How To Generate Authentication Token For FMC REST API Interactions

Introduction

This document describes how an Application programming interface (API) administrator can authenticate to Firepower Management Center (FMC), generate tokens and use them for any further API interactions.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Firepower Management Center (FMC) features and configuration. (Config Guide)
- Understanding of various REST API calls. (What are REST APIs?)
- Review of the FMC API Quick Start Guide.

Components Used

- Firepower Management Center that supports REST APIs (version 6.1 or higher) with REST API enabled.
- REST clients like Postman, Python scripts, CURL, etc.

Background Information

REST APIs are increasingly popular due to the lightweight programmable approach that network managers can use to configure and manage their networks. FMC supports configuration and management using any REST Client and also using the in-built API explorer.

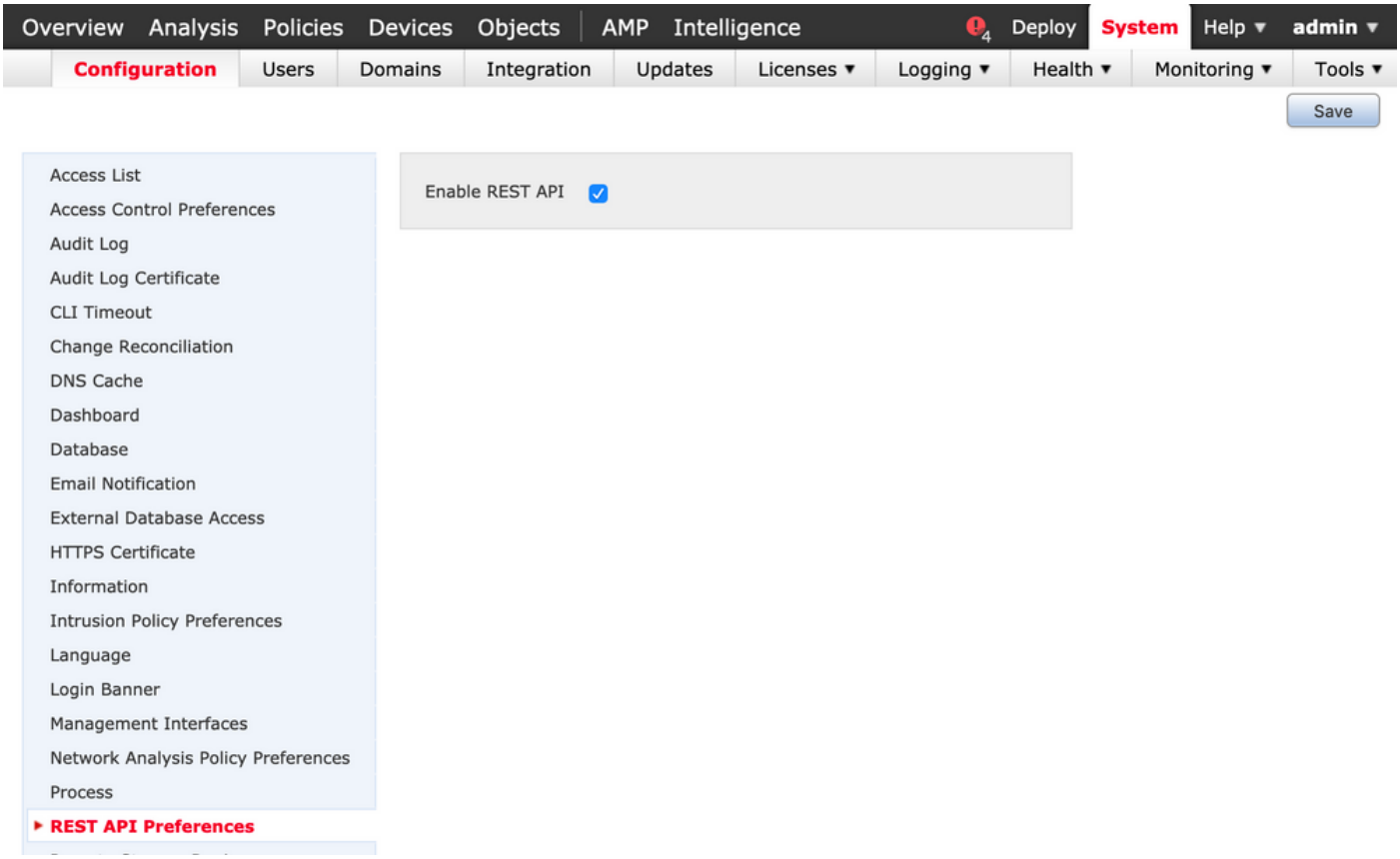
Configure

Enabling REST API on FMC

Step 1. Navigate to **System**>**Configuration**>**REST API Preferences**>Enable **REST API.**

Step 2. Check the **Enable REST API** checkbox.

Step 3. Click **Save,** a **Save Successful** dialog box is displayed when the REST API is enabled, as shown in the image:



Creating a user on FMC

As a best practice to use the API infrastructure on FMC is to keep UI users and script users separate. Refer the User Accounts for FMC Guide for the understanding of various user roles and the guidelines for creating a new user.

Steps To Request an Authentication token

Step 1. Open your **REST API Client**.

Step 2. Set the client to make a POST command, URL: https://<management_center_IP_or_name>/api/fmc_platform/v1/auth/generatetoken.

Step 3. Include the username and password as a basic authentication header. The **POST** body should be blank.

For example, an authentication request using Python:

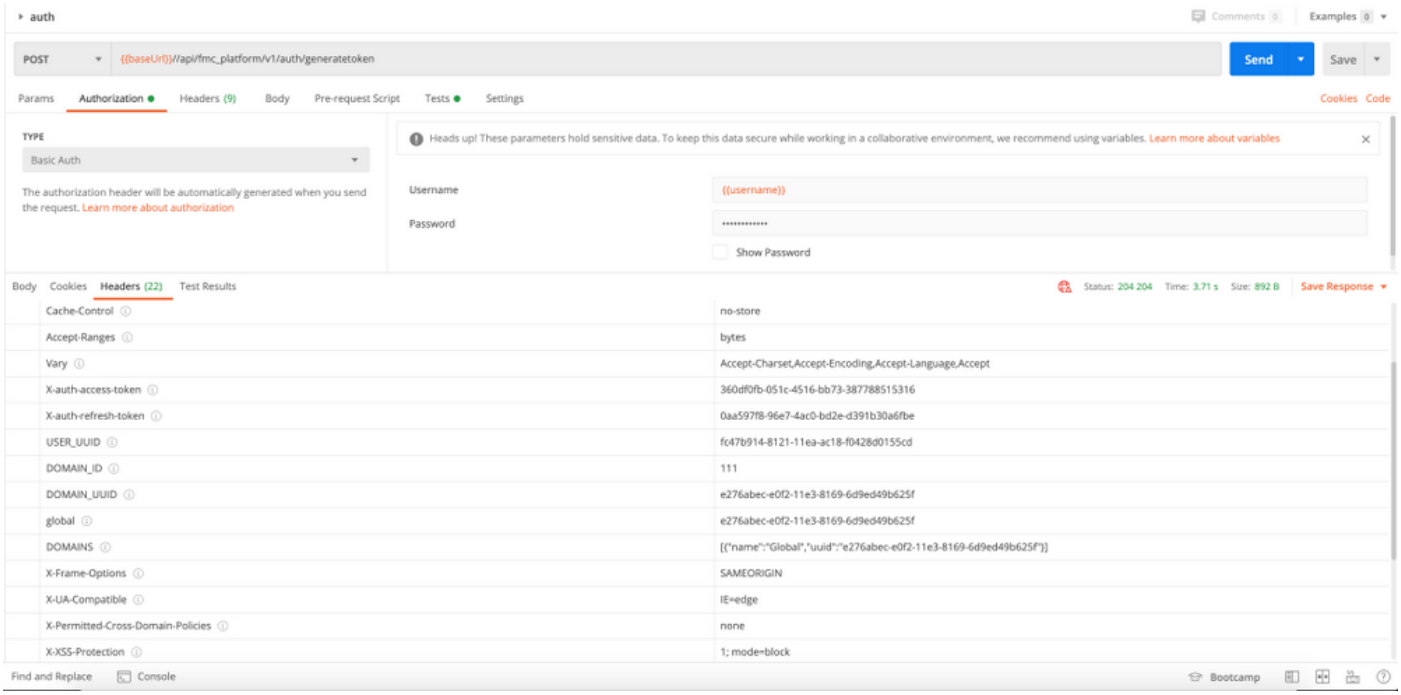
```
import requests url = "https://10.10.10.1//api/fmc_platform/v1/auth/generatetoken" payload = {}
headers = { 'Authorization': 'Basic Y2lzY291c2VyOmNpc2NwYXBpdXNlcg==' } response =
requests.request("POST", url, headers=headers, data = payload, verify=False)
print(response.headers)
```

Another example of an authentication request using CURL:

```
$ 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
```

Example from a GUI based client like Postman, as shown in the image:



Sending subsequent API requests

> **Note**: What you see in the output are the response headers and not the response body. The actual response body is blank. The important header information that needs to be extracted is **X-auth-access-token**, **X-auth-refresh-token**, and **DOMAIN_UUID**.

Once you have authenticated successfully to FMC and extracted the tokens, for further API requests you need to leverage below information:

- Add the header X-auth-access-token **<authentication token value>** as a part of the request.
- Add the headers X-auth-access-token **<authentication token value>** and X-auth-refresh-token **<refresh token value>** in requests to refresh the token.
- Use the Domain_UUID from the authentication token in all REST requests to the server.

With this header information, you can successfully interact with the FMC using REST APIs.

Troubleshoot common issues

- The request and response body of the POST sent for the authentication are blank. You need to pass the basic authentication parameters in the request header. All the token information is returned via the response headers.
- When using the REST client, you may see errors related to the SSL certificate problem due to a self-signed certificate. You can turn off this validation depending on the client you are using.

- User credentials cannot be used for both REST API And GUI interfaces simultaneously, and the user will be logged out without warning if used for both.
- The FMC REST API authentication tokens are valid for 30 minutes and can be refreshed up to three times.