

# Démonstration de la navigation dans l'API-Explorer de Secure Firewall

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Vérifier la navigation dans l'Explorateur FMC API](#)

[Vérifier la navigation via l'Explorateur FDM API](#)

[Dépannage](#)

---

## Introduction

Ce document décrit la navigation à travers l'explorateur d'interface de programmation d'application (API) de Cisco FMC et de Cisco FDM.

## Conditions préalables

Compréhension de base de l'API REST.

## Exigences

Pour cette démonstration, vous devez avoir accès à l'interface utilisateur graphique de Firepower Management Center (FMC) avec au moins un périphérique géré par ce Firepower Management Center (FMC). Pour la partie FDM de cette démonstration, il est nécessaire de disposer d'un pare-feu Firepower Threat Defense (FTD) géré localement pour accéder à l'interface utilisateur graphique FDM.

## Composants utilisés

- FMCv
- FTDv
- FTDv Géré localement

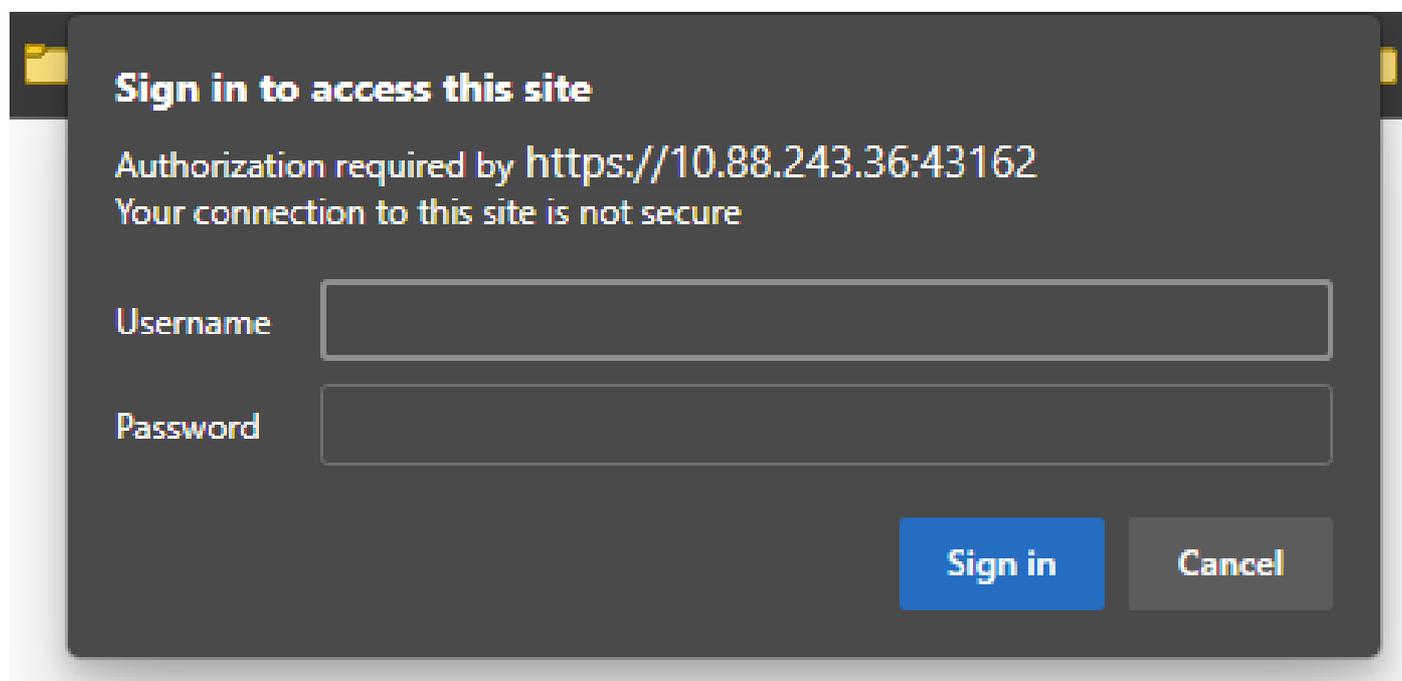
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Vérifier la navigation via l'Explorateur d'API FMC

Pour accéder à l'explorateur d'API FMC, accédez à l'URL suivante :

[https://<FMC\\_mgmt\\_IP>/api/api-explorer](https://<FMC_mgmt_IP>/api/api-explorer)

Vous devez vous connecter avec les mêmes informations d'identification que celles utilisées pour l'interface utilisateur graphique FMC. Ces informations d'identification sont entrées dans une fenêtre semblable à la suivante lorsque vous entrez les URL de l'explorateur d'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**

Une fois connectées, les requêtes API sont divisées en catégories correspondant aux appels possibles que vous pouvez effectuer à l'aide des API.



Remarque : toutes les fonctions de configuration disponibles depuis l'interface utilisateur graphique ou l'interface de ligne de commande ne sont pas disponibles via les 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:

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

Lorsque vous cliquez sur une catégorie, elle se développe et vous affiche les différents appels disponibles pour cette catégorie. Ces appels sont affichés avec leurs méthodes REST respectives et l'URI (Universal Resource Identifier) de cet appel.

- 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}

Dans l'exemple suivant, vous demandez à voir les stratégies d'accès configurées dans le FMC. Cliquez sur la méthode correspondante pour la développer, puis cliquez sur le bouton Try it out.

Il est important de souligner que vous pouvez paramétrer vos requêtes avec les paramètres disponibles dans chaque appel d'API. Seuls les astérisques rouges sont obligatoires, les autres peuvent rester vides.

**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 (query)	If set to true, the GET response displays a list of objects with additional attributes. <input type="text" value="--"/>

Par exemple, domainUUID est obligatoire pour tous les appels d'API, mais dans l'Explorateur d'API, il remplit automatiquement.

L'étape suivante consiste à cliquer sur Exécute pour passer cet appel.

<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

Avant de cliquer sur Exécuter, vous pouvez voir des exemples de réponses aux appels pour avoir une idée des réponses possibles que vous pouvez obtenir selon que la demande est correcte ou non.

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"
      }
    }
  ]
}

```

Une fois l'appel d'API exécuté, vous obtenez, avec la charge utile de réponse, le code de réponse. Dans ce cas 200, ce qui correspond à une requête OK. Vous obtenez également l'URLc et l'URL de l'appel que vous venez de passer. Ces informations sont utiles si vous souhaitez passer cet appel avec un client/logiciel externe.

La réponse obtenue renvoie les ACP configurés dans le FMC avec leur objectID. Dans ce cas, vous pouvez voir ces informations dans la zone rouge de l'image suivante :

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

Cet objectID est la valeur que vous entrez dans les appels qui nécessitent une référence à cet ACP. Par exemple, pour créer une règle dans cet ACP.

Les URI qui contiennent des valeurs entre accolades {} sont des valeurs requises pour effectuer cet appel. N'oubliez pas que domainUUID est la seule valeur qui est automatiquement remplie.

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

Les valeurs requises pour ces appels sont spécifiées dans la description de l'appel. Pour créer des règles pour un ACP, vous avez besoin du policyID, comme vous pouvez le voir dans l'image suivante :

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).	

Ce policyID est entré dans le champ spécifié comme containerUUID, un autre champ requis pour les méthodes POST est la charge utile ou le corps de la requête. Vous pouvez utiliser les exemples donnés pour modifier selon vos besoins.

**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",

```

### Exemple de charge utile modifiée :

```
{ "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" ] }
```



**Remarque** : les zones disponibles, ainsi que leurs ID, peuvent être obtenues à l'aide de la requête suivante.

---

**GET**

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

Une fois que vous avez exécuté l'appel précédent, vous obtenez un code de réponse 201, indiquant que la demande a réussi et a conduit à la création de la ressource.

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": [
```

Enfin, vous devez effectuer un déploiement pour que ces modifications prennent effet dans le FTD dont l'ACP a été modifié.

Pour cela, vous devez obtenir la liste des périphériques dont les modifications sont prêtes à être déployées.

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

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

L'exemple contient une paire de périphériques configurés en haute disponibilité. Vous devez obtenir l'ID de cette haute disponibilité. Dans le cas d'un périphérique autonome, vous devez obtenir l'ID de ce périphérique.

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
  }
}
```

La requête requise pour obtenir l'ID de périphérique de la haute disponibilité est la suivante :

**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.

Avec l'ID de périphérique et le numéro de version du déploiement, vous pouvez modifier la charge utile de l'exemple d'appel suivant pour passer l'appel pour effectuer ce déploiement.

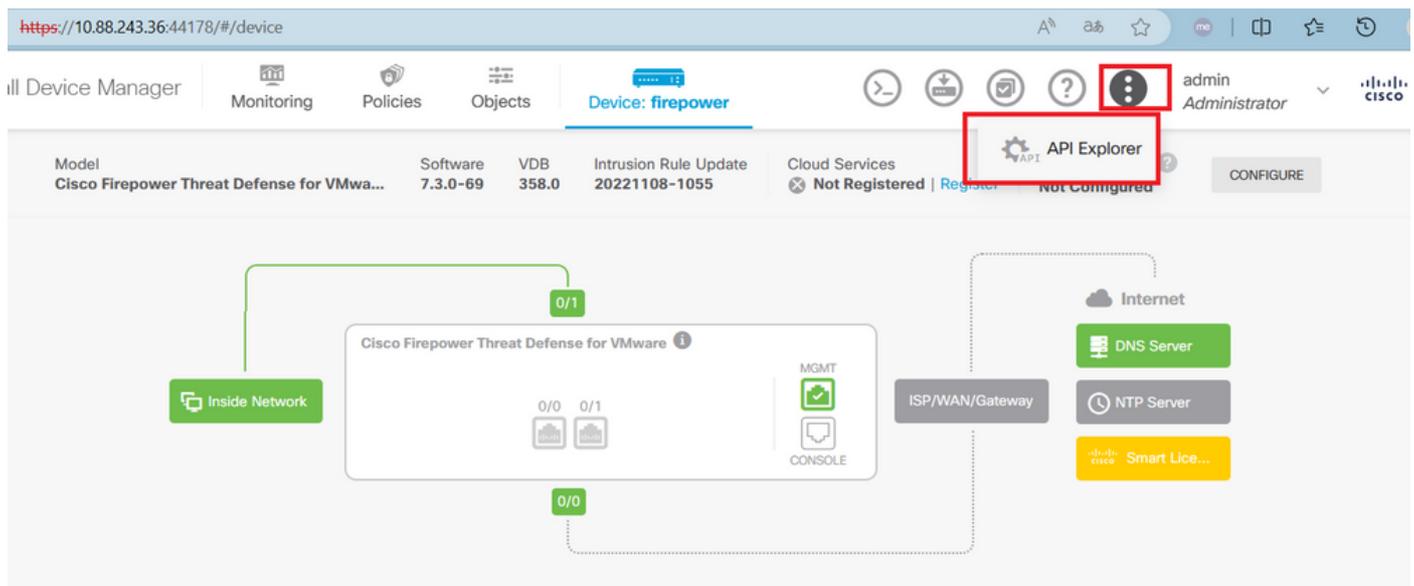
**POST** /api/fmc\_config/v1/domain/{domainUUID}/deployment/deploymentrequests

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

Une fois cet appel exécuté, si tout est correct, vous obtenez une réponse avec le code 202.

Vérifier la navigation via l'Explorateur d'API FDM

Pour accéder à l'explorateur d'API FDM, il est possible d'utiliser un bouton de l'interface utilisateur graphique FDM pour y accéder directement, comme illustré dans l'image suivante :



Une fois dans l'Explorateur d'API, vous remarquerez que les requêtes sont également divisées en catégories.

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.

**AAASetting** Show/Hide List Operations Expand Operations

**ASPathList** Show/Hide List Operations Expand Operations

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

Pour développer une catégorie, vous devez cliquer dessus, puis vous pouvez développer chacune des opérations en cliquant sur l'une d'entre elles. La première chose trouvée dans chaque opération est un exemple de réponse OK pour cet appel.

**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>

La prochaine chose que vous voyez sont les paramètres disponibles pour contraindre les réponses de l'appel que vous faites. N'oubliez pas que seuls les champs marqués comme obligatoires sont obligatoires pour passer un tel appel.

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

Enfin, vous trouverez les codes de réponse possibles que cet appel peut renvoyer.

### 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>						

Si vous voulez passer cet appel, vous devez cliquer sur **Try It Out**. Pour trouver ce bouton, vous devez faire défiler la page vers le bas jusqu'à ce que vous trouviez ce bouton puisqu'il est situé au bas de chaque appel.

internal\_error\_code: 0  
}

520

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

**TRY IT OUT!**

Lorsque vous cliquez sur le bouton Try It Out, s'il s'agit d'un appel qui ne nécessite pas plus de champs, il s'exécute immédiatement et vous donne la réponse.

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

Chaque appel génère un code de réponse HTTP et un corps de réponse. Cela vous aide à identifier où se trouve l'erreur.

La suivante est une erreur courante qui se produit lorsque la session a expiré, indiquant que le jeton est non valide car il a expiré.

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

- Responses**: The main header.
- Curl**: A terminal window showing 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**: `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 **401** and **Error: 401**, both highlighted with a red box.
- Response body**: A JSON object: `{ "error": { "category": "FRAMEWORK", "messages": [ { "description": "Access token invalid." } ] }, "severity": "ERROR" }`. The `"description": "Access token invalid."` field is highlighted with a red box.

Voici quelques exemples de codes de réponse HTTP que les appels peuvent renvoyer :

- Série 2xx : réussite. Il existe plusieurs codes d'état : 200 (GET et PUT), 201 (POST), 202, 204 (DELETE). Elles indiquent un appel API réussi.
- Série 30x : redirection. Peut être utilisé lorsqu'un client a utilisé HTTP à l'origine et a été redirigé vers HTTPS.
- Série 4xx : échec côté client de l'appel d'API envoyé du client au serveur. Deux exemples incluent un code d'état 401, indiquant que la session n'est pas authentifiée, et un code 403, indiquant une tentative d'accès interdit.
- Série 5xx : défaillance du serveur, du périphérique ou du service. Cela peut être dû à la désactivation du service API du périphérique ou à l'inaccessibilité sur le réseau IP

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.