針對ISE 2.x配置Prime 3.1 TACACS身份驗證

目錄

簡介

本文檔介紹如何配置Prime基礎設施以通過ISE 2.x的TACACS進行身份驗證。

需求

思科建議您瞭解以下主題的基本知識：

- 身分識別服務引擎 (ISE)
- Prime基礎架構

設定

Cisco Prime網路控制系統3.1

Cisco Identity Service Engine 2.0或更高版本。

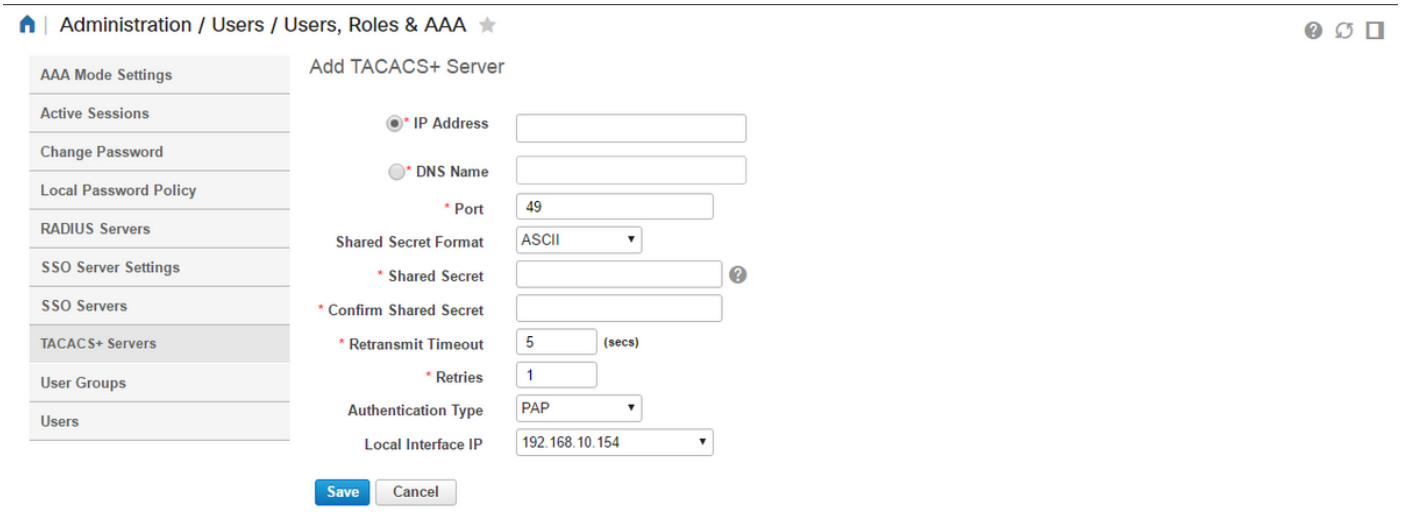
(附註：ISE僅支援從版本2.0開始的TACACS，但是可以將Prime配置為使用Radius。如果您希望將Radius與較舊版本的ISE或第三方解決方案配合使用，Prime除了TACACS還包括Radius屬性清單。)

Prime配置

導航到以下螢幕：管理/使用者/使用者、角色和AAA，如下所示。

在此之後，選擇TACACS+伺服器頁籤，然後選擇右上角的Add TACACS+伺服器選項並選擇go。

在下一個螢幕上，TACACS伺服器條目的配置可用（此操作必須針對每個單獨的TACACS伺服器完成）



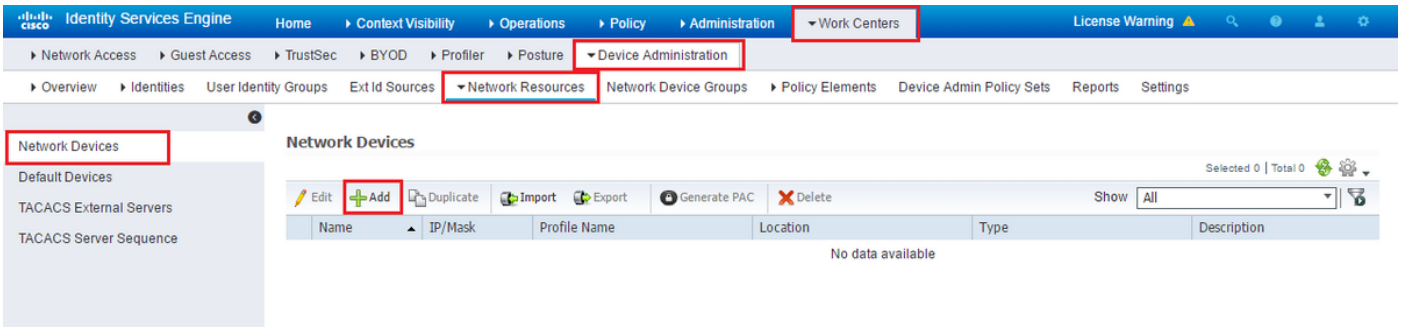
在這裡，您需要輸入伺服器的IP地址或DNS地址以及共用金鑰。另請注意您要使用的本地介面IP，因為稍後需要在ISE中將此相同的IP地址用於AAA客戶端。

以便完成Prime上的配置。您需要在AAA mode settings頁籤下的Administration / Users / Users，Roles & AAA下啟用TACACS。

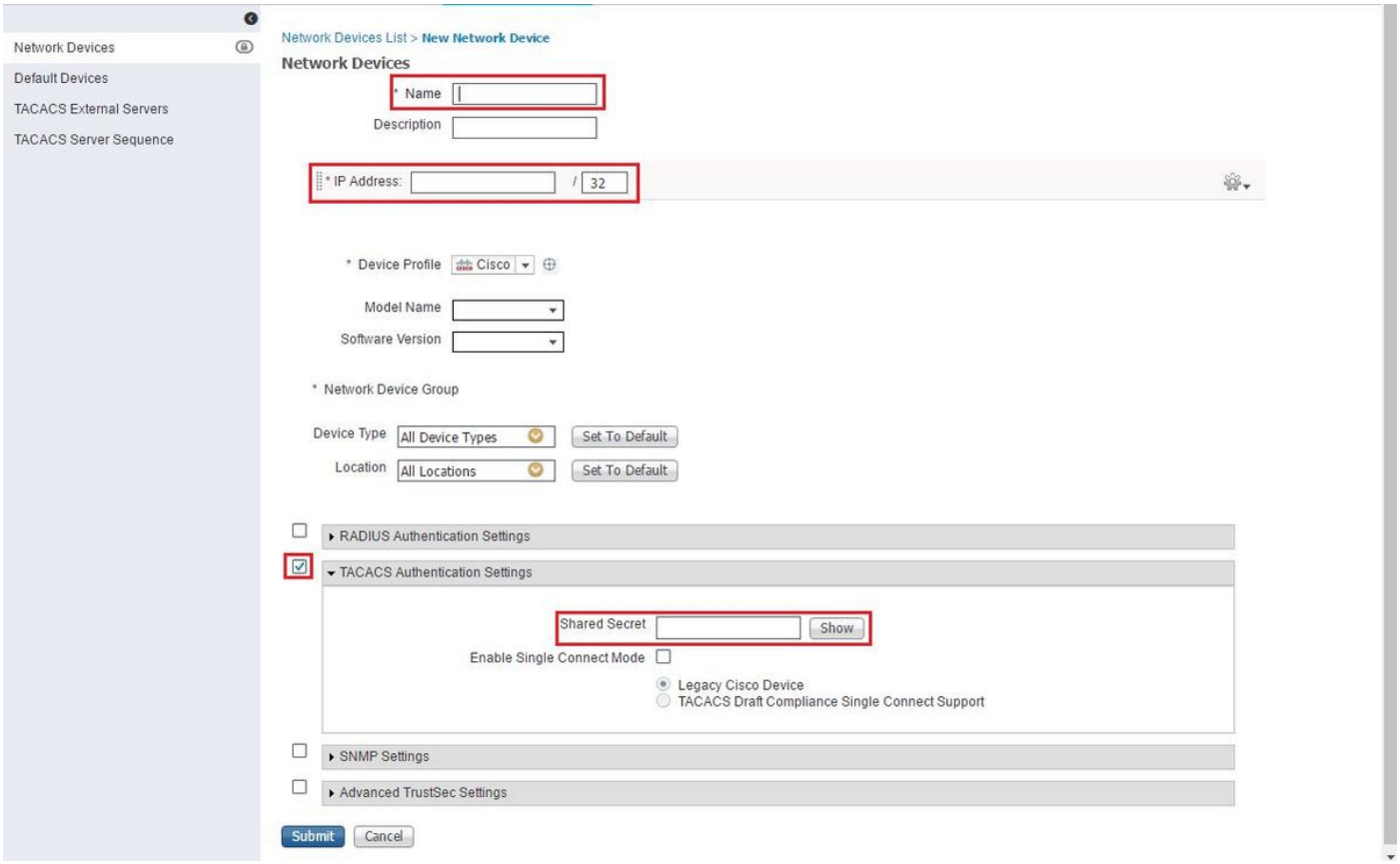
(附註：建議選中Enable fallback to Local選項，該選項包含ONLY on no server response或On no response or failure選項（特別是在測試配置時）

ISE 組態

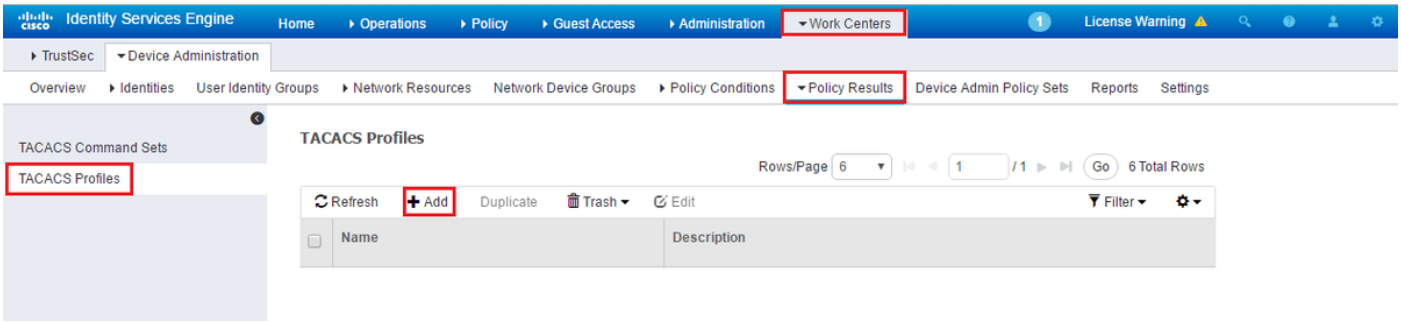
在工作中心/裝置管理/網路資源/網路裝置/新增Prime配置為ISE上的AAA客戶端



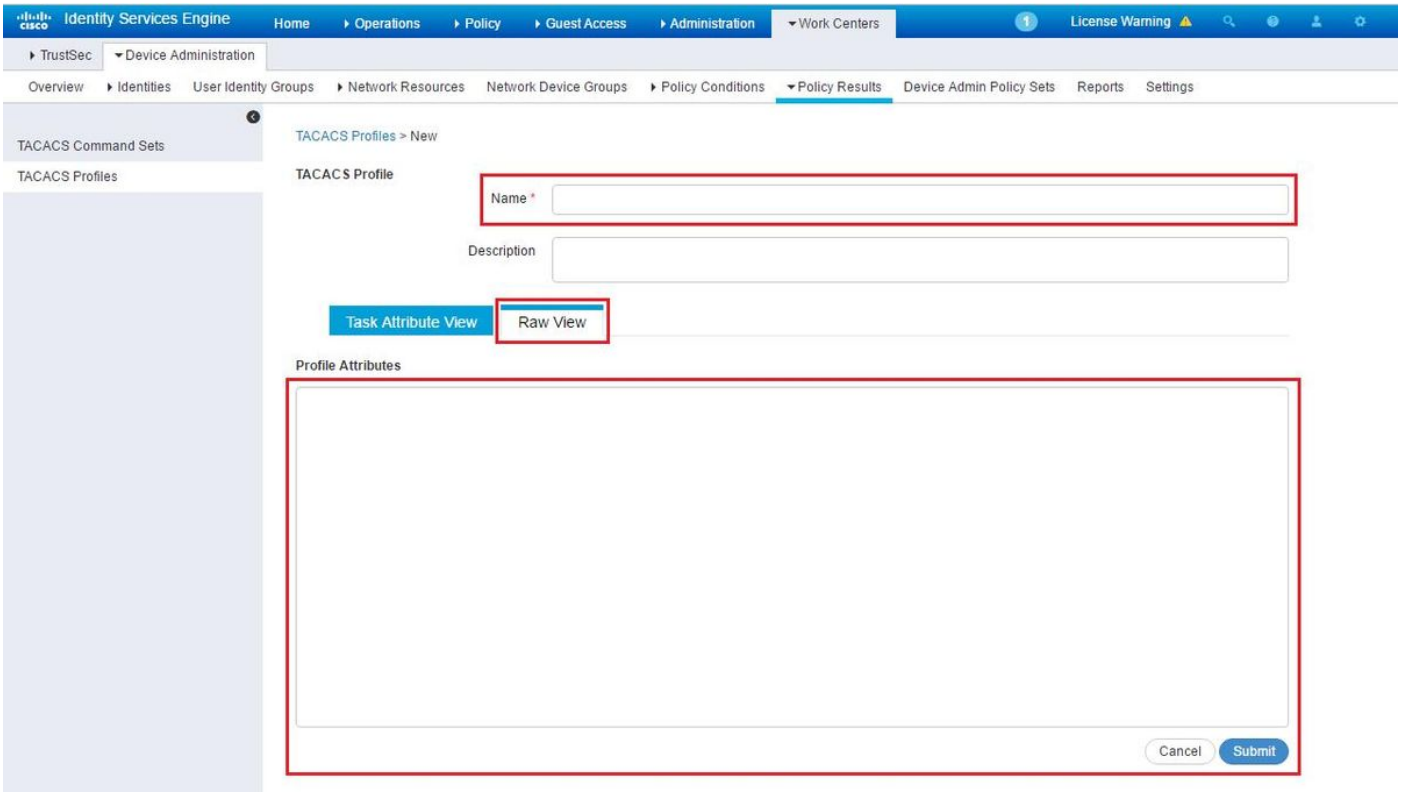
輸入Prime伺服器的資訊。您需要包括的屬性包括Name（名稱）、IP address（IP地址），為TACACS和Shared Secret（共用金鑰）選擇選項。您可能還希望新增裝置型別，特別是為Prime，以便稍後作為授權規則或其他資訊的條件使用，但這是可選的。



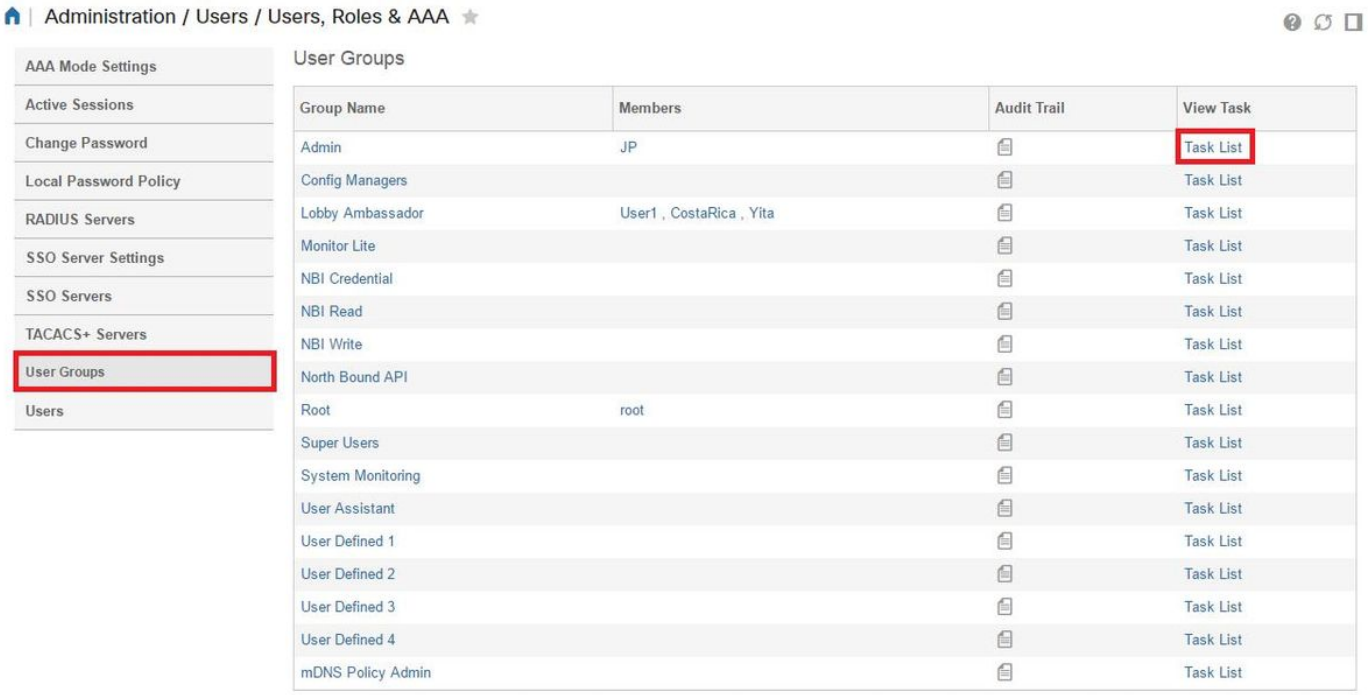
然後建立TACACS配置檔案結果以將所需的屬性從ISE傳送到Prime，以提供正確的訪問級別。導航至Work Centers/Policy Results/Tacacs Profiles並選擇Add選項。



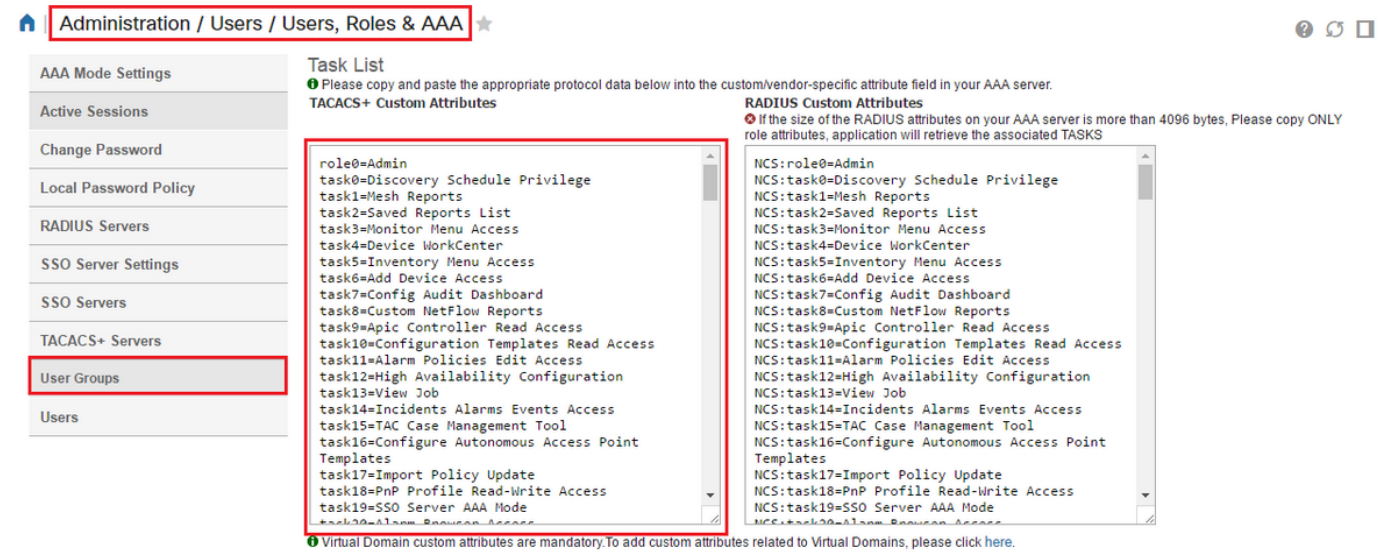
配置名稱，並使用Raw View選項在Profile attributes框中輸入屬性。屬性將來自初級伺服器本身。



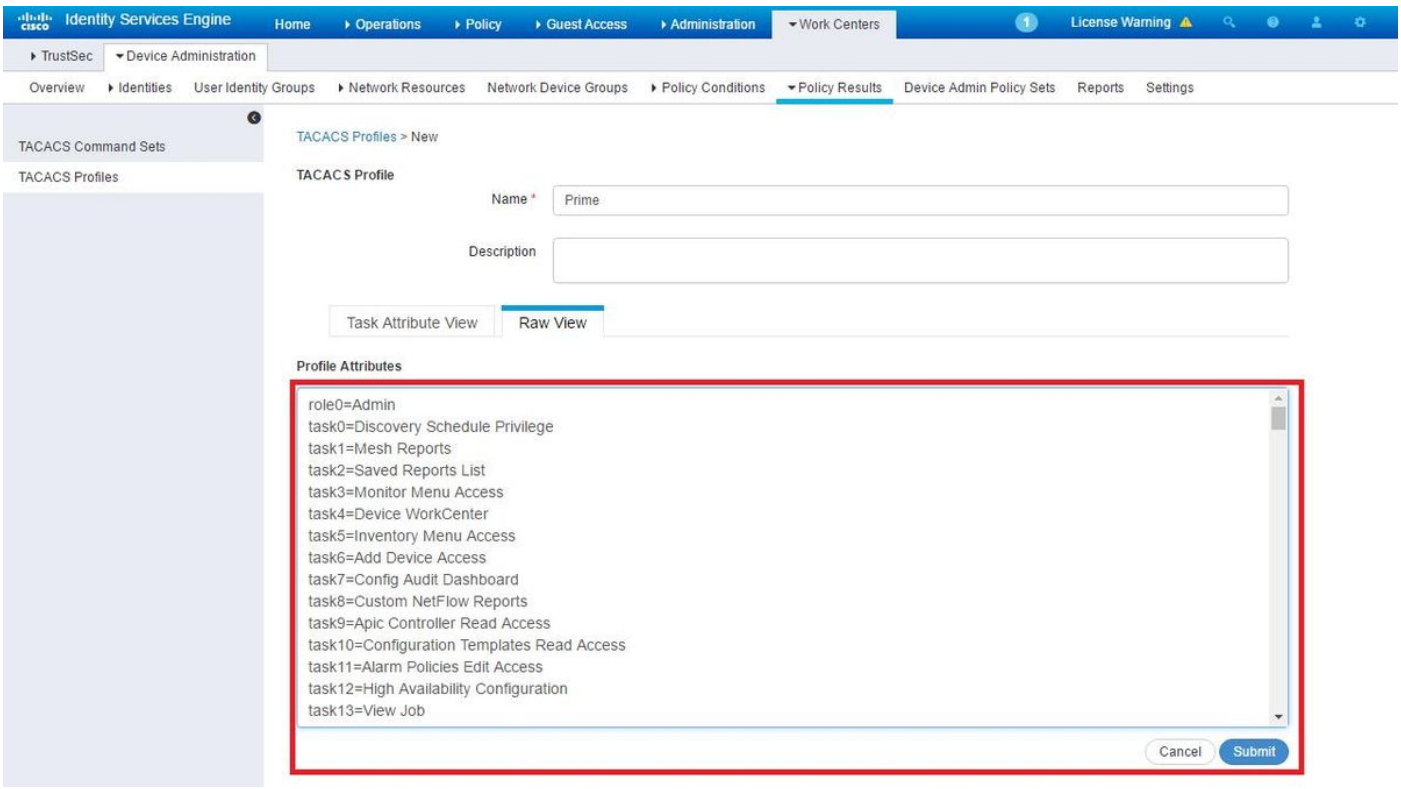
獲取管理/使用者/使用者、角色和AAA螢幕下的屬性，然後選擇使用者組頁籤。在此，您可以選擇要提供的組訪問許可權級別。在本示例中，通過在左側選擇適當的「任務清單」來提供管理員訪問許可權。



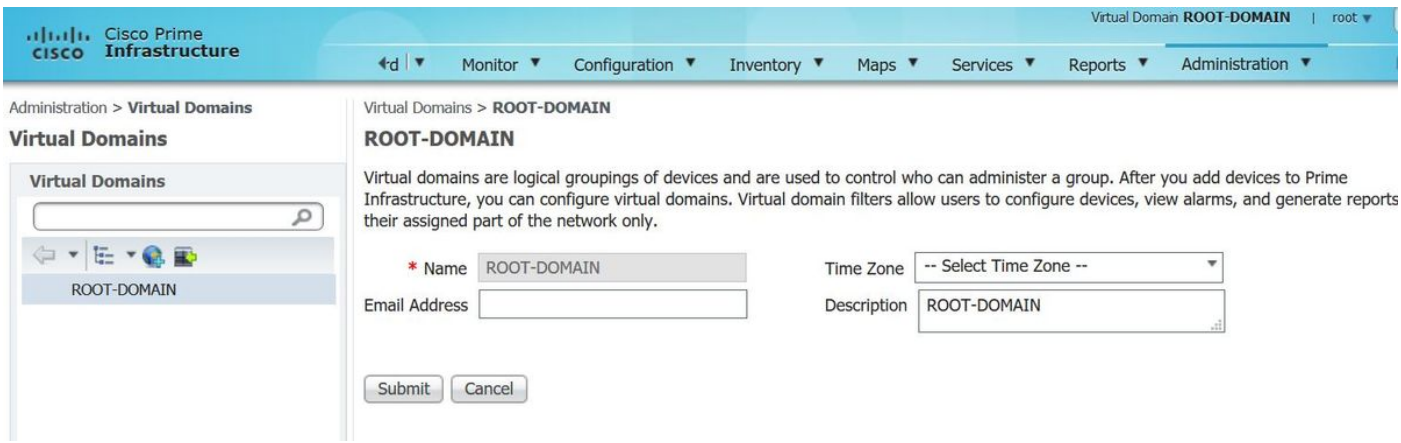
複製所有TACACS自定義屬性。



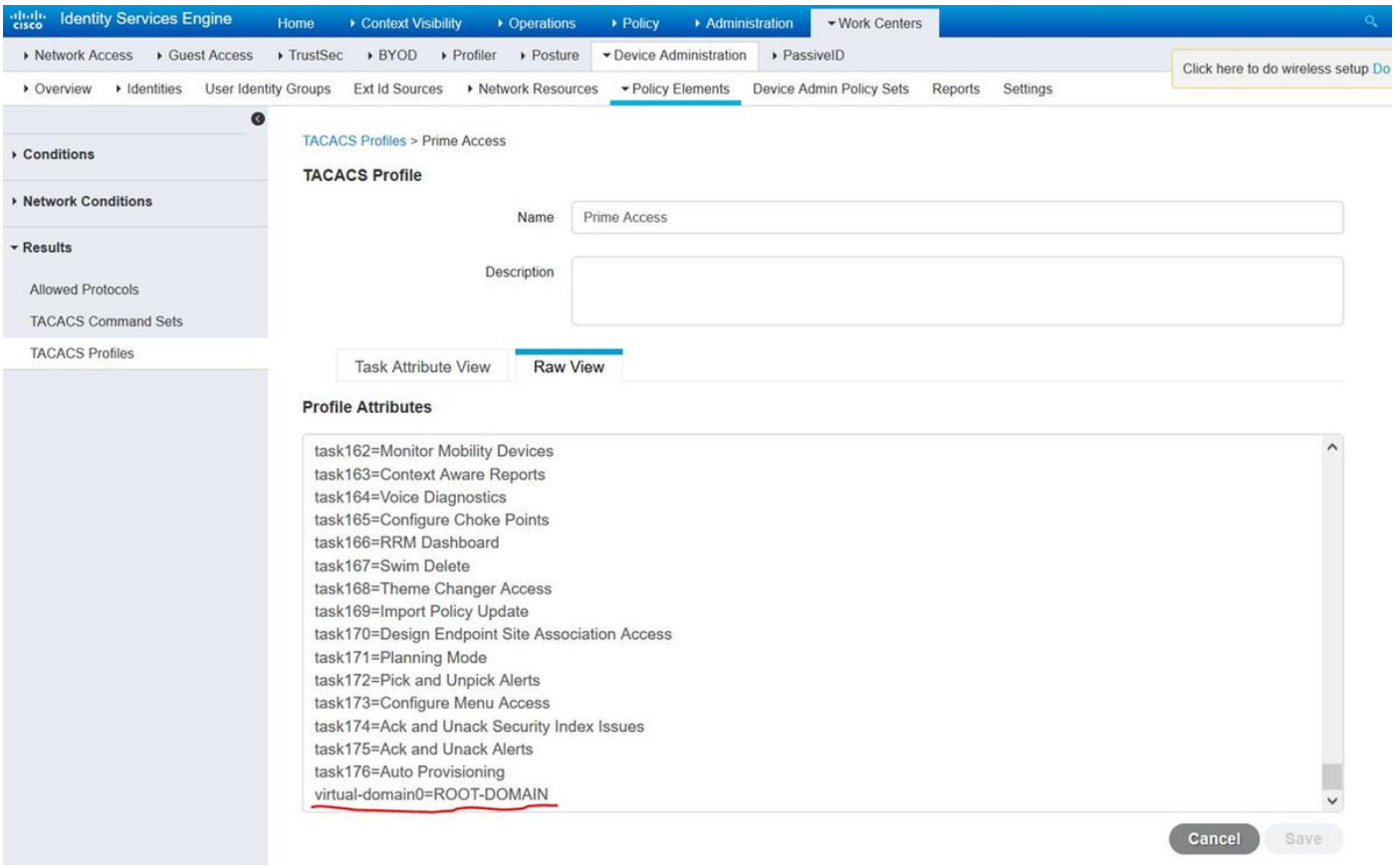
然後將其貼上到ISE上的配置檔案的原始檢視部分。



虛擬域自定義屬性是必需的。根域資訊可在Prime Administration -> Virtual Domains下找到。

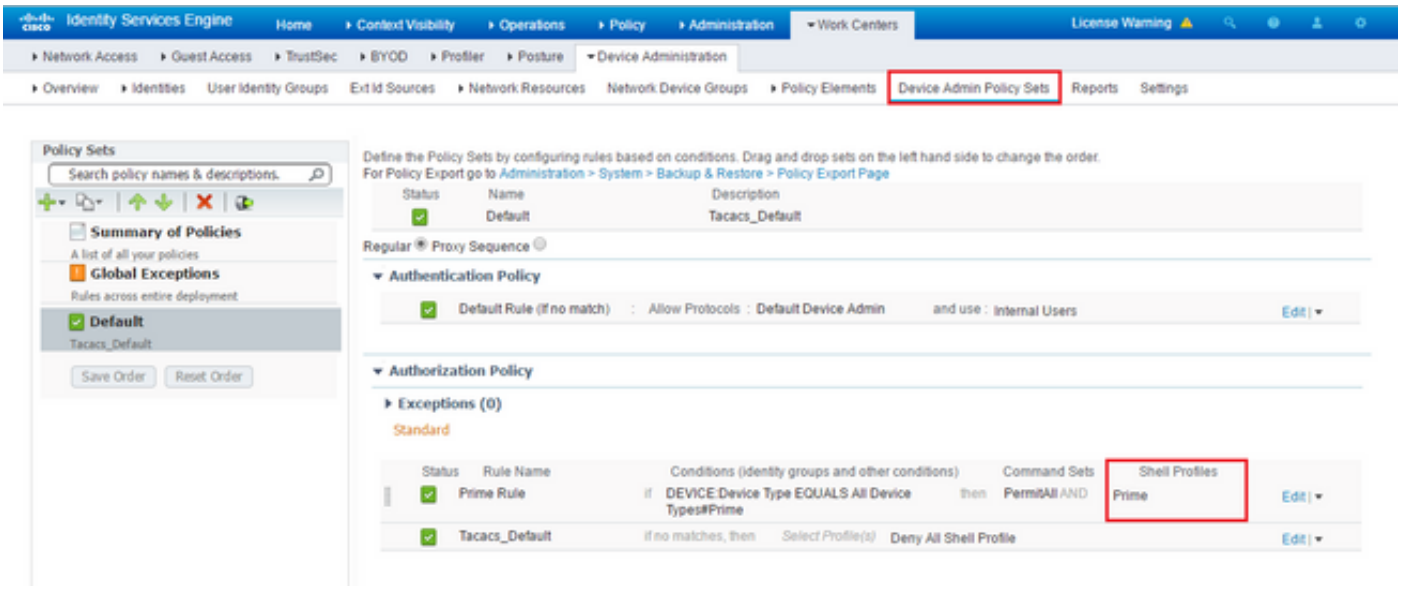


Prime虛擬域名稱必須新增為屬性**virtual-domain0=**"virtual domain name"



完成此操作後，您需要做的只是建立一個規則以分配在上一步中「工作中心/裝置管理/裝置管理策略集」下建立的外殼配置檔案

(附註：「條件」因部署而異，但是您可以將「裝置型別」專門用於Prime或其他型別的過濾器（例如Prime的IP地址）作為「條件」之一，以便此規則可以正確地過濾請求)



此時，配置應該已完成。

疑難排解

如果此配置不成功，並且在Prime上啟用本地回退選項，您可以通過刪除Prime的IP地址強制從ISE進行故障轉移。這將導致ISE不響應並強制使用本地憑證。如果本地回退配置為對拒絕執行，則本地帳戶仍可正常工作並提供對客戶的訪問許可權。

如果ISE顯示成功的身份驗證並且匹配正確的規則，但是Prime仍拒絕請求，您可能需要仔細檢查屬性在配置檔案中是否正確配置，並且沒有傳送其他屬性。