

Demostrar la navegación a través del Explorador de API de Secure Firewall

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Revisar la navegación a través del Explorador FMC API](#)

[Revisar la navegación a través del Explorador FDM API](#)

[Troubleshoot](#)

Introducción

Este documento describe la navegación a través del explorador de la interfaz de programación de aplicaciones (API) de Cisco FMC y Cisco FDM.

Prerequisites

Comprensión básica de la API REST.

Requirements

Es necesario que esta demostración tenga acceso a la GUI de Firepower Management Center (FMC) con al menos un dispositivo administrado por este Firepower Management Center (FMC). Para la parte de FDM de esta demostración, es necesario tener un Firepower Threat Defence (FTD) administrado localmente para tener acceso a la GUI de FDM.

Componentes Utilizados

- FMCv
- FTDv
- FTDv gestionado localmente

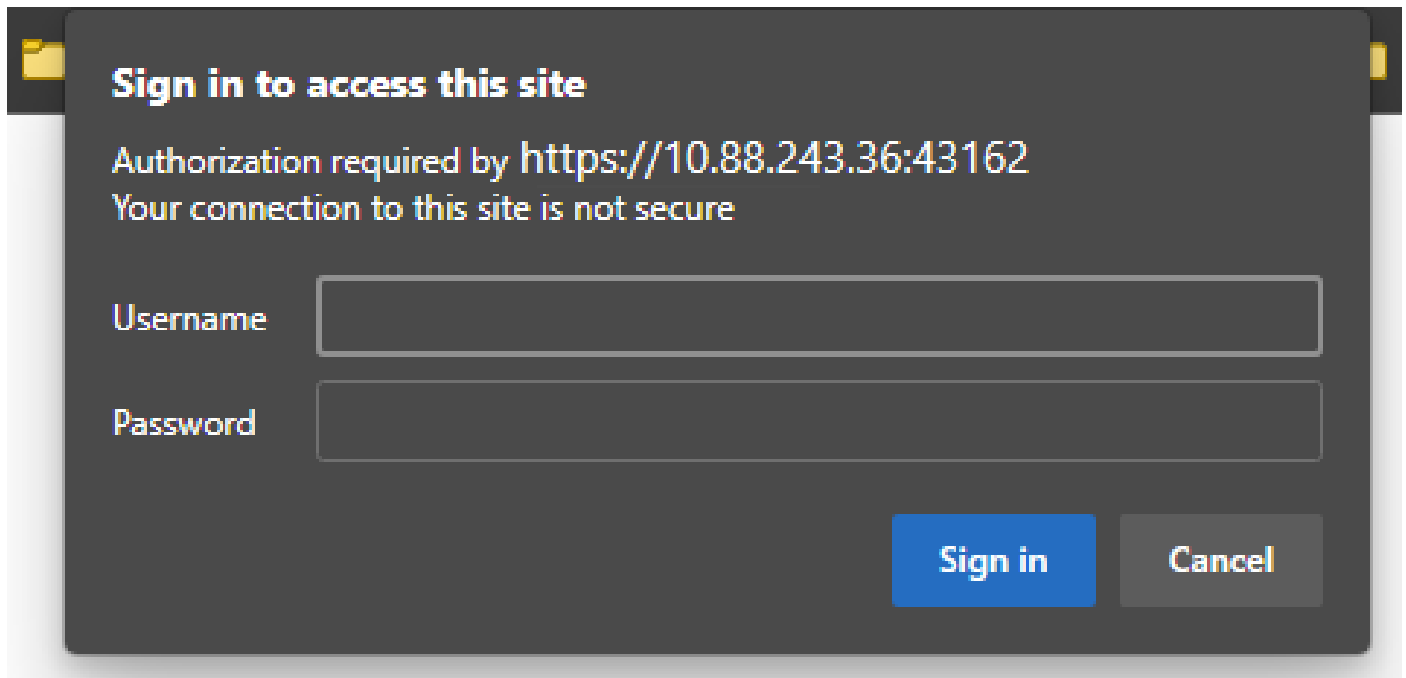
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Revisar la navegación a través del Explorador API FMC

Para acceder al explorador de API de FMC, vaya a la siguiente URL:

`https://<FMC_mgmt_IP>/api/api-explorer`

Debe iniciar sesión con las mismas credenciales utilizadas para la GUI de FMC. Estas credenciales se introducen en una ventana similar a la siguiente en la que se introducen las URL del explorador de API.

A dark gray dialog box with a title bar. The title is "Sign in to access this site" in white. Below the title, it says "Authorization required by https://10.88.243.36:43162" and "Your connection to this site is not secure". There are two input fields: "Username" and "Password". At the bottom right, there are two buttons: "Sign in" (blue) and "Cancel" (gray).

Sign in to access this site

Authorization required by `https://10.88.243.36:43162`
Your connection to this site is not secure

Username

Password

Sign in **Cancel**

Una vez iniciada la sesión, se observa que las consultas de API se dividen por categorías correspondientes a las posibles llamadas que puede realizar mediante las API.



Nota: No todas las funciones de configuración disponibles en la GUI o la CLI están disponibles a través de las API.

No seguro | <https://10.88.243.36:43162/api/api-explorer/>

Cisco Download OAS 2.0 Spec Download OAS 3.0 Spec Logout

Cisco Firewall Management Center Open API Specification 1.0.0 OAS3

/fmc_oas3.json

Specifies the REST URLs and methods supported in the Cisco Firewall Management Center API. Refer to the version specific [REST API Quick Start Guide](#) for additional information.

[Cisco Technical Assistance Center \(TAC\) - Website](#)
[Send email to Cisco Technical Assistance Center \(TAC\)](#)
[Cisco Firewall Management Center Licensing](#)

Domains
Global

- Troubleshoot
- Backup
- Network Map
- Devices
- Policy Assignments
- Device HA Pairs
- Health

Al hacer clic en una categoría, se expande y muestra las diferentes llamadas disponibles para esta categoría. Estas llamadas se muestran junto con sus respectivos métodos REST y el identificador de recursos universal (URI) de esa llamada.

- Integration
- Device Groups
- Status
- Device Clusters
- System Information
- Object
- Policy**

GET	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{objectId}
PUT	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{objectId}
DELETE	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{objectId}
GET	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies
POST	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies
GET	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/accessrules/{objectId}

En el siguiente ejemplo, se realiza una solicitud para ver las políticas de acceso configuradas en el FMC. Haga clic en el método correspondiente para expandirlo y, a continuación, haga clic en el botón Try it out.

Algo a destacar es que puede parametrizar sus consultas con los parámetros disponibles en cada llamada API. Solo son obligatorios aquellos con asteriscos rojos, los demás pueden dejarse

vacíos.

GET /api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies

Retrieves, deletes, creates, or modifies the access control policy associated with the specified ID. Also, retrieves list of all access control policies.

Parameters

Try it out

Name	Description
name string (query)	If parameter is specified, only the policy matching with the specified name will be displayed. Cannot be used if object ID is specified in path. name - If parameter is specified, only the poli
filter string (query)	Value is of format (including quotes): "locked:{true false}" locked query parameter when set to 'true' returns list of Access Policies which are locked and when set to 'false' returns policies which are unlocked. filter - Value is of format (including quotes): <
offset integer(\$int32) (query)	Index of first item to return. offset - Index of first item to return.
limit integer(\$int32) (query)	Number of items to return. limit - Number of items to return.
expanded boolean (query)	If set to true, the GET response displays a list of objects with additional attributes. --

Por ejemplo, domainUUID es obligatorio para todas las llamadas API, pero en el Explorador de API esto se completa automáticamente.

El siguiente paso es hacer clic en Ejecutar para realizar esta llamada.

name string (query)	If parameter is specified, only the policy matching with the specified name will be displayed. Cannot be used if object ID is specified in path. name - If parameter is specified, only the poli
filter string (query)	Value is of format (including quotes): "locked:{true false}" locked query parameter when set to 'true' returns list of Access Policies which are locked and when set to 'false' returns policies which are unlocked. filter - Value is of format (including quotes): <
offset integer(\$int32) (query)	Index of first item to return. offset - Index of first item to return.
limit integer(\$int32) (query)	Number of items to return. limit - Number of items to return.
expanded boolean (query)	If set to true, the GET response displays a list of objects with additional attributes. --
domainUUID * required string (path)	Domain UUID e276abec-e0f2-11e3-8169-6d9ed49b625f

Execute

Antes de hacer clic en Ejecutar, puede ver ejemplos de respuestas a las llamadas para hacerse una idea de las posibles respuestas que puede obtener en función de si la solicitud es correcta o no.

Execute

Responses

Code	Description	Links
200	OK	No links

Media type

application/json

Examples

Example 1 : GET /fmc_config/v1/domain/DomainUUID/policy/accesspolicies (Test GET ALL Success of Acc

Controls Accept header.

Example Value
Schema

```

{
  "links": "/fmc_config/v1/domain/DomainUUID/policy/accesspolicies?offset=0&limit=2",
  "items": [
    {
      "type": "AccessPolicy",
      "name": "AccessPolicy1_updated",
      "description": "policy to test FMC implementation",
      "defaultAction": {
        "id": "id_of_default_action",
        "type": "AccessPolicyDefaultAction"
      }
    },
    {
      "type": "AccessPolicy",
      "name": "AccessPolicy2_updated",
      "description": "policy to test FMC implementation",
      "defaultAction": {
        "id": "id_of_default_action",
        "type": "AccessPolicyDefaultAction"
      }
    }
  ]
}

```

Una vez que se ejecuta la llamada API, se obtiene, junto con la carga útil de respuesta, el código de respuesta. En este caso 200, que corresponde a una solicitud OK. También obtendrá la dirección URL y la dirección URL de la llamada que acaba de realizar. Esta información es útil si desea realizar esta llamada con un cliente/software externo.

La respuesta obtenida devuelve los ACP configurados en el FMC junto con su objectID. En este caso, puede ver esta información en el cuadro rojo de la siguiente imagen:

Execute
Clear

Responses

Curl

```

curl -X 'GET' \
  'https://10.88.243.36:43162/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies' \
  -H 'accept: application/json' \
  -H 'X-auth-access-token: d1594a50-3f98-4519-875b-50c70b454552'

```

Request URL

```
https://10.88.243.36:43162/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies
```

Server response

Code	Details
200	Response body <pre> { "links": { "self": "https://10.88.243.36:43162/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies?offset=0&limit=25" }, "items": [{ "type": "AccessPolicy", "links": { "self": "https://10.88.243.36:43162/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies/00505683-186A-0ed3-0000-004294967299" }, "name": "ACP_cchanes", "id": "00505683-186A-0ed3-0000-004294967299" }], "paging": { "offset": 0, "limit": 25, "count": 1, "pages": 1 } } </pre>

Download

Este objectID es el valor que se introduce en las llamadas que requieren referencia a este ACP. Por ejemplo, para crear una regla dentro de este ACP.

Los URI que contienen valores entre corchetes {0} son valores necesarios para realizar esta llamada. Recuerde que domainUUID es el único valor que se completa automáticamente.

GET	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/accessrules/{objectId}
PUT	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/accessrules/{objectId}
DELETE	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/accessrules/{objectId}
GET	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/accessrules
PUT	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/accessrules
POST	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/accessrules
DELETE	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/accessrules
GET	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/defaultactions/{objectId}
PUT	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/defaultactions/{objectId}
GET	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/loggingsettings/{objectId}
PUT	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/loggingsettings/{objectId}
GET	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/operational/hitcounts
PUT	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/operational/hitcounts
DELETE	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/operational/hitcounts

Los valores necesarios para estas llamadas se especifican en la descripción de la llamada. Para crear reglas para un ACP, necesita policyID, como puede ver en la siguiente imagen:

POST	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/accessrules
Retrieves, deletes, creates, or modifies the access control rule associated with the specified policy ID and rule ID. If no ID is specified, retrieves list of all access rules associated with the specified policy ID. Check the response section for applicable examples (if any).	

Este policyID se introduce en el campo especificado como containerUUID; otro campo obligatorio para los métodos POST es la carga útil o el cuerpo de la solicitud. Puede utilizar los ejemplos proporcionados para modificarlos según sus necesidades.

containerUUID required

string

(path)

The container id under which this specific resource is contained.

005056B3-1B6A-0ed3-0000-004294967299

domainUUID required

string

(path)

Domain UUID

e276abec-e0f2-11e3-8169-6d9ed49b625f

Request body required

application/json

The input access control rule model.

Examples:

Example 1 : POST /fmc_config/v1/domain/DomainUUID/policy/accesspolicies/containerUUID/accessrules (Test POST of Access rule)

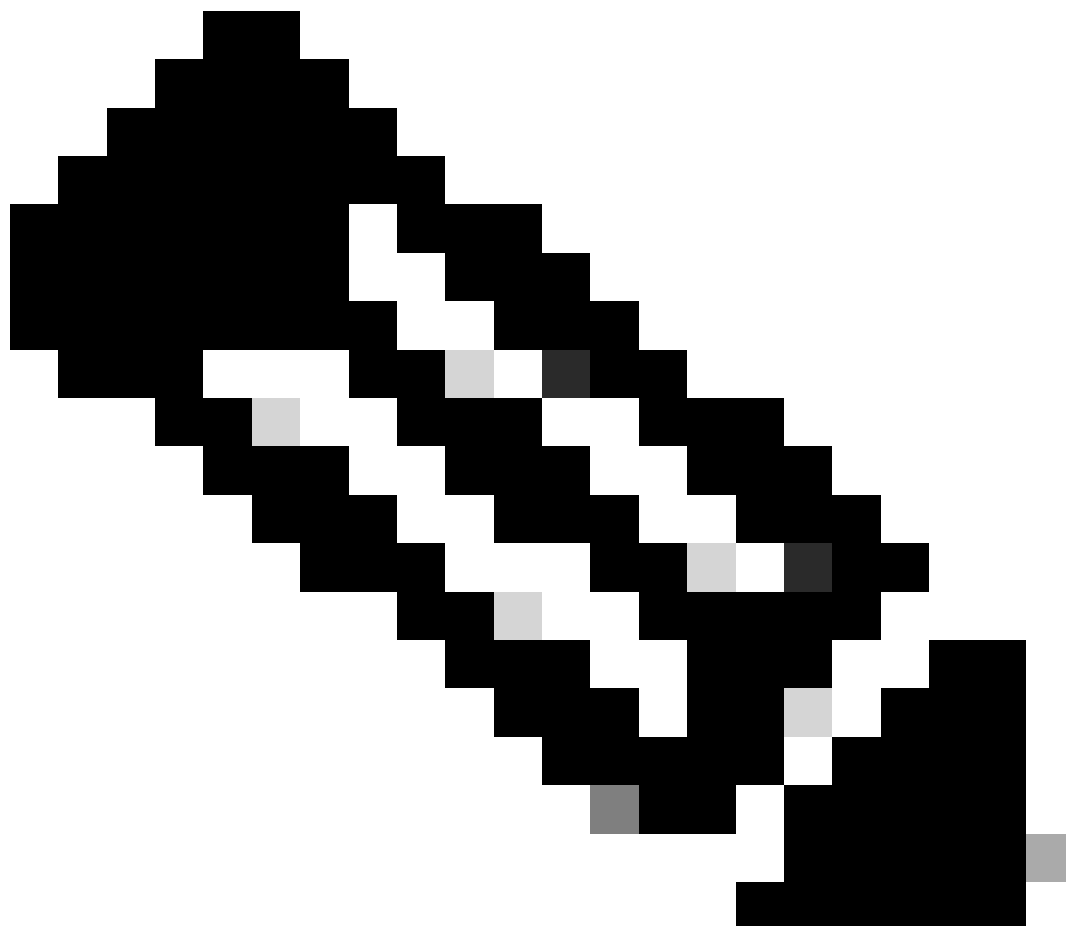
```

{
  "action": "ALLOW",
  "enabled": true,
  "type": "AccessRule",
  "name": "Rule1",
  "sendEventsToFMC": false,
  "logFiles": false,
  "logBegin": false,
  "logEnd": false,
  "variableSet": {
    "name": "Default Set",
    "id": "VariableSetUUID",
    "type": "VariableSet"
  },
  "vlanTags": {
    "objects": [
      {
        "type": "VlanTag",

```

Ejemplo de carga útil modificada:

```
{ "action": "ALLOW", "enabled": true, "type": "AccessRule", "name": "Testing API rule", "sendEventsToFMC": false, "logFiles": false,
"logBegin": false, "logEnd": false, "sourceZones": { "objects": [ { "name": "Inside_Zone", "id": "8c1c58ec-8d40-11ed-b39b-f2bc2b448f0d",
"type": "SecurityZone" } ] }, "destinationZones": { "objects": [ { "name": "Outside_Zone", "id": "c5e0a920-8d40-11ed-994a-900c72fc7112",
"type": "SecurityZone" } ] }, "newComments": [ "comment1", "comment2" ] }
```



Nota: Las zonas disponibles, junto con sus ID, se pueden obtener mediante la siguiente consulta.

GET

`/api/fmc_config/v1/domain/{domainUUID}/object/securityzones`

Una vez ejecutada la llamada anterior, se obtiene un código de respuesta 201, que indica que la solicitud se ha realizado correctamente y que ha dado lugar a la creación del recurso.

Server response

Code	Details
201	Response body <pre>{ "metadata": { "ruleIndex": 6, "section": "Default", "category": "--Undefined--", "accessPolicy": { "name": "ACP_cchanes", "id": "00505683-186A-0ed3-0000-004294967299", "type": "AccessPolicy" } }, "links": { "self": "https://10.88.243.36:43162/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies/00505683-186A-0ed3-0000-004294967299/accessrules/00505683-186A-0ed3-0000-000268435456" }, "enabled": true, "action": "ALLOW", "name": "Testing API rule", "type": "AccessRule", "id": "00505683-186A-0ed3-0000-000268435456", "variableSet": { "name": "Default Set", "id": "76fa83ea-c972-11e2-8be8-8e45bb1343c0", "type": "VariableSet" }, "sourceZones": { "objects": [</pre>

Por último, debe realizar un despliegue para que estos cambios surtan efecto en el FTD cuyo ACP se ha modificado.

Para esto, debe obtener la lista de dispositivos que tienen cambios listos para ser implementados.

GET `/api/fmc_config/v1/domain/{domainUUID}/deployment/deployabledevices`

Retrieves list of all devices with configuration changes, ready to be deployed.

El ejemplo contiene un par de dispositivos configurados en Alta disponibilidad. Debe obtener la ID de este HA; en caso de ser un dispositivo independiente, debe obtener la ID de ese dispositivo.

Responses

Curl

```
curl -X 'GET' \
  'https://10.88.243.36:43162/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/deployment/deployabledevices' \
  -H 'accept: application/json' \
  -H 'X-auth-access-token: 41f2e4aa-c681-4064-8cdc-6f734785dba9'
```

Request URL

```
https://10.88.243.36:43162/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/deployment/deployabledevices
```

Server response

Code	Details
200	Response body <pre>{ "links": { "self": "https://10.88.243.36:43162/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/deployment/deployabledevices?offset=0&limit=25" }, "items": [{ "version": "1689794173607", "name": "HA_FTD72", "type": "DeployableDevice" }], "paging": { "offset": 0, "limit": 25, "count": 1, "pages": 1 } }</pre>

La consulta necesaria para obtener el ID de dispositivo del HA es la siguiente:

GET /api/fmc_config/v1/domain/{domainUUID}/devicepairs/ftdddevicepairs

Retrieves or modifies the Firewall Threat Defense HA record associated with the specified ID. Creates or breaks or deletes a Firewall Threat Defense HA pair. If no ID is specified for a GET, retrieves list of all Firewall Threat Defense HA pairs.

Con el ID de dispositivo y el número de versión de implementación, puede modificar la carga útil del siguiente ejemplo de llamada para realizar la llamada para realizar esta implementación.

POST /api/fmc_config/v1/domain/{domainUUID}/deployment/deploymentrequests

Creates a request for deploying configuration changes to devices. *Check the response section for applicable examples (if any).*

Una vez ejecutada esta llamada, si todo es correcto, obtendrá una respuesta con el código 202.

Revisar la navegación mediante el Explorador de API de FDM

Para acceder al Explorador de la API de FDM, es posible utilizar un botón de la GUI de FDM para ir directamente a ella, como se muestra en la siguiente imagen:

The screenshot shows the Cisco FDM GUI interface. The top navigation bar includes tabs for Device Manager, Monitoring, Policies, Objects, and Device: firepower. A red box highlights the API Explorer button in the top right corner. Below the navigation bar, a table displays device information: Model (Cisco Firepower Threat Defense for VMwa...), Software (7.3.0-69), VDB (358.0), and Intrusion Rule Update (20221108-1055). The main content area shows a network diagram with an Inside Network connected to a Cisco Firepower Threat Defense for VMware device, which is connected to an ISP/WAN/Gateway. The gateway is connected to the Internet, which includes DNS Server, NTP Server, and Smart License.

Una vez en el Explorador de API, observará que las consultas también se dividen en categorías.

Secure Firewall Threat Defense REST API

The following is a list of resources you can use for programmatic access to the device using the Secure Firewall Threat Defense REST API. The resources are organized into groups of related resources. Click a group name to see the available methods and resources. Click a method/resource within a group to see detailed information. Within a method/resource, click the **Model** link under **Response Class** to see documentation for the resource.

You can test the various methods and resources through this page. When you fill in parameters and click the **Try it Out!** button, you interact directly with the system. GET calls retrieve real information. POST calls create real objects. PUT calls modify existing objects. DELETE calls remove real objects. However, most changes do not become active until you deploy them using the POST /operational/deploy resource in the Deployment group. Although some changes, such as to the management IP address and other system-level changes, do not require deployment, it is safer to do a deployment after you make any configuration changes.

The REST API uses OAuth 2.0 to validate access. Use the resources under the Token group to get a password-granted or custom access token, to refresh a token, or to revoke a token. You must include a valid access token in the Authorization: Bearer header on any HTTPS request from your API client.

Before using the REST API, you need to finish the device initial setup. You can complete the device initial setup either through UI or through InitialProvision API.

You can also refer to [this](#) page for a list of API custom error codes. (Additional errors might exist.)

NOTE: The purpose of the API Explorer is to help you learn the API. Testing calls through the API Explorer requires the creation of access locks that might interfere with regular operation. We recommend that you use the API Explorer on a non-production device.

Cisco makes no guarantee that the API version included on this Firepower Threat Device (the "API") will be compatible with future releases. Cisco, at any time in its sole discretion, may modify, enhance or otherwise improve the API based on user feedback.

Resource	Show/Hide	List Operations	Expand Operations
AAASetting			
ASPathList			
AccessPolicy			

Para expandir una categoría, debe hacer clic en ella y, a continuación, puede expandir cada una de las operaciones haciendo clic en cualquiera de ellas. Lo primero que se encuentra dentro de cada operación es un ejemplo de una respuesta OK para esta llamada.

AccessPolicy Show/Hide List Operations Expand Operations

Method	URL
GET	/policy/accesspolicies/{parentId}/accessrules
POST	/policy/accesspolicies/{parentId}/accessrules
DELETE	/policy/accesspolicies/{parentId}/accessrules/{objId}
GET	/policy/accesspolicies/{parentId}/accessrules/{objId}
PUT	/policy/accesspolicies/{parentId}/accessrules/{objId}
GET	/policy/accesspolicies

Response Class (Status 200)

Model	Example Value
	<pre>{ "items": [{ "version": "string", "name": "string", "defaultAction": { "action": "PERMIT", "eventLogAction": "LOG_FLOW_START", "intrusionPolicy": { "id": "string", "action": "string" } } }] }</pre>

Lo siguiente que verá son los parámetros disponibles para restringir las respuestas de la llamada que realice. Recuerde que solo los campos marcados como obligatorios son obligatorios para realizar dicha llamada.

Response Content Type application/json				
Parameters				
Parameter	Value	Description	Parameter Type	Data Type
offset		An integer representing the index of the first requested object. Index starts from 0. If not specified, the returned objects will start from index 0	query	integer
limit		An integer representing the maximum amount of objects to return. If not specified, the maximum amount is 10	query	integer
sort		The field used to sort the requested object list	query	string
filter		The criteria used to filter the models you are requesting. It should have the following format: {key}{operator}{value}; {key}{operator}{value}. Supported operators are: "!=" (not equals), "=" (equals), "~" (similar). Supported keys are: "name", "fts". The "fts" filter cannot be used with other filters.	query	string

Por último, encontrará los posibles códigos de respuesta que puede devolver esta llamada.

Response Messages			
HTTP Status Code	Reason	Response Model	Headers
401		Model Example Value <pre>{ "status_code": 0, "message": "string", "internal_error_code": 0 }</pre>	
403		Model Example Value <pre>{ "status_code": 0, "message": "string", "internal_error_code": 0 }</pre>	

Si desea realizar esta llamada, debe hacer clic en Try It Out. Para encontrar este botón, debe desplazarse hacia abajo hasta que encuentre este botón, ya que se encuentra en la parte inferior

de cada llamada.

520

Model

Example Value

```
{
  "status_code": 0,
  "message": "string",
  "internal_error_code": 0
}
```

TRY IT OUT!

Al hacer clic en el botón Try It Out, si se trata de una llamada que no requiere más campos, se ejecuta inmediatamente y proporciona la respuesta.

TRY IT OUT!

Hide Response

Curl

```
curl -X GET --header 'Accept: application/json' 'https://10.88.243.36:44178/api/fdm/v6/policy/accesspolicies'
```

Request URL

```
https://10.88.243.36:44178/api/fdm/v6/policy/accesspolicies
```

Response Body

```
{
  "items": [
    {
      "version": "ka4esjod4iebr",
      "name": "NGFW-Access-Policy",
      "defaultAction": {
        "action": "DENY",
        "eventLogAction": "LOG_NONE",
        "intrusionPolicy": null,
        "syslogServer": null,
        "hitCount": {
          "hitCount": 0,
          "firstHitTimeStamp": "",
          "lastHitTimeStamp": "",
          "lastFetchTimeStamp": ""
        }
      }
    }
  ]
}
```

Troubleshoot

Cada llamada genera un código de respuesta HTTP y un cuerpo de respuesta. Esto le ayuda a identificar dónde está el error.

El siguiente es un error común que ocurre cuando la sesión ha caducado, indicando que el token no es válido porque ha caducado.

Responses

Curl

```
curl -X 'GET' \
'https://10.88.243.36:43162/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies' \
-H 'accept: application/json' \
-H 'X-auth-access-token: d1594a50-3f98-4519-875b-50c70b454552'
```

Request URL

https://10.88.243.36:43162/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies

Server response

Code	Details
401	Error: 401

Response body

```
{
  "error": {
    "category": "FRAMEWORK",
    "messages": [
      {
        "description": "Access token invalid."
      }
    ],
    "severity": "ERROR"
  }
}
```

A continuación, se muestran ejemplos de códigos de respuesta HTTP que las llamadas pueden devolver:

- 2xx Series: Éxito. Existen varios códigos de estado: 200 (GET y PUT), 201 (POST), 202, 204 (DELETE). Indican una llamada API correcta.
- Serie 30x: redirección. Se puede utilizar cuando un cliente utilizó originalmente HTTP y fue redirigido a HTTPS.
- 4xx Series: error en el lado del cliente en la llamada API que se envió desde el cliente al servidor. Dos ejemplos incluyen un código de estado 401, que indica que la sesión no está autenticada, y un código 403, que indica un intento de acceso prohibido.
- 5xx Series: fallo de servidor, dispositivo o servicio. Esto podría deberse a que el servicio API del dispositivo se ha deshabilitado o es inaccesible a través de la red IP

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).