Cómo Generar Token de Autenticación para Interacciones de API FMC REST

Introducción

Este documento describe cómo un administrador de la interfaz de programación de aplicaciones (API) puede autenticarse en Firepower Management Center (FMC), generar tokens y utilizarlos para cualquier interacción de API adicional.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Funciones y configuración de Firepower Management Center (FMC). (Guía de configuración)
- Comprensión de varias llamadas de API REST. (¿Qué son las API REST?)
- Revisión de la Guía de Inicio Rápido de la API de FMC.

Componentes Utilizados

- Firepower Management Center que admite API REST (versión 6.1 o superior) con API REST habilitada.
- Clientes REST como Postman, scripts Python, CURL, etc.

Antecedentes

Las API REST son cada vez más populares debido al enfoque programable ligero que los administradores de red pueden utilizar para configurar y gestionar sus redes. FMC admite la configuración y la gestión mediante cualquier cliente REST y también mediante el explorador API integrado.

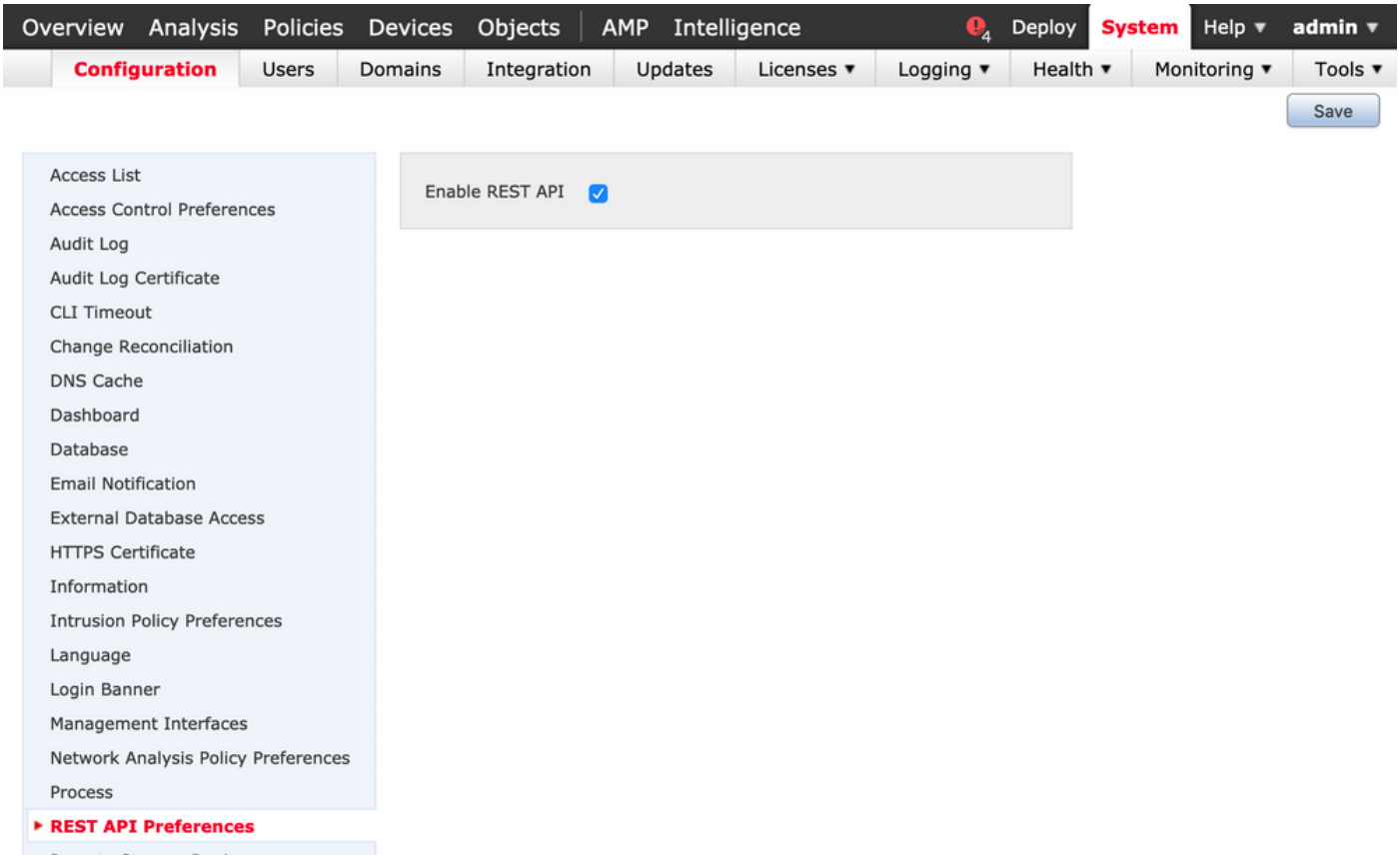
Configurar

Habilitación de la API REST en FMC

Paso 1. Vaya a **System** > **Configuration** > **REST API Preferences** > Enable **REST API API.**

Paso 2. Marque la casilla **Enable REST API** .

Paso 3. Haga clic en **Guardar,** se muestra un cuadro de diálogo **Guardar exitoso** cuando se habilita la API REST, como se muestra en la imagen:



Creación de un usuario en FMC

Como práctica recomendada para utilizar la infraestructura de la API en FMC, es mantener separados a los usuarios de la interfaz de usuario y a los usuarios de secuencias de comandos. Refiérase a la Guía de Cuentas de Usuario para FMC para conocer las diferentes funciones de usuario y las pautas para crear un nuevo usuario.

Pasos para solicitar un token de autenticación

Paso 1. Abra su **cliente de API REST**.

Paso 2. Configure el cliente para que realice un comando POST, URL: https://<management_center_IP_or_name>/api/fmc_platform/v1/auth/generatetoken.

Paso 3. Incluya el nombre de usuario y la contraseña como un encabezado de autenticación básico. El cuerpo **POST** debe estar vacío.

Por ejemplo, una solicitud de autenticación mediante Python:

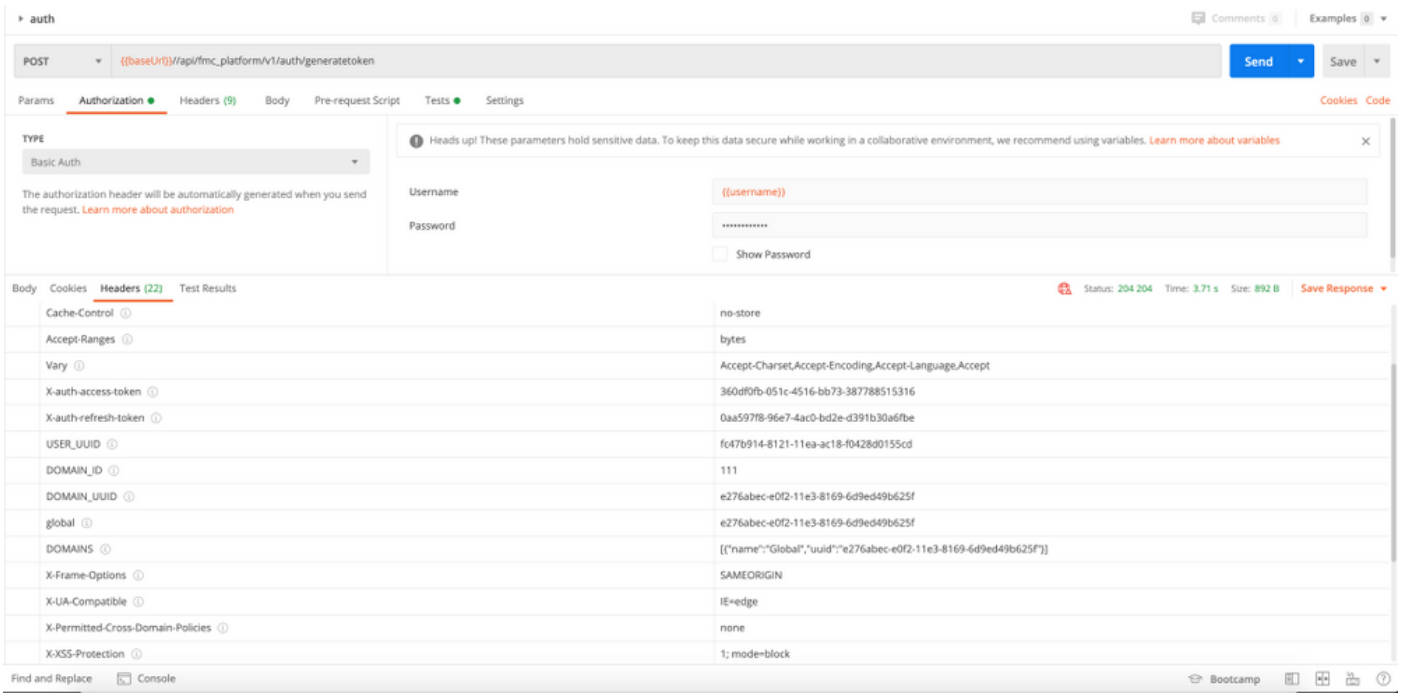
```
import requests url = "https://10.10.10.1//api/fmc_platform/v1/auth/generatetoken" payload = {}
headers = { 'Authorization': 'Basic Y2lzY291c2VyOmNpc2NwYXBpdXNlcg==' } response =
requests.request("POST", url, headers=headers, data = payload, verify=False)
print(response.headers)
```

Otro ejemplo de una solicitud de autenticación mediante 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
```

Ejemplo de un cliente basado en GUI como Postman, como se muestra en la imagen:



Envío de solicitudes API posteriores

> **Nota:** Lo que se ve en el resultado son los encabezados de respuesta y no el cuerpo de respuesta. El cuerpo de respuesta real está en blanco. La información importante del encabezado que debe extraerse es **X-auth-access-token**, **X-auth-refresh-token** y **DOMAIN_UID**.

Una vez que se haya autenticado correctamente en FMC y se hayan extraído los tokens, para obtener más solicitudes de API debe aprovechar la siguiente información:

- Agregue el encabezado X-auth-access-token **<authentication token value>** como parte de la solicitud.
- Agregue los encabezados X-auth-access-token **<authentication token value>** y X-auth-refresh-token **<refresh token value>** en las solicitudes para actualizar el token.
- Utilice el valor Domain_UID del token de autenticación en todas las solicitudes REST al servidor.

Con esta información de encabezado, puede interactuar con el FMC con las API REST.

Resolución de problemas comunes

- El cuerpo de solicitud y respuesta del POST enviado para la autenticación está en blanco. Debe pasar los parámetros básicos de autenticación en el encabezado de solicitud. Toda la

información del token se devuelve a través de los encabezados de respuesta.

- Al utilizar el cliente REST, puede ver errores relacionados con el problema del certificado SSL debido a un certificado autofirmado. Puede desactivar esta validación en función del cliente que esté utilizando.
- Las credenciales de usuario no se pueden utilizar para las interfaces REST API y GUI simultáneamente, y el usuario se desconectará sin previo aviso si se utiliza para ambas.
- Los tokens de autenticación de la API FMC REST son válidos durante 30 minutos y se pueden actualizar hasta tres veces.