# 如何為FMC REST API互動生成身份驗證令牌

## 簡介

本文檔介紹應用程式程式設計介面(API)管理員如何向Firepower管理中心(FMC)進行身份驗證、生成令牌並將其用於任何進一步的API互動。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- Firepower管理中心(FMC)功能和配置。(配置指南)
- 瞭解各種REST API呼叫。(什麼是REST API?)
- 檢視FMC API快速入門手冊。

### 採用元件

- 支援REST API（6.1版或更高版本）並啟用REST API的Firepower管理中心。
- REST客戶端，如Postman、Python指令碼、CURL等。

## 背景資訊

REST API日益流行，因為網路管理員可以使用輕量級的可程式設計方法配置和管理其網路。FMC支援使用任何REST客戶端以及使用內建API資源管理器的配置和管理。

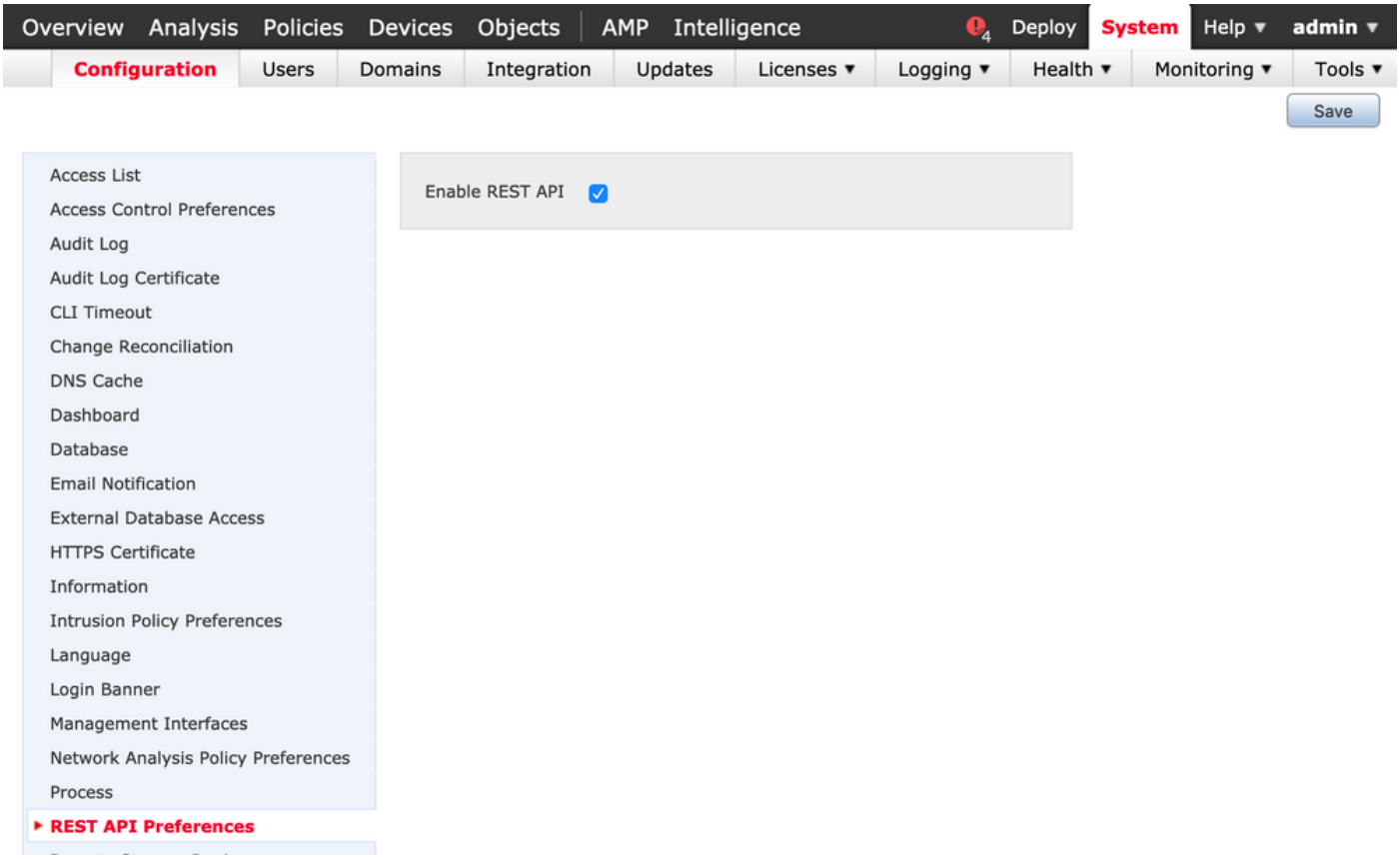
## 設定

### 在FMC上啟用REST API

**步驟1**.導覽至**System>Configuration>REST API Preferences>**Enable **REST API。**

**步驟2.**選中**Enable REST API復**選框。

**步驟3**.按一下**Save，**啟用**REST API時，會顯示**Save Successful**對話方塊，如下圖所示：**




## 在FMC上建立使用者

在FMC上使用API基礎架構的最佳做法是將UI使用者和指令碼使用者分隔開來。請參閱FMC使用者帳戶指南以瞭解各種使用者角色和建立新使用者的准則。

## 請求身份驗證令牌的步驟

**步驟1.**開啟您的**REST API客戶端**。

**步驟2.**將客戶端設定為執行POST命令
，URL:https://<management_center_IP_or_name>/api/fmc_platform/v1/auth/generatetoken。

**步驟3.**將使用者名稱和密碼作為基本身份驗證標頭。**POST**主體應為空。

例如，使用Python的身份驗證請求：

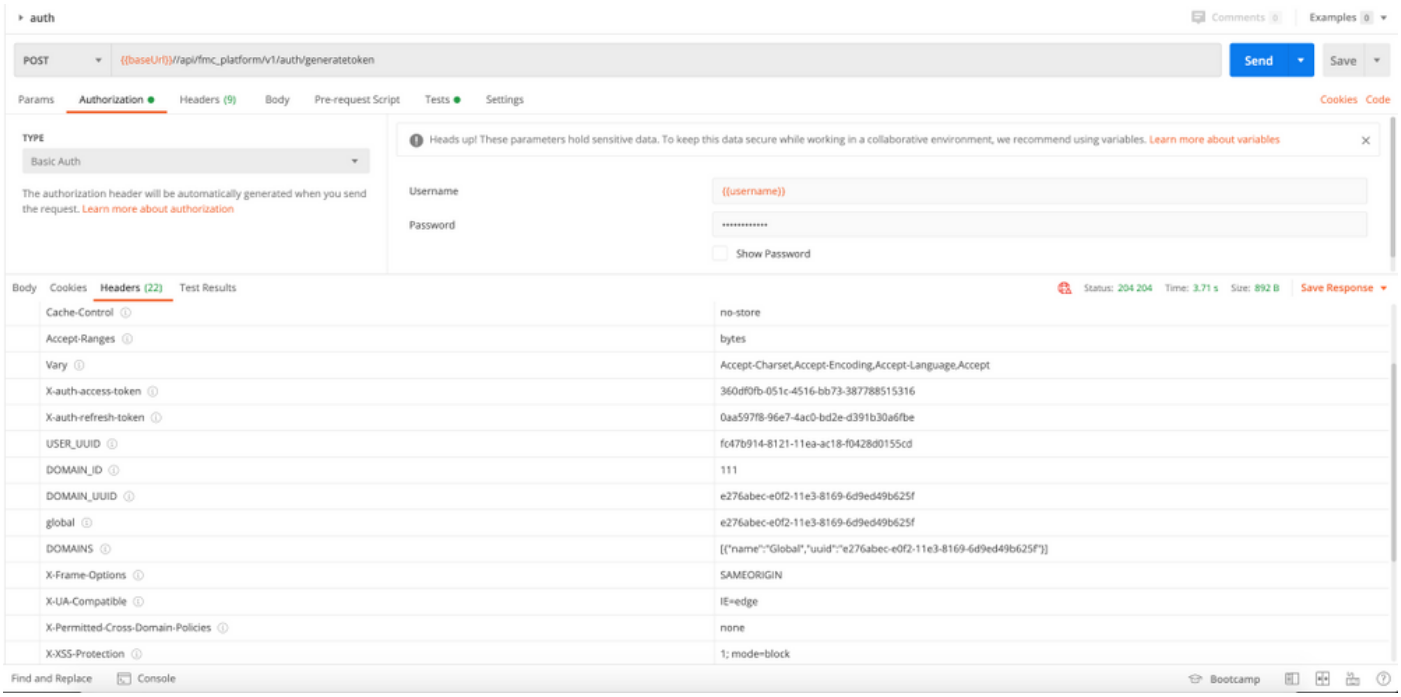
```
import requests url = "https://10.10.10.1//api/fmc_platform/v1/auth/generatetoken" payload = {}
headers = { 'Authorization': 'Basic Y2lzY291c2VyOmNpc2NwYXBpdXNlcg==' } response =
requests.request("POST", url, headers=headers, data = payload, verify=False)
print(response.headers)
```

使用CURL的驗證請求的另一個示例：

```
$ curl --request POST 'https://10.10.10.1/api/fmc_platform/v1/auth/generatetoken' --header
'Authorization: Basic Y2lzY291c2VyOmNpc2NwYXBpdXNlcg==' -k -i HTTP/1.1 204 204 Date: Tue, 11 Aug
2020 02:54:06 GMT Server: Apache Strict-Transport-Security: max-age=31536000; includeSubDomains
Cache-Control: no-store Accept-Ranges: bytes Vary: Accept-Charset,Accept-Encoding,Accept-
Language,Accept X-auth-access-token: aa6f8326-0a0c-4f48-9d85-7a920c0fdca5 X-auth-refresh-token:
674e87d1-1572-4cd1-b86d-3abec04ca59d USER_UUID: fc47b914-8121-11ea-ac18-f0428d0155cd DOMAIN_ID:
111 DOMAIN_UUID: e276abec-e0f2-11e3-8169-6d9ed49b625f global: e276abec-e0f2-11e3-8169-
```

6d9ed49b625f DOMAINS: [{"name":"Global","uuid":"e276abec-e0f2-11e3-8169-6d9ed49b625f"}] X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block Referrer-Policy: same-origin Content-Security-Policy: base-uri 'self' X-Content-Type-Options: nosniff

來自基於GUI的客戶端（如Postman）的示例，如下圖所示：




## 傳送後續API請求

> **附註**：您在輸出中看到的只是響應報頭，而不是響應正文。實際響應正文為空。 需要提取的重要標頭資訊是**X-auth-access-token**、**X-auth-refresh-token**和**DOMAIN_UUID**。

成功向FMC驗證並提取令牌後，對於進一步的API請求，您需要利用以下資訊：

- 新增標頭X-auth-access-token **<authentication token value>**作為請求的一部分。
- 在請求刷新令牌時新增X-auth-access-token **<authentication token value>**和X-auth-refresh-token **<refresh token value>**標頭。
- 在向伺服器的所有REST請求中，使用身份驗證令牌中的Domain_UUID。

使用此報頭資訊，您可以使用REST API成功與FMC互動。

# 排除常見問題

- 為身份驗證傳送的POST請求和響應正文為空。您需要在請求報頭中傳遞基本身份驗證引數。通過響應報頭返回所有令牌資訊。
- 使用REST客戶端時，您可能會看到由於自簽名證書而導致與SSL證書問題有關的錯誤。您可以根據所使用的客戶端關閉此驗證。
- 使用者憑證不能同時用於REST API和GUI介面，如果同時用於這兩種介面，使用者將無警告地註銷。
- FMC REST API身份驗證令牌有效期為30分鐘，最多可刷新三次。