在安全終端控制檯中配置二元身份驗證

目錄

簡介

本文檔介紹帳戶的型別以及在思科安全終端控制檯中配置雙因素身份驗證的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- 安全端點
- 對安全終端控制檯的訪問

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 安全終端控制檯5.4.20211013

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

存取控制

安全終端控制檯中有兩種型別的帳戶：管理員和非特權帳戶或普通帳戶。建立新使用者名稱時，您必須選擇其許可權級別，但您可以隨時更改其訪問級別。

管理員擁有完全控制許可權，可以檢視組織中任何組或電腦的資料，並對組、策略、清單和使用者名稱進行更改。

附註：管理員可以將其他管理員降級為常規帳戶，但不能將自己降級。

無許可權或普通使用者帳戶只能檢視他們有權訪問的組的資訊。建立新使用者帳戶時，您可以選擇是否授予其管理員許可權。如果不授予他們這些許可權，您可以選擇他們有權訪問的組、策略和清單。

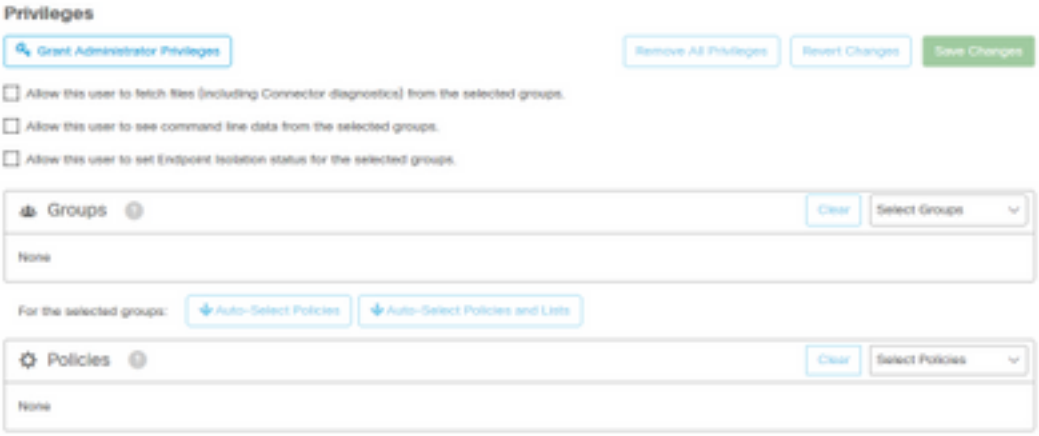
雙因素身份驗證

雙因素身份驗證針對未經授權嘗試訪問您的安全終端控制檯帳戶提供了額外的安全層。

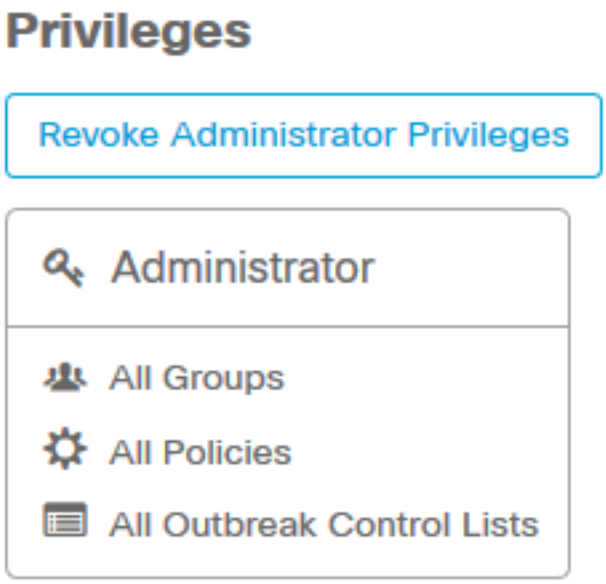
設定

許可權

如果您是管理員，要更改許可權或授予管理員許可權，可以導航到「帳戶」>「使用者」，選擇使用者帳戶並選擇許可權，請參見下圖。



管理員還可以將管理員許可權撤消給其他管理員，為此，您可以導航到管理員帳戶以檢視選項，如下圖所示。

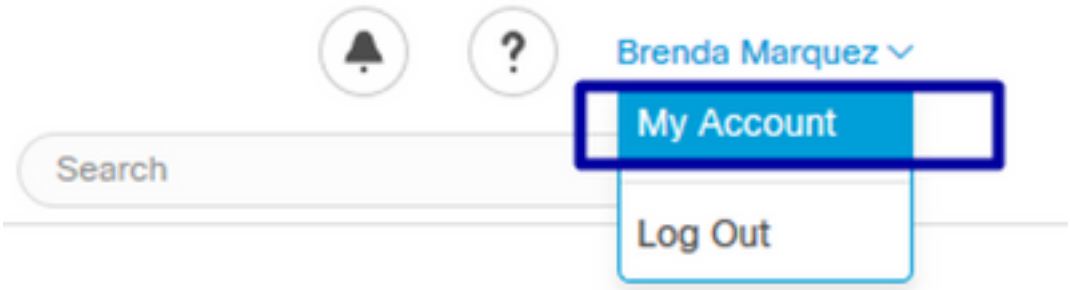


附註：當使用者許可權更改時，某些資料將在搜尋結果中快取，這樣，即使使用者不再具有訪問組的許可權，該使用者仍可以在一段時間內檢視資料。大多數情況下，快取記憶體會在5分鐘後刷新。

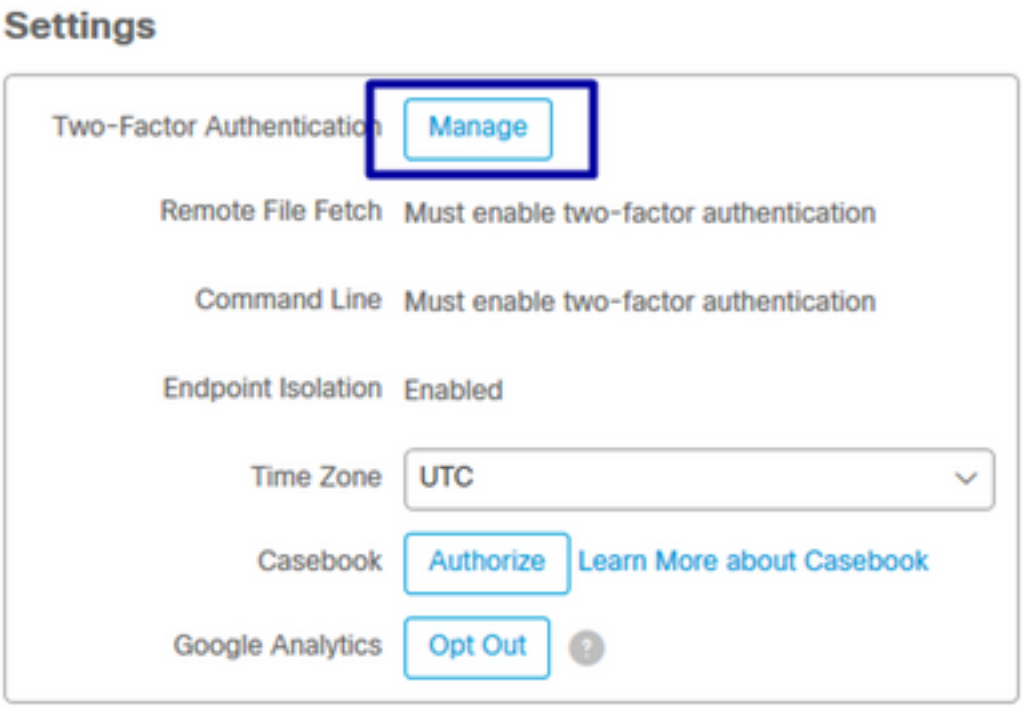
雙因素身份驗證

此功能允許您對外部訪問請求實施身份驗證。若要設定此程式，請依照以下程式操作：

步驟1.導覽至Secure Endpoint Console右上角的My Account，如下圖所示。

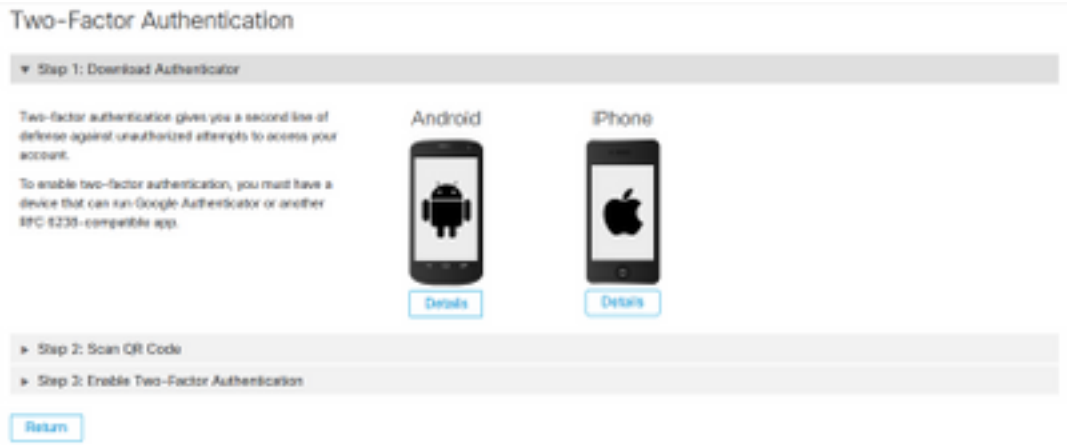


步驟2.在「設定」部分中選擇「管理」，以便看到包含啟用此功能所需的三個步驟的簡單指南，如下圖所示。

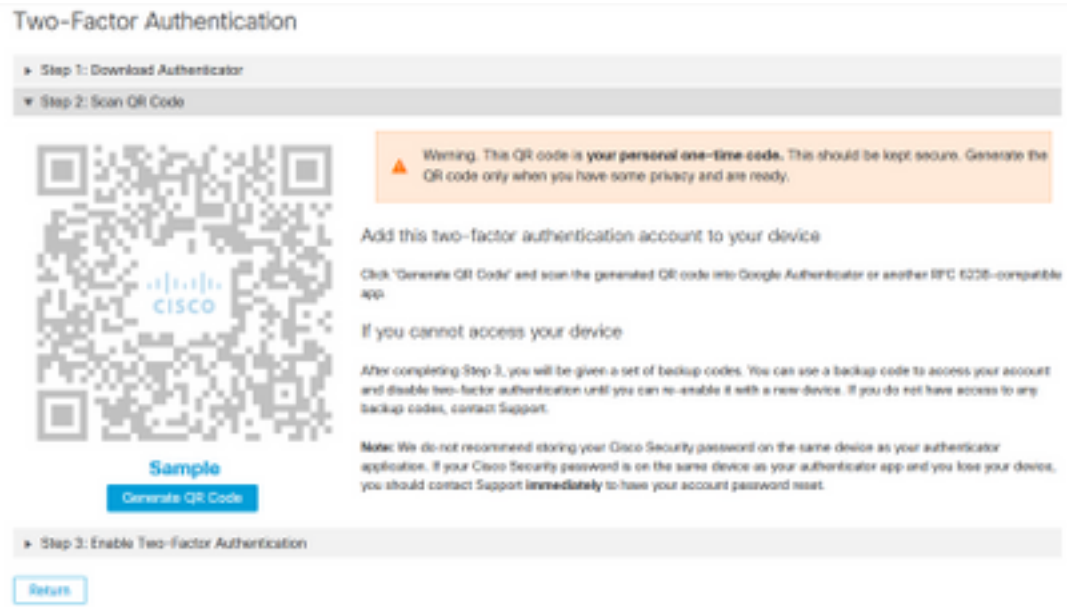


步驟3.共有三個快速步驟：

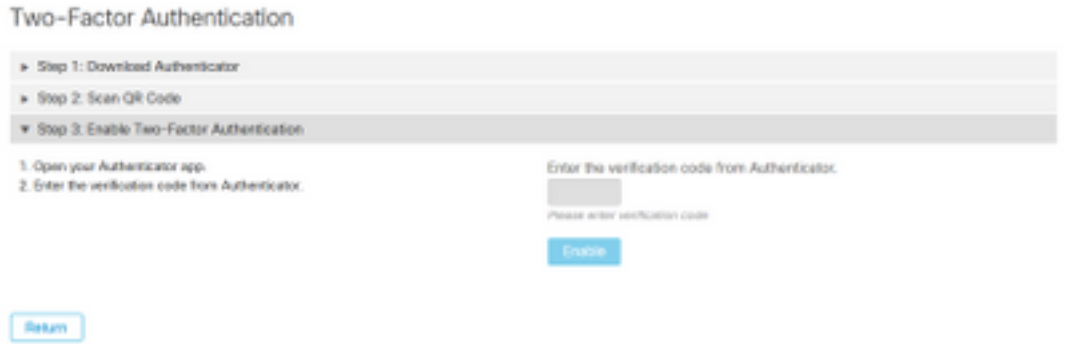
a)下載身份驗證器，您可以從Android或iPhone獲得可以運行Google身份驗證器的身份驗證器。選擇任一手機上的詳細資訊生成一個QR代碼，該代碼會將您重定向到下載頁面。請參見此圖。



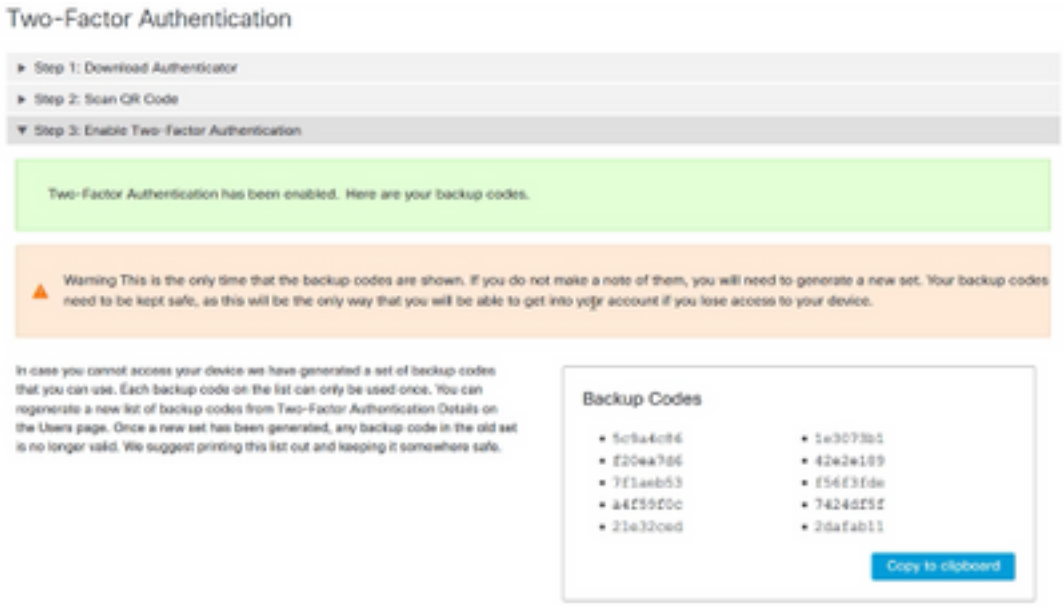
b)掃描QR碼，選擇生成QR碼，Google Authenticator必須對其進行掃描，如下圖所示。



c)啟用雙因素身份驗證器，在手機上開啟身份驗證器應用程式並輸入驗證代碼。選擇「啟用」以完成此過程，如下圖所示。



步驟4。完成後，它會為您提供一些備份代碼。選擇「複製到剪貼簿」以儲存它們，請參閱影象作為示例。



附註：每個備份代碼只能使用一次。使用完所有備份代碼後，您必須返回此頁才能生成新代碼。

有關進一步參考，請參閱安全端點使用手冊。

此外，您還可以觀看Accounts and Enable Two-Factor Authentication視頻。