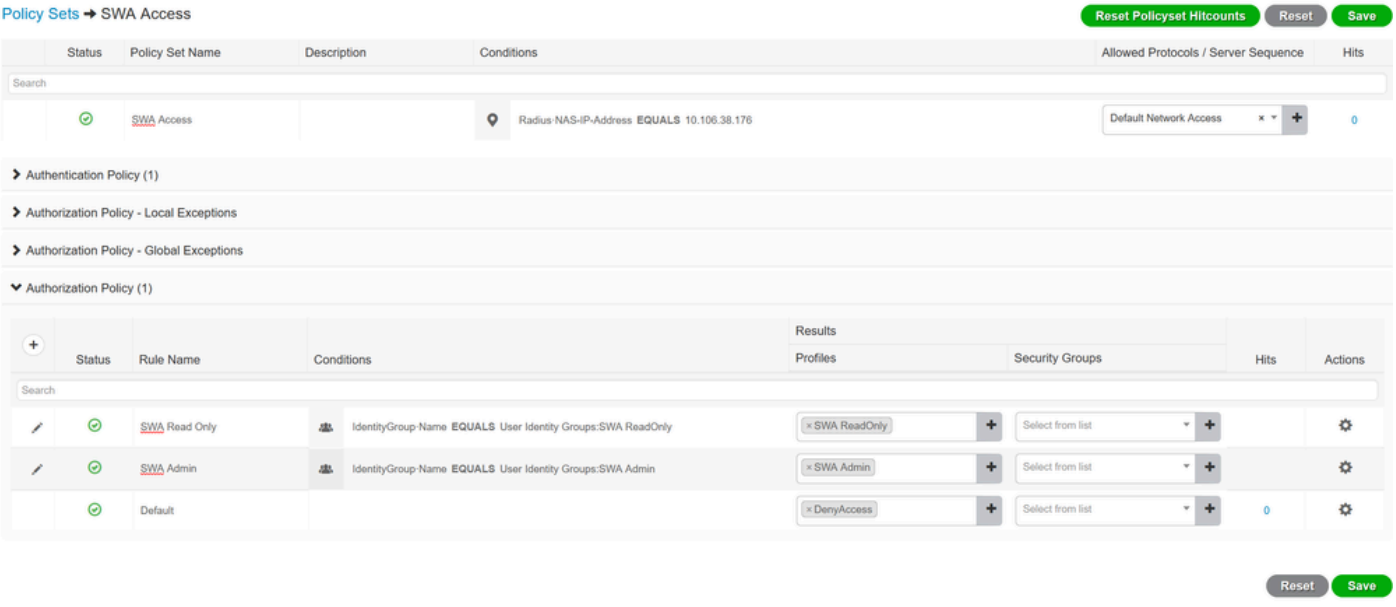
設定名稱。

設定條件以匹配Dictionary Identity Group和Attribute Name Equals User Identity Groups： SWA ReadOnly，然後按一下Use。



選擇只讀使用者組的授權策略

步驟 11. 分別為每個規則設定Authorization Profile，然後按一下Save。

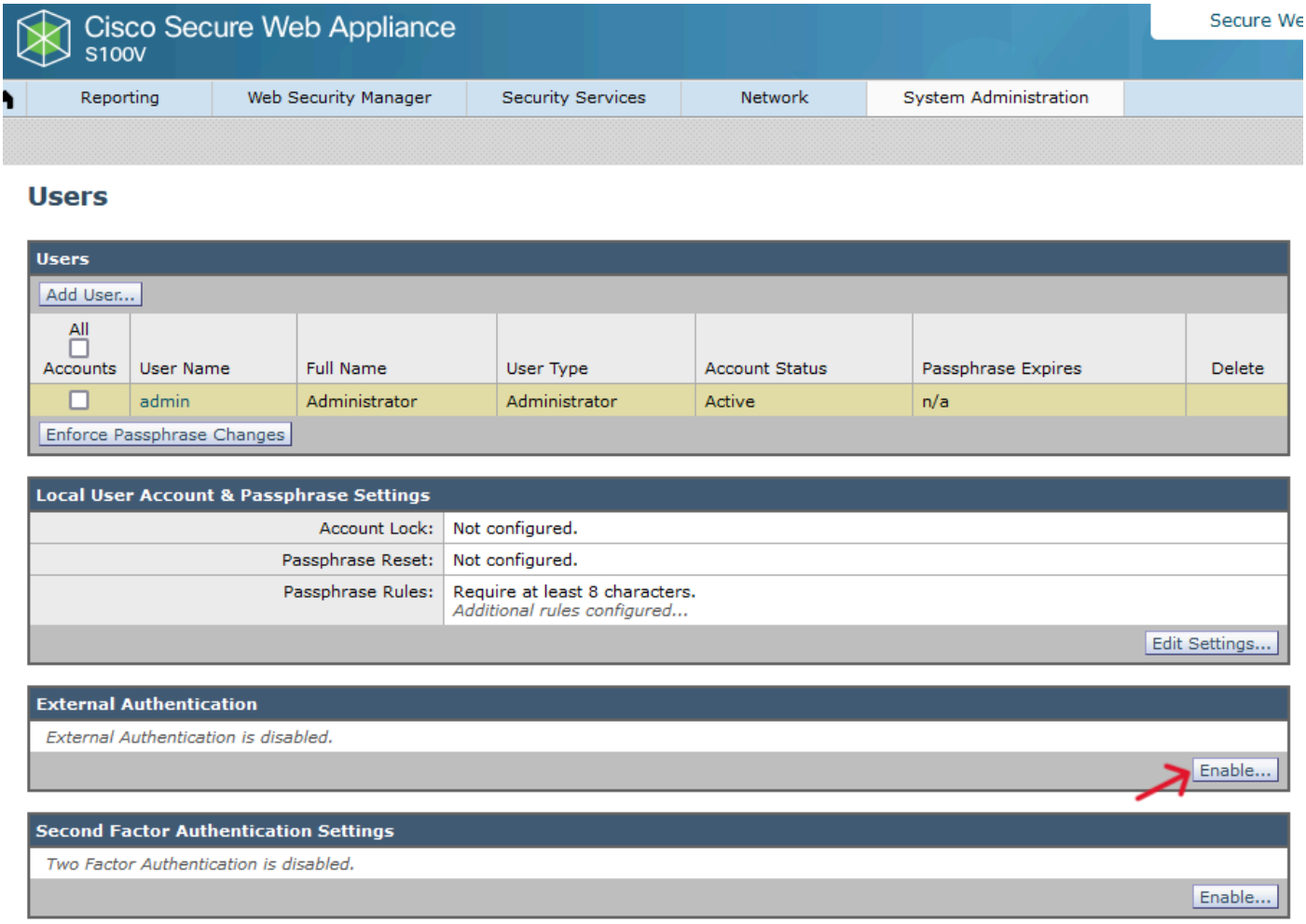


選擇授權配置檔案

SWA配置

步驟 1.從SWA GUI導航至系統管理，然後按一下使用者。

步驟 2.在External Authentication中按一下Enable。



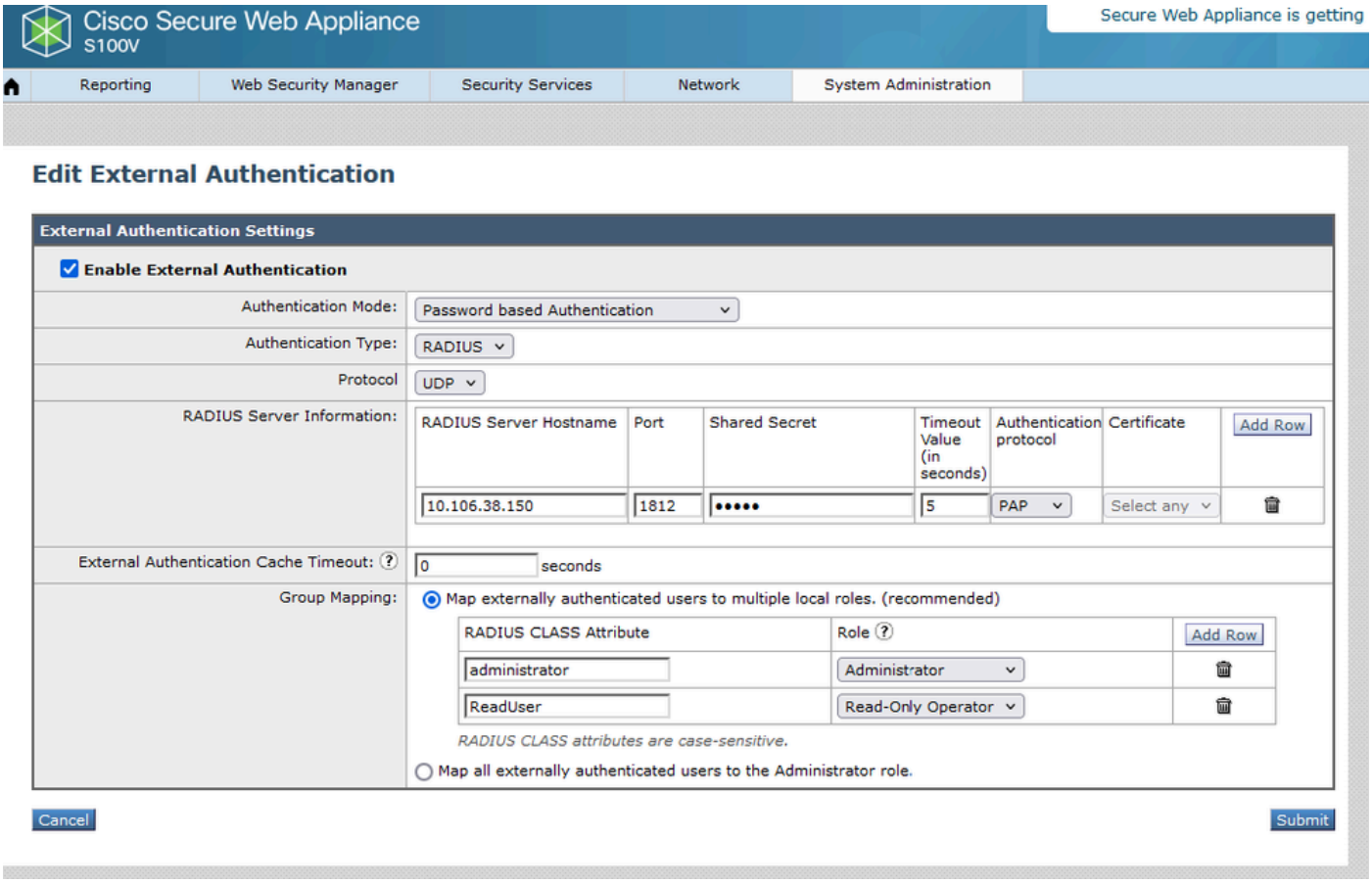
在SWA中啟用外部身份驗證

步驟 3.在RADIUS伺服器主機名欄位中輸入ISE的IP地址或FQDN，並輸入在步驟2 ISE配置中配置的相同共用金鑰。

步驟 4.在Group Mapping中選擇Map external authenticated users to multiple local roles。

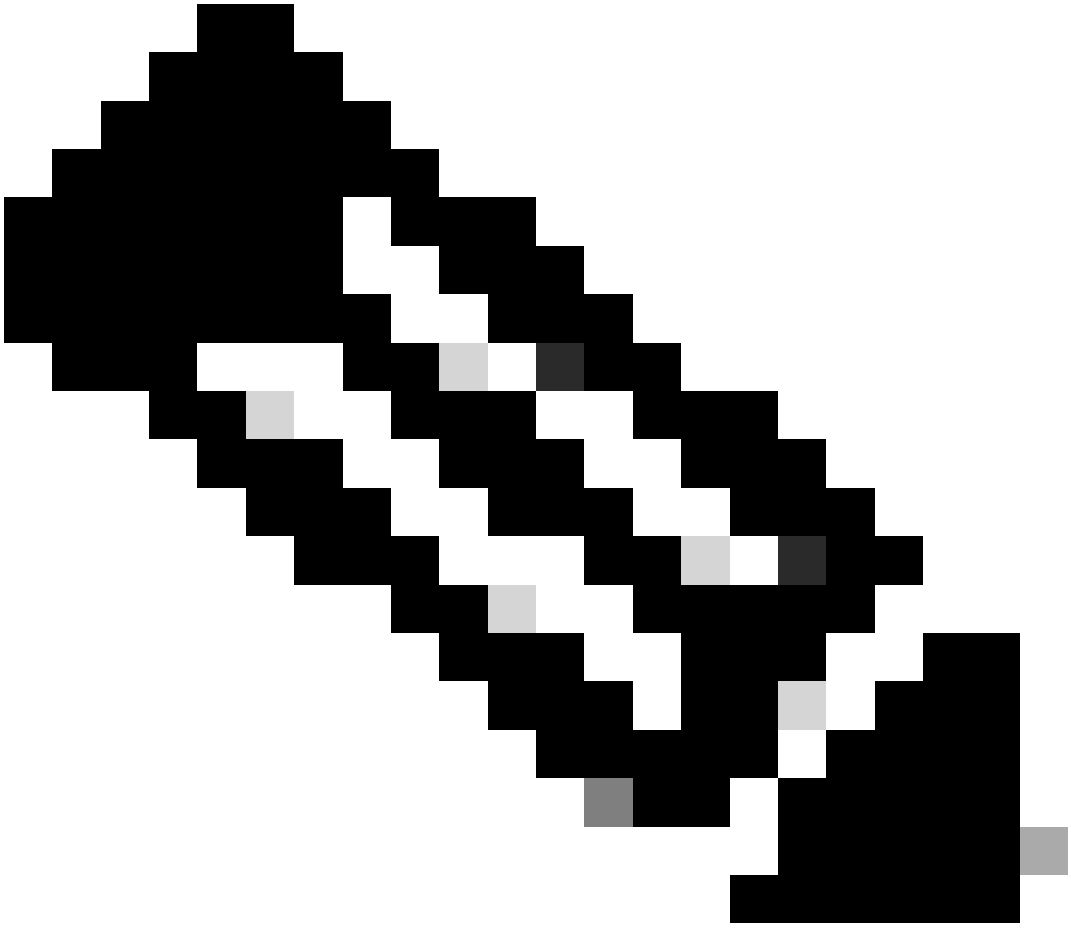
步驟 4.1.在「RADIUS CLASS Attribute」欄位中輸入Administrator，然後選擇Role Administrator。

步驟 4.2.在RADIUS CLASS Attribute欄位中輸入ReadUser並選擇角色只讀運算子。



RADIUS伺服器的外部身份驗證配置

第5步：要在SWA中配置使用者，請點選增加使用者。輸入使用者名稱並選擇所需角色所需的使用者型別。輸入Passphrase和Retype Passphrase，如果裝置無法連線到任何外部RADIUS伺服器，則需要此密碼才能進行GUI訪問。



注意：如果裝置無法連線到任何外部伺服器，它會嘗試將使用者驗證為在Secure Web裝置上定義的本地使用者。

Users

Users

Add User...

* When RADIUS external authentication is enabled, all local user accounts except "admin" are disabled. If all RADIUS services fail, local user accounts will be used for authentication.

All Accounts	User Name	Full Name	User Type*	Account Status	Passphrase Expires	Delete
☐	adminuser	Admin User	*Administrator*	Active	n/a	🗑
☐	rouser	RO User	*Read-Only Operator*	Active	n/a	🗑

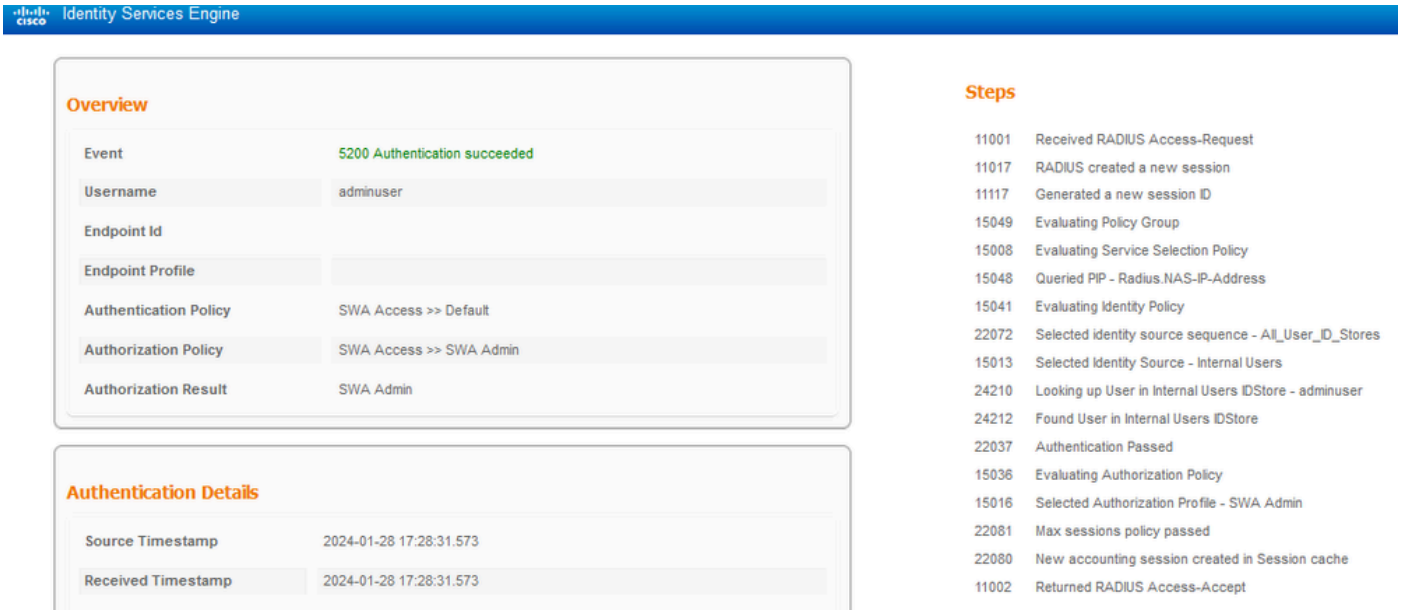
SWA中的使用者配置

第6步：點選提交和提交更改。

驗證

使用配置的使用者憑證訪問SWA GUI，並檢查ISE中的即時日誌。要檢查ISE中的即時日誌，請導航

到操作>即時日誌：



驗證使用者登入ISE

相關資訊

- Cisco Secure Web Appliance AsyncOS 14.0使用手冊
- ISE 3.0管理指南
- 安全Web裝置的ISE相容性清單
- 思科技術支援與下載

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）。