

# Demonstre a navegação por meio do API-Explorer do Secure Firewall

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Revisar Navegação através do Explorador FMC-API](#)

[Revisar Navegação pelo Explorador FDM-API](#)

[Troubleshooting](#)

---

## Introdução

Este documento descreve a navegação por meio do explorador da Interface de Programação de Aplicativos (API) do Cisco FMC e do Cisco FDM.

## Pré-requisitos

Entendimento básico da API REST.

## Requisitos

Para esta demonstração, é necessário ter acesso à GUI do Firepower Management Center (FMC) com pelo menos um dispositivo gerenciado por esse Firepower Management Center (FMC). Para a parte FDM desta demonstração, é necessário ter um Firepower Threat Defense (FTD) gerenciado localmente para ter acesso à GUI do FDM.

## Componentes Utilizados

- FMCv
- FTDv
- FTDv Gerenciado localmente

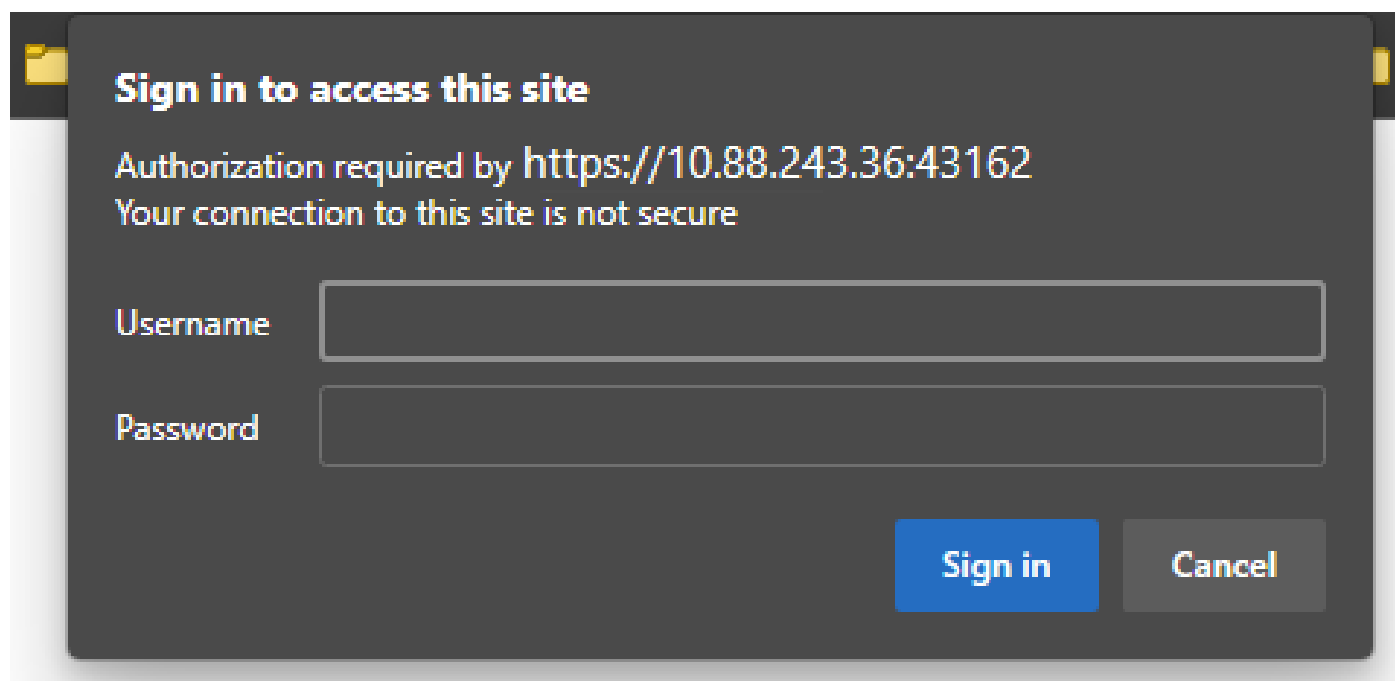
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Revisar a navegação pelo FMC API Explorer

Para acessar o FMC API explorer, navegue até o próximo URL:

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

Você deve fazer login com as mesmas credenciais usadas para a GUI do FMC. Essas credenciais são inseridas em uma janela semelhante à seguinte quando você insere os URLs do explorador de API.



**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**

Após o login, é visto que as consultas de API são divididas por categorias correspondentes às possíveis chamadas que você pode fazer usando APIs.



Observação: nem todas as funções de configuração disponíveis na GUI ou na CLI estão disponíveis através das APIs.

---

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

Quando você clica em uma categoria, ela é expandida, mostrando as diferentes chamadas disponíveis para essa categoria. Essas chamadas são mostradas junto com seus respectivos métodos REST e o Universal Resource Identifier (URI) dessa chamada.

- 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}

No próximo exemplo, você faz uma solicitação para ver as políticas de acesso configuradas no FMC. Clique no método correspondente para expandi-lo e, em seguida, clique no botão Try it out.

É importante enfatizar que você pode parametrizar suas consultas com os parâmetros disponíveis em cada chamada de API. Somente aqueles com asteriscos vermelhos são obrigatórios, os outros podem ser deixados vazios.

**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
<b>name</b> 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. <input type="text" value="name - If parameter is specified, only the poli"/>
<b>filter</b> 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. <input type="text" value="filter - Value is of format (including quotes): &lt;"/>
<b>offset</b> integer(\$int32) (query)	Index of first item to return. <input type="text" value="offset - Index of first item to return."/>
<b>limit</b> integer(\$int32) (query)	Number of items to return. <input type="text" value="limit - Number of items to return."/>
<b>expanded</b> boolean	If set to true, the GET response displays a list of objects with additional attributes. <input type="text" value="--"/>

Por exemplo, o domainUUID é obrigatório para todas as chamadas de API, mas no Explorador de API isso é preenchido automaticamente.

A próxima etapa é clicar em Executar para fazer essa chamada.

<b>name</b> 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. <input type="text" value="name - If parameter is specified, only the poli"/>
<b>filter</b> 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. <input type="text" value="filter - Value is of format (including quotes): &lt;"/>
<b>offset</b> integer(\$int32) (query)	Index of first item to return. <input type="text" value="offset - Index of first item to return."/>
<b>limit</b> integer(\$int32) (query)	Number of items to return. <input type="text" value="limit - Number of items to return."/>
<b>expanded</b> boolean (query)	If set to true, the GET response displays a list of objects with additional attributes. <input type="text" value="--"/>
<b>domainUUID</b> * required string (path)	Domain UUID <input type="text" value="e276abec-e0f2-11e3-8169-6d9ed49b625f"/>

Execute

Antes de clicar em Executar, você poderá ver exemplos de respostas às chamadas para ter uma ideia das respostas possíveis, dependendo se a solicitação está correta ou não.

Execute

**Responses**

Code	Description	Links
200	OK	No links

Media type:  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"
      }
    }
  ]
}

```

Depois que a chamada de API é executada, você obtém, junto com o payload de resposta, o código de resposta. Nesse caso, 200, que corresponde a um pedido OK. Você também obtém a cURL e a URL da chamada que acabou de fazer. Essas informações serão úteis se você quiser fazer essa chamada com um software/cliente externo.

A resposta obtida retorna os ACPs configurados no FMC junto com seu objectID. Nesse caso, você pode ver essas informações na caixa vermelha na próxima imagem:

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

```

{
  "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
  }
}

```

Download

Este objectID é o valor inserido em chamadas que requerem referência a este ACP. Por exemplo, para criar uma regra neste ACP.

Os URIs que contêm valores entre chaves {} são valores necessários para fazer essa chamada. Lembre-se de que domainUID é o único valor preenchido automaticamente.

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

Os valores necessários para essas chamadas são especificados na descrição da chamada. Para criar regras para um ACP, é necessário o policyID, como você pode ver na próxima imagem:

POST	/api/fmc_config/v1/domain/{domainUID}/policy/accesspolicies/{containerUID}/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).	

Essa policyID é inserida no campo especificado como containerUID, outro campo obrigatório para métodos POST é o corpo da carga ou da solicitação. Você pode usar os exemplos fornecidos para modificar de acordo com suas necessidades.

**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",

```

### Exemplo 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" ] }
```





**Observação:** as zonas disponíveis, juntamente com suas IDs, podem ser obtidas usando a próxima consulta.

---

GET

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

Depois de executar a chamada anterior, você obtém um código de resposta 201, indicando que a solicitação foi bem-sucedida e levou à criação do recurso.

```
Server response
Code    Details
201    Response body
{
  "metadata": {
    "ruleIndex": 6,
    "section": "Default",
    "category": "--Undefined--",
    "accessPolicy": {
      "name": "ACP_cchanes",
      "id": "005056B3-1B6A-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/005056B3-1B6A-0ed3-0000-004294967299/accessrules/005056B3-1B6A-0ed3-0000-000268435456"
  },
  "enabled": true,
  "action": "ALLOW",
  "name": "Testing API rule",
  "type": "AccessRule",
  "id": "005056B3-1B6A-0ed3-0000-000268435456",
  "variableSet": {
    "name": "Default Set",
    "id": "76fa83ea-c972-11e2-8be8-8e45bb1343c0",
    "type": "VariableSet"
  },
  "sourceZones": {
    "objects": [

```

Finalmente, você deve fazer uma implantação para que essas alterações entrem em vigor no FTD cujo ACP foi modificado.

Para isso, você precisa obter a lista de dispositivos que têm alterações prontas para serem implantadas.

**GET** /api/fmc\_config/v1/domain/{domainUUID}/deployment/deployabledevices

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

O exemplo contém um par de dispositivos configurados em Alta Disponibilidade. Você deve obter a ID deste HA, caso seja um dispositivo autônomo, você deve obter a ID desse 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
{
  "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_FT072",
      "type": "DeployableDevice"
    }
  ],
  "paging": {
    "offset": 0,
    "limit": 25,
    "count": 1,
    "pages": 1
  }
}
```

A consulta necessária para obter a ID do dispositivo do HA é a seguinte:

**GET** /api/fmc\_config/v1/domain/{domainUUID}/devicepairs/ftddevicepairs

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.

Com o ID do dispositivo e o número da versão de implantação, você pode modificar o payload do próximo exemplo de chamada para fazer a chamada para executar essa implantação.

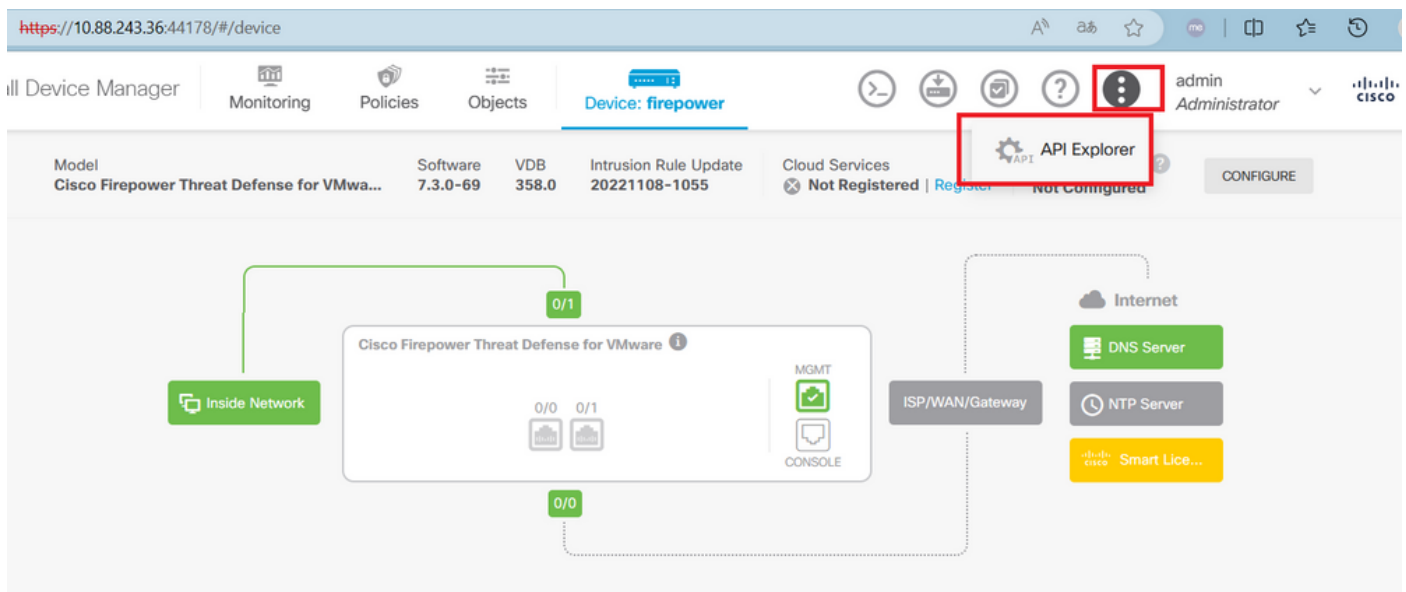
**POST** /api/fmc\_config/v1/domain/{domainUUID}/deployment/deploymentrequests

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

Uma vez executada esta chamada, se tudo estiver correto, você obterá uma resposta com o código 202.

Revise a Navegação por meio do FDM API Explorer

Para acessar o API Explorer do FDM, é possível usar um botão na GUI do FDM para ir diretamente para ele, como mostrado na imagem a seguir:



No API Explorer, você observa que as consultas também são divididas em categorias.

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.

<b>AAASetting</b>	Show/Hide	List Operations	Expand Operations
<b>ASPathList</b>	Show/Hide	List Operations	Expand Operations
<b>AccessPolicy</b>	Show/Hide	List Operations	Expand Operations

Para expandir uma categoria, você deve clicar nela e, em seguida, pode expandir cada uma das operações clicando em qualquer uma delas. A primeira coisa encontrada dentro de cada operação é um exemplo de uma resposta OK para essa chamada.

**AccessPolicy** Show/Hide List Operations Expand Operations

- 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",           "name": "string"         }       }     }   ] }</pre>

Em seguida, você verá os parâmetros disponíveis para restringir as respostas da chamada feita. Lembre-se de que somente os campos marcados como obrigatórios são obrigatórios para fazer essa chamada.

Response Content Type

### Parameters

Parameter	Value	Description	Parameter Type	Data Type
offset	<input type="text"/>	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	<input type="text"/>	An integer representing the maximum amount of objects to return. If not specified, the maximum amount is 10	query	integer
sort	<input type="text"/>	The field used to sort the requested object list	query	string
filter	<input type="text"/>	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

Finalmente, você encontrará os possíveis códigos de resposta que essa chamada pode retornar.

### Response Messages

HTTP Status Code	Reason	Response Model	Headers				
401		<table border="1"><thead><tr><th>Model</th><th>Example Value</th></tr></thead><tbody><tr><td></td><td><pre>{   "status_code": 0,   "message": "string",   "internal_error_code": 0 }</pre></td></tr></tbody></table>	Model	Example Value		<pre>{   "status_code": 0,   "message": "string",   "internal_error_code": 0 }</pre>	
Model	Example Value						
	<pre>{   "status_code": 0,   "message": "string",   "internal_error_code": 0 }</pre>						
403		<table border="1"><thead><tr><th>Model</th><th>Example Value</th></tr></thead><tbody><tr><td></td><td><pre>{   "status_code": 0,   "message": "string",   "internal_error_code": 0 }</pre></td></tr></tbody></table>	Model	Example Value		<pre>{   "status_code": 0,   "message": "string",   "internal_error_code": 0 }</pre>	
Model	Example Value						
	<pre>{   "status_code": 0,   "message": "string",   "internal_error_code": 0 }</pre>						

Para fazer essa chamada, clique em **Try It Out**. Para encontrar esse botão, você deve rolar para baixo até encontrar esse botão, pois ele está localizado na parte inferior de cada chamada.

520

Model	Example Value
	<pre>{   "status_code": 0,   "message": "string",   "internal_error_code": 0 }</pre>

**TRY IT OUT**

Quando você clica no botão Try It Out, se for uma chamada que não requer mais campos, ela é executada imediatamente e fornece a resposta.

**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": ""
        }
      }
    }
  ]
}
```

## Troubleshooting

Cada chamada gera um código de resposta HTTP e um corpo de resposta. Isso ajuda a identificar onde o erro está.

O próximo é um erro comum que ocorre quando a sessão expira, indicando que o token é inválido porque expirou.

The screenshot displays a REST client interface with the following sections:

- Responses**: The main header of the interface.
- Curl**: A text area containing the command: `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**: A text area containing the URL: `https://10.88.243.36:43162/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies`
- Server response**: A table with two columns: **Code** and **Details**. The first row shows the code `401` and the detail `Error: 401`. Both the code and detail cells are highlighted with a red border.
- Response body**: A text area containing a JSON object: `{ "error": { "category": "FRAMEWORK", "messages": [ { "description": "Access token invalid." } ] }, "severity": "ERROR" }`. The `"description": "Access token invalid."` field is highlighted with a red border.

A seguir estão exemplos de códigos de resposta HTTP que as chamadas podem retornar:

- Série 2xx: sucesso. Existem vários códigos de status: 200 (GET e PUT), 201 (POST), 202, 204 (DELETE). Indicam uma chamada à API bem-sucedida.
- Série 30x: redirecionamento. Pode ser usado quando um cliente originalmente usou HTTP e foi redirecionado para HTTPS.
- Série 4xx: falha do lado do cliente na chamada API enviada do cliente para o servidor. Dois exemplos incluem um código de status 401, indicando que a sessão não está autenticada, e um código 403, indicando uma tentativa de acesso proibido.
- Série 5xx: falha no servidor, dispositivo ou no lado do serviço. Isso pode ser o resultado de o serviço API do dispositivo estar desabilitado ou inacessível pela rede IP

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.