配置FMC域 ；使用者訪問和角色

問題

本文檔介紹如何為跨全域性域和子域的FMC中的多個使用者配置不同的使用者許可權。

環境

- 思科安全防火牆管理中心(FMC)- 7.6.4（適用於所有FMC）
- 具有全域性域和子域的多域部署
- 多個FTD裝置指派給不同的子域
- 多個使用者要求不同的許可權級別

解析

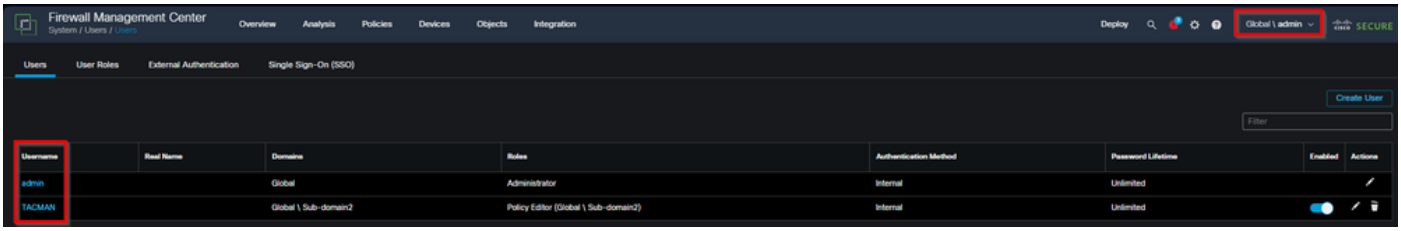
本文檔解決了如何在FMC中跨全域性域和子域為多個使用者配置不同的使用者許可權，從而能夠限制域之間的訪問並限制特定使用者的全域性域訪問。Cisco FMC支援跨多個域的精細使用者角色分配，並能夠限制域之間的訪問。配置涉及在特定域中建立使用者，並分配適當的角色來控制訪問級別。

建立使用者和域訪問行為

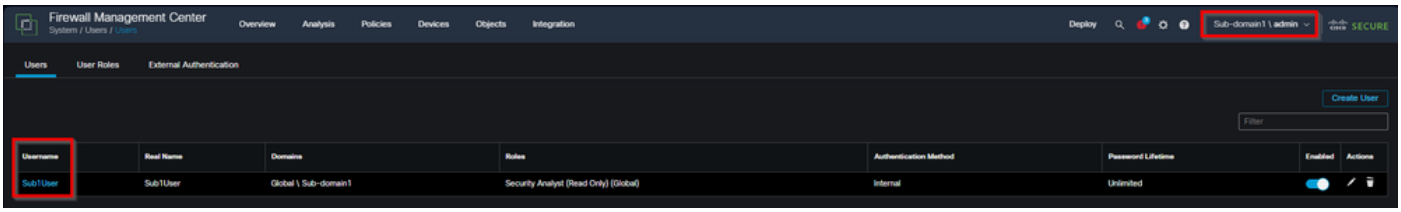
FMC使用者管理系統根據使用者的建立位置以不同的方式運行：

在子域中建立的使用者

- 在子域中直接建立的使用者僅在特定域中可見：

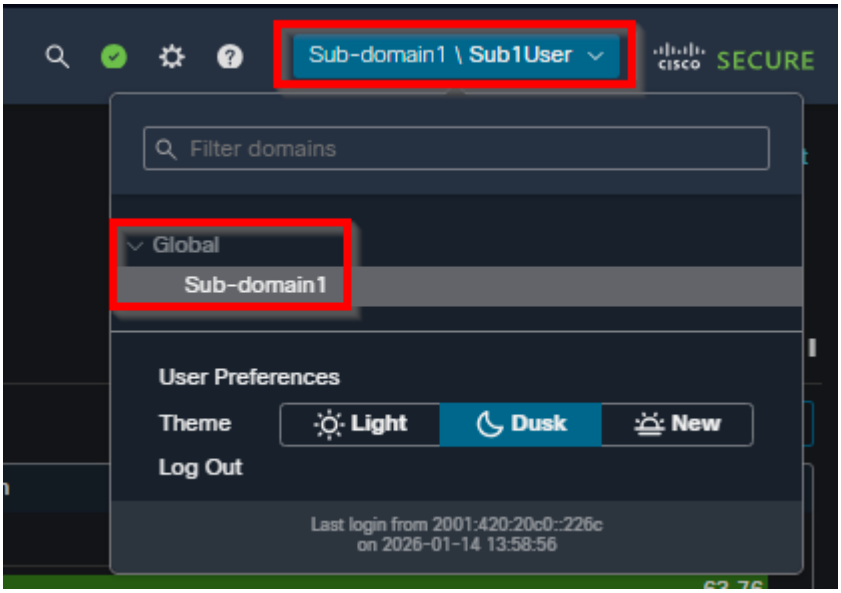


inline_image_0.png



inline_image_1.png

- 這些使用者必須使用域規範格式subdomain\username登入。
- 訪問自動限制到建立使用者的域：

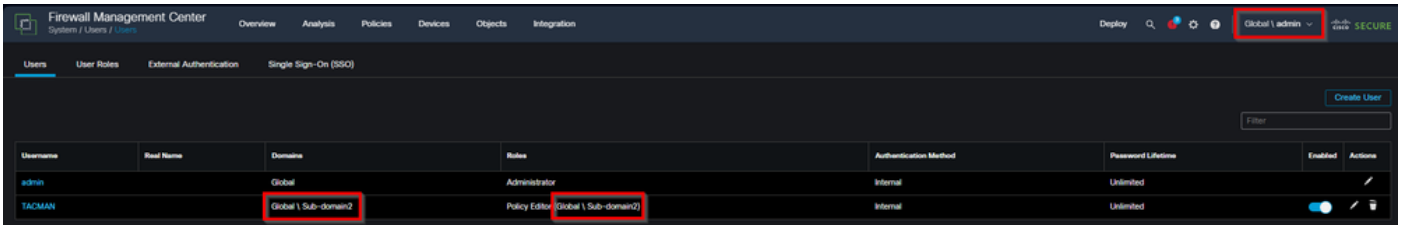


inline_image_2.png

- 在子域中建立的自定義角色僅應用於該域。

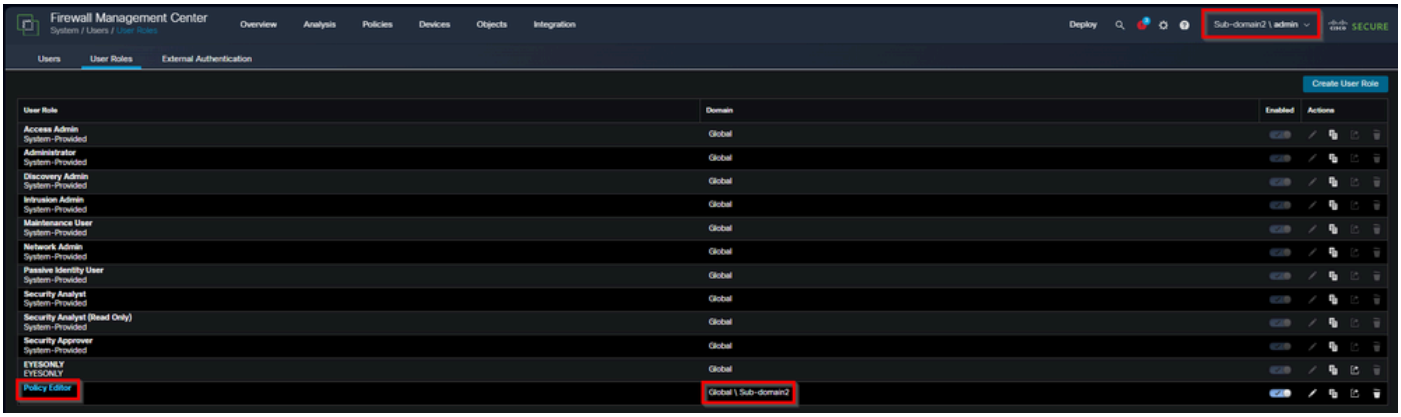
在全域性域中建立的使用者：

- 從全域性域建立的使用者僅可使用其使用者名稱登入，即使其角色僅在子域中也是如此。
- 這些使用者在「全域性域使用者」清單中仍然可見：



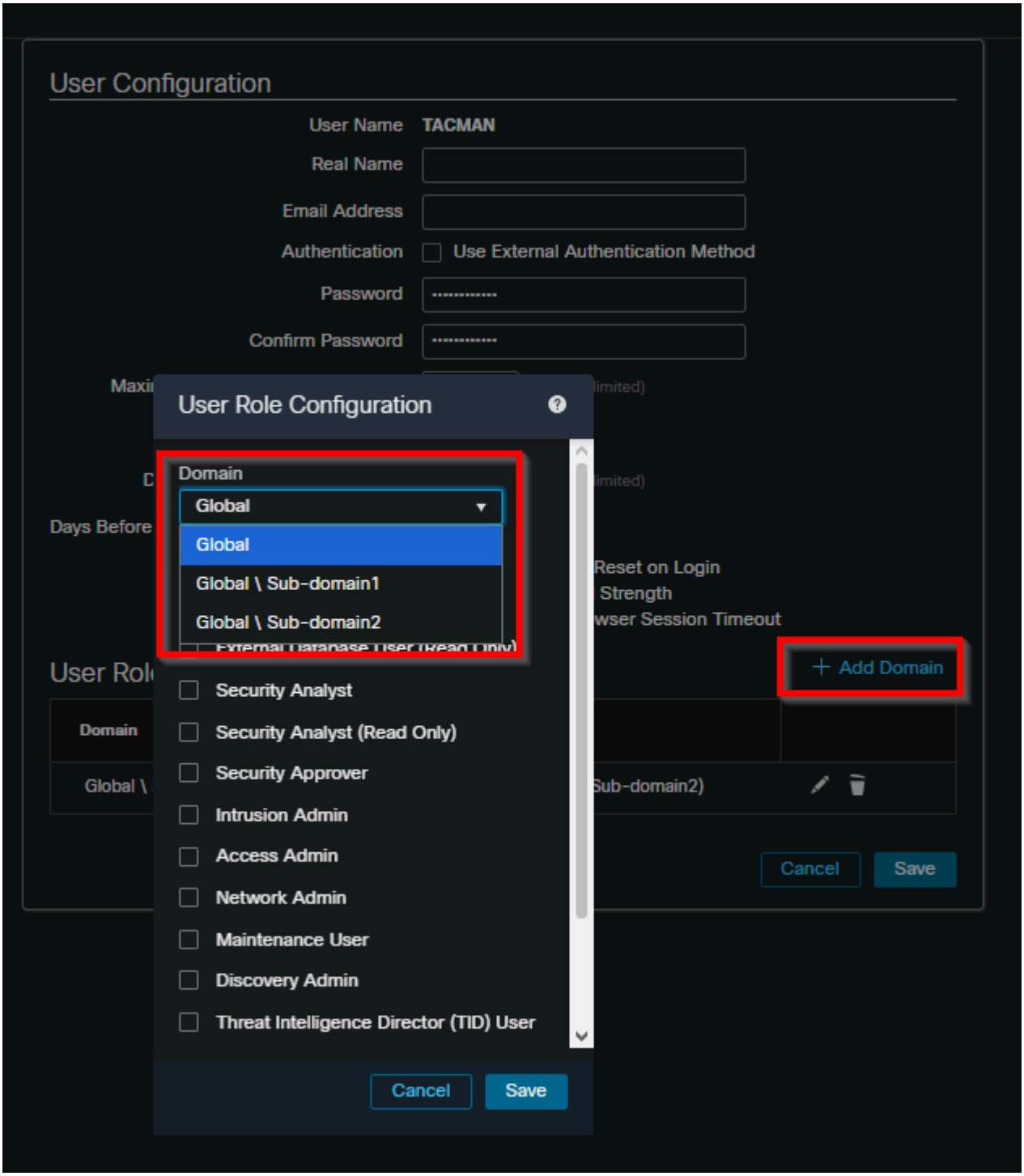
inline_image_3.png

- 可以為任何後代域分配角色：



inline_image_4.png

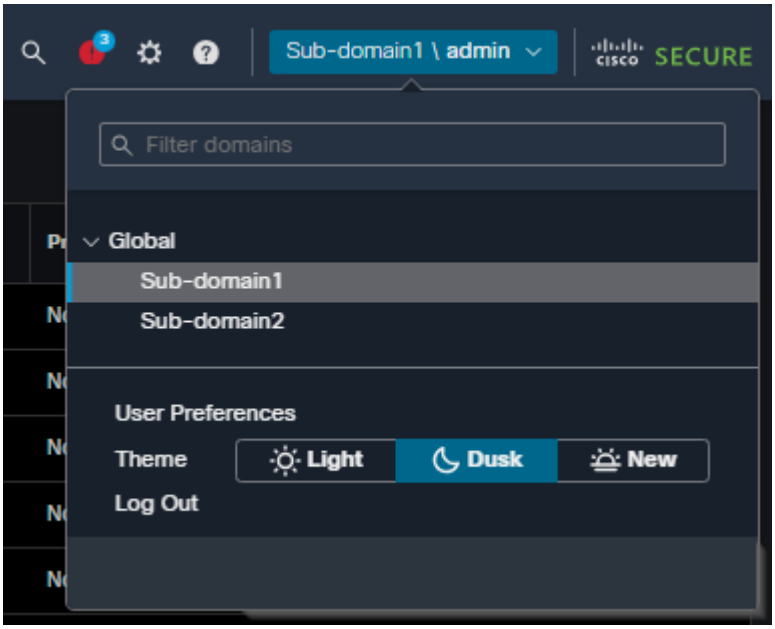
- 可以通過角色分配限制對特定子域的訪問：



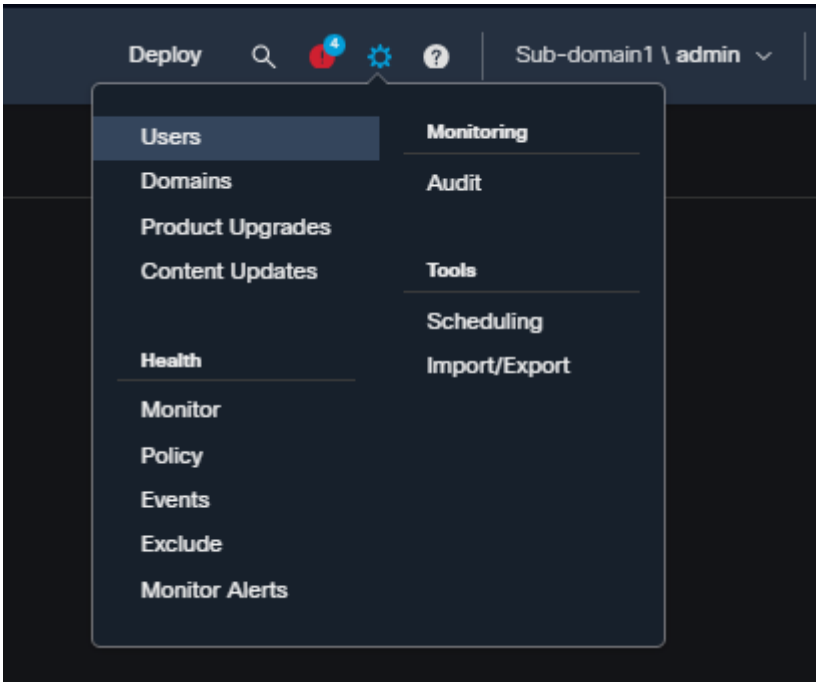
inline_image_5.png

子域使用者限制的配置步驟

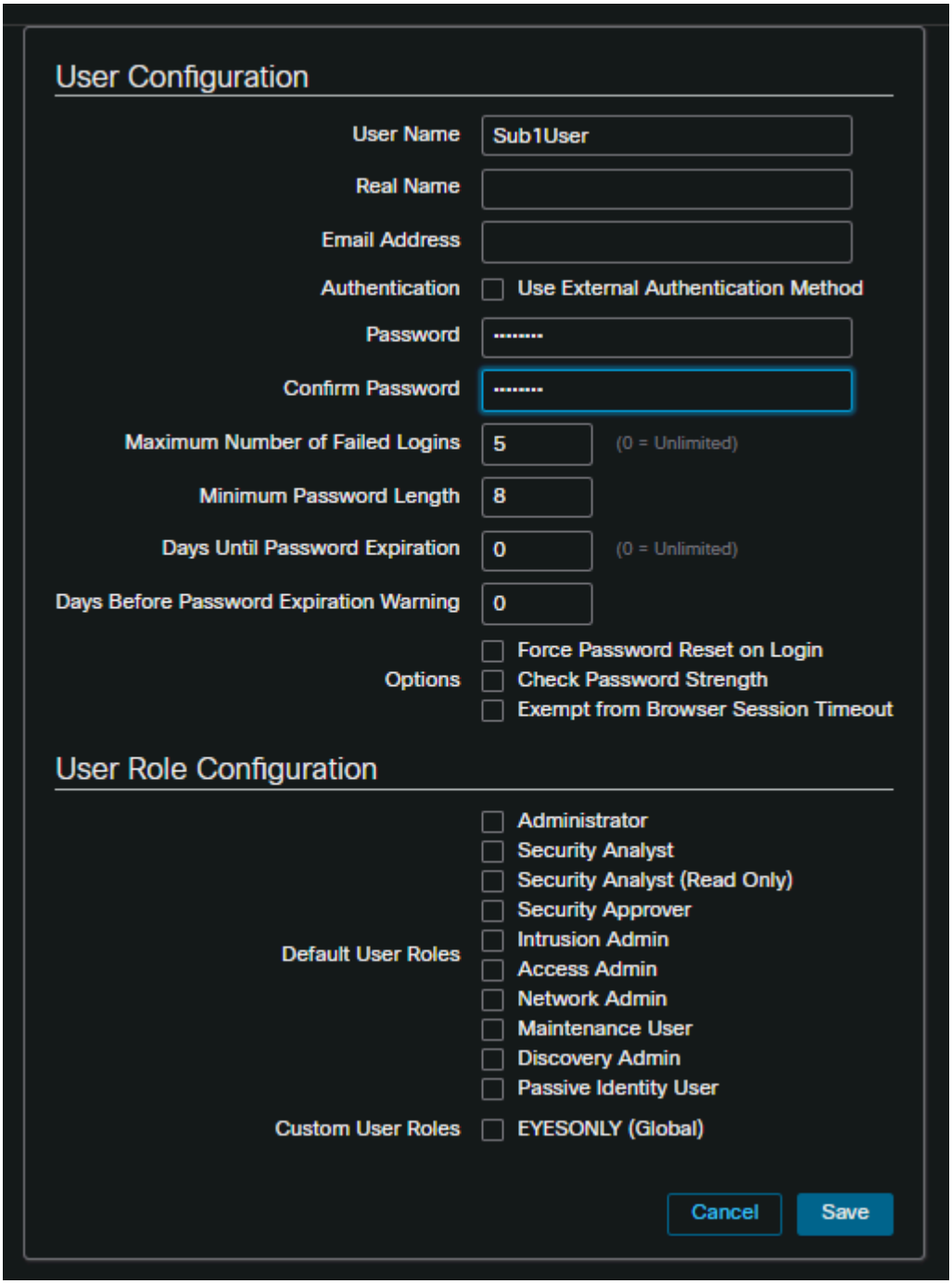
- 導航到必須限制訪問的特定子域，然後在系統/使用者下建立使用者帳戶。



inline_image_6.png

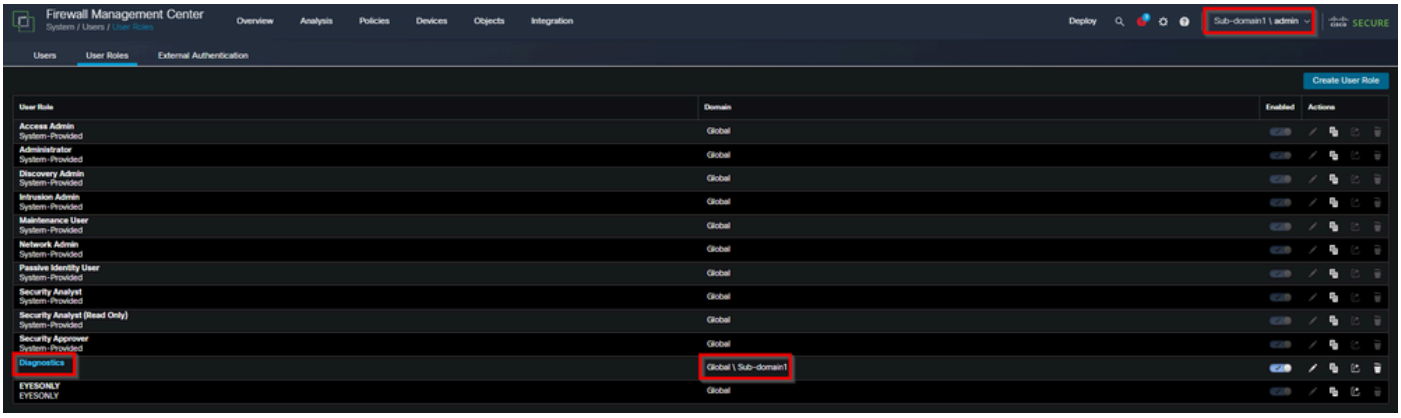


inline_image_7.png



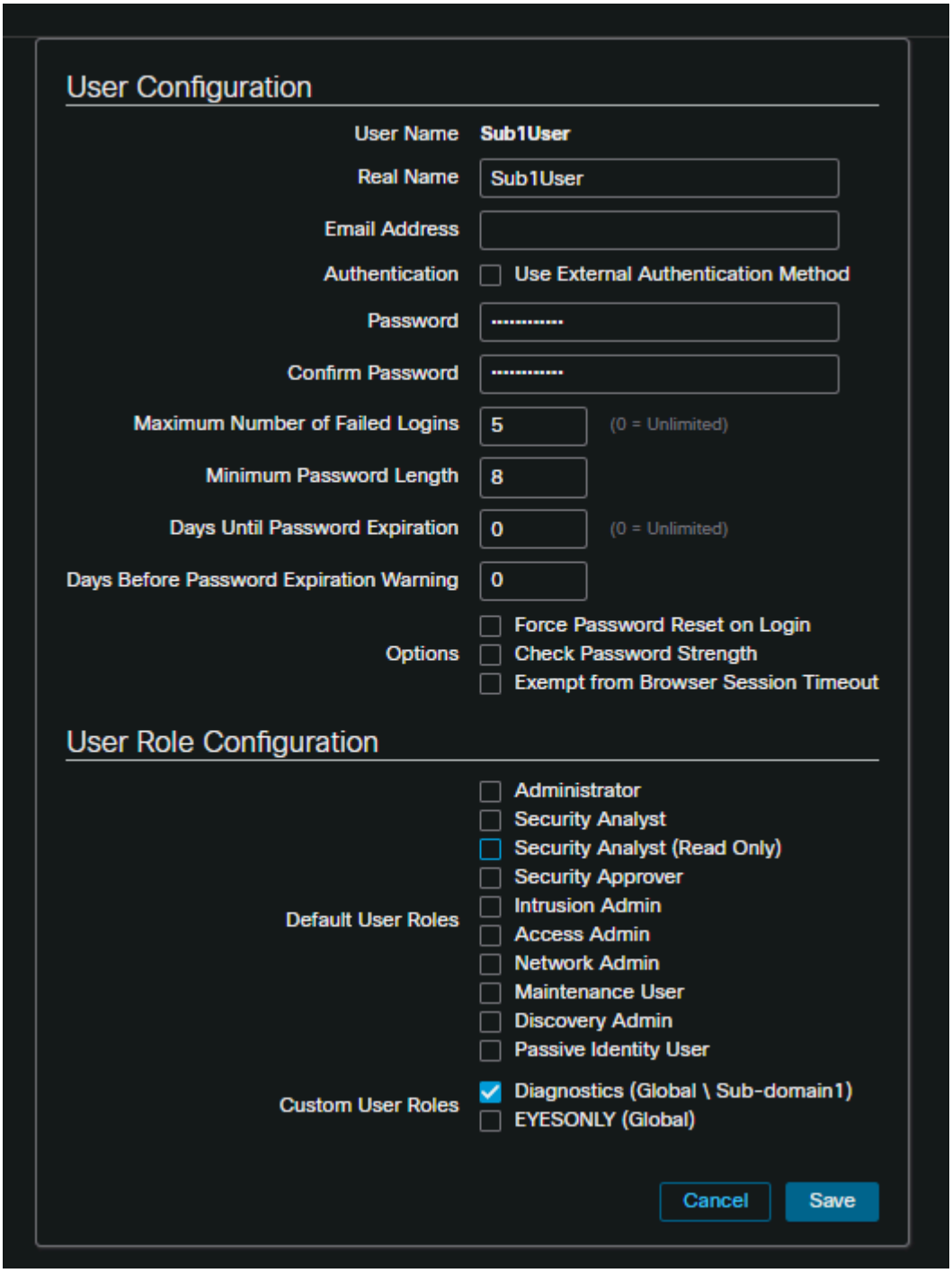
inline_image_8.png

- 在系統/使用者角色下的子域中建立自定義角色。在子域中建立的自定義使用者角色僅在該域中可用，無法從其他域訪問。



inline_image_9.png

- 將自定義角色分配給使用者。使用者僅繼承建立使用者和角色的域的許可權。



inline_image_10.png

- 子域使用者的使用者登入格式。在子域中建立的使用者必須使用以下登入格式：

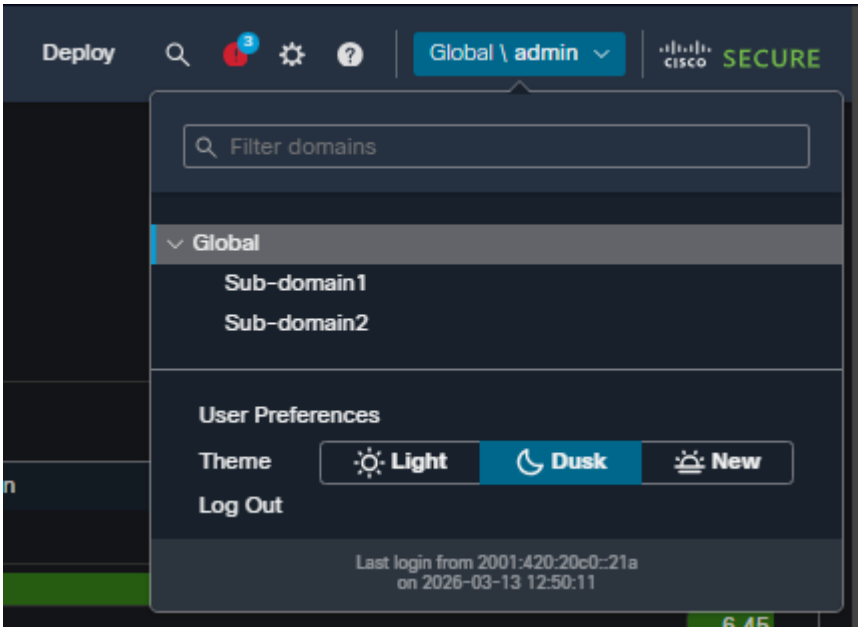
使用者名稱：子域\使用者名稱

密碼：［使用者密碼］

inline_image_11.png

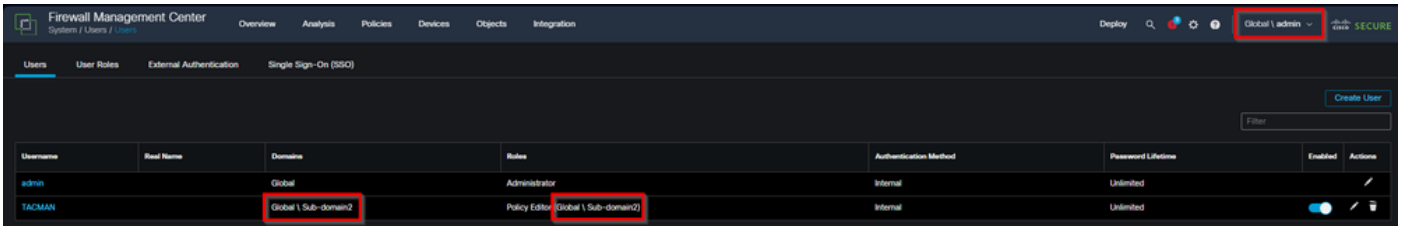
具有子域限制的全域性域使用者的配置步驟

- 在「系統/使用者」下的全域性域中建立使用者。使用具有全域性域訪問許可權的管理帳戶來建立使用者。

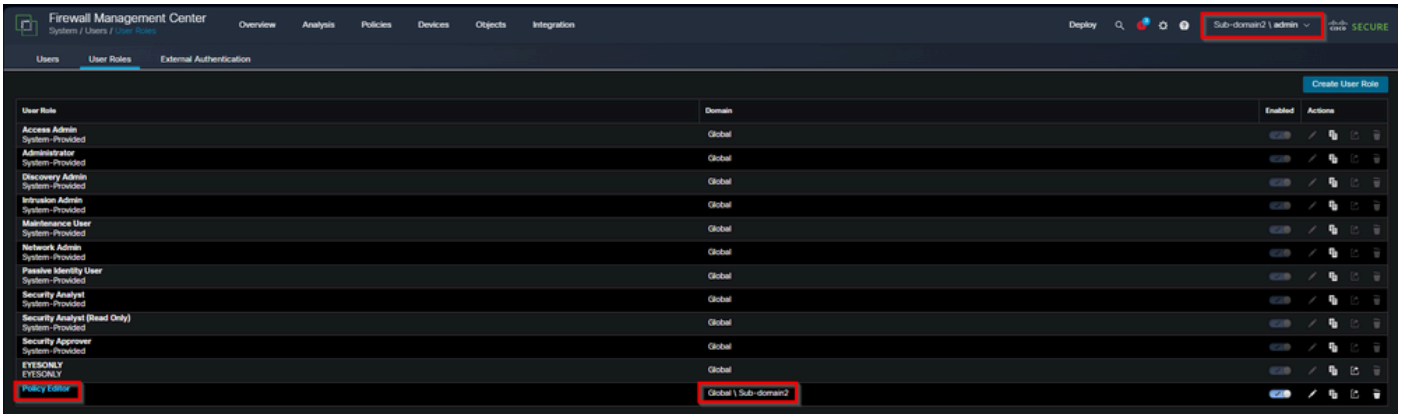


inline_image_12.png

- 僅為「系統/使用者」下的特定子域分配角色。在使用者配置中，只為目標子域分配角色，而不提供任何全域性域許可權。



inline_image_3.png



inline_image_14.png

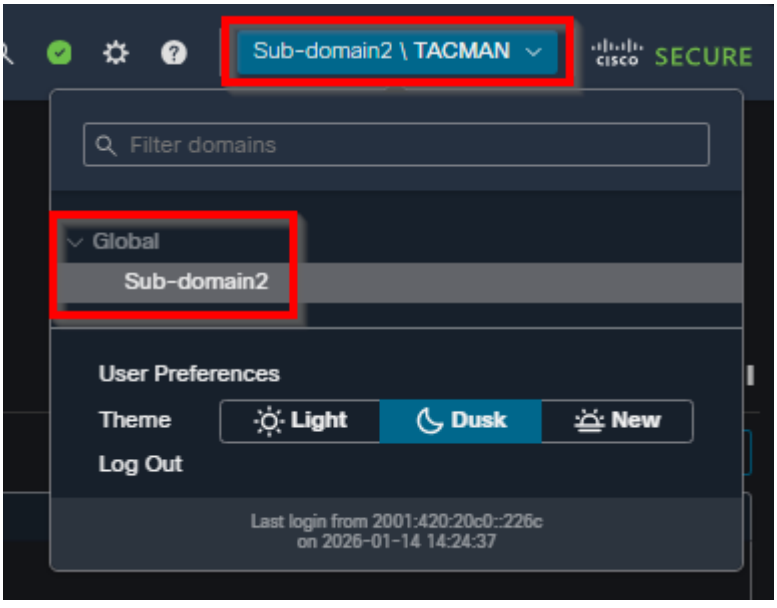
- 這些使用者只能使用其使用者名稱登入，無需指定域：

使用者名稱：使用者名稱

密碼：［使用者密碼］

inline_image_15.png

- 使用者只能訪問專門分配了角色的子域，不能訪問全域性域或其他子域。



inline_image_16.png

角色分配靈活性

使用者在每個域中可以具有不同的許可權：

- 全域性域中的只讀許可權和子域中的管理員許可權
- 在特定子域中沒有具有完全管理員許可權的全域性域訪問
- 一個子域中的策略編輯器許可權，無法訪問其他子域

外部使用者注意事項

對於外部使用者（LDAP或RADIUS身份驗證）：

- 如果通過組成員資格或使用者屬性分配使用者角色，則無法刪除最低訪問許可權。
- 可以為其他許可權分配比預設使用者角色更大的範圍。
- 外部身份驗證對象僅在建立它們的域中可用。
- 為了進行適當的限制，必須在比預設使用者角色更大的範圍內配置單個使用者許可權。

限制和注意事項

- 無法從後代域編輯在祖先域中建立的自定義使用者角色。
- 外殼身份驗證僅在全域性域中可用，在子域中不可用。
- 使用者首選項和儀表板設定適用於帳戶具有訪問許可權的所有域。
- 使用者的許可權修改是單獨配置的，而不是分組或批次配置的。

原因

這一要求源於在多域FMC部署中實施精細訪問控制的需要，在這些部署中，使用者需要對全域性域和子域的不同級別的訪問，並在域之間設定特定限制以維護安全邊界。

相關內容

- 思科安全防火牆管理中心管理指南7.6:使用者
- 思科安全防火牆管理中心管理指南7.6:建立自定義使用者角色
- 思科安全防火牆管理中心管理指南7.6:新增或編輯內部使用者
- 思科安全防火牆管理中心管理指南7.6:使用者和域
- 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）。