

Navigation durch API-Explorer der Secure Firewall demonstrieren

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Navigation durch FMC API Explorer überprüfen](#)

[Navigation durch FDM API Explorer überprüfen](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird die Navigation durch den API-Explorer (Application Programming Interface) von Cisco FMC und Cisco FDM beschrieben.

Voraussetzungen

Grundlegendes Verständnis der REST-API.

Anforderungen

Für diese Demonstration ist der Zugriff auf die Benutzeroberfläche des Firepower Management Center (FMC) mit mindestens einem von diesem Firepower Management Center (FMC) verwalteten Gerät erforderlich. Für den FDM-Teil dieser Demonstration ist eine lokale Verwaltung einer FirePOWER Threat Defense (FTD) erforderlich, um Zugriff auf die FDM-GUI zu erhalten.

Verwendete Komponenten

- FMC V
- FTDv
- FTDv Lokal verwaltet

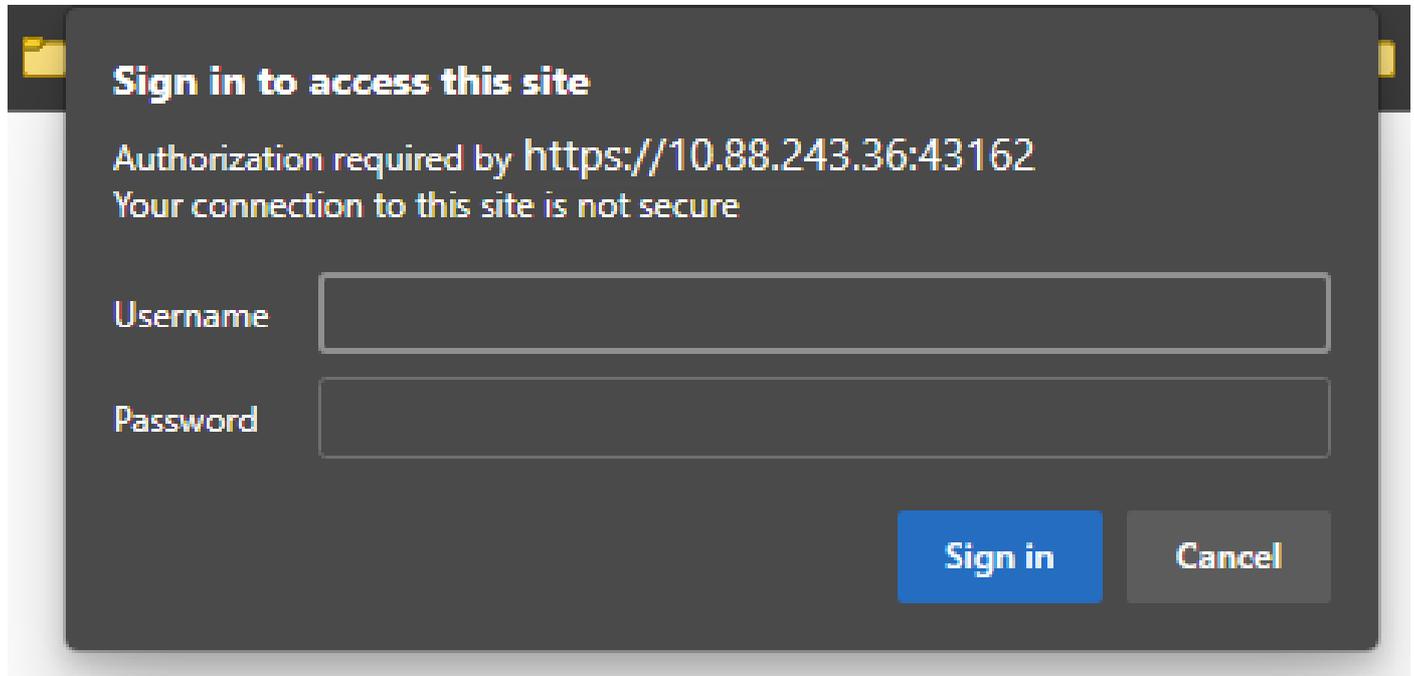
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Navigation durch FMC API-Explorer überprüfen

Um auf den FMC API Explorer zuzugreifen, navigieren Sie zur nächsten URL:

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

Sie müssen sich mit denselben Anmeldeinformationen anmelden, die auch für die FMC-GUI verwendet werden. Diese Anmeldeinformationen werden in einem Fenster eingegeben, das dem nächsten ähnelt, wenn Sie die API-Explorer-URLs eingeben.



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**

Nach der Anmeldung wird deutlich, dass die API-Abfragen nach Kategorien unterteilt sind, die den möglichen Aufrufen entsprechen, die Sie mithilfe von APIs durchführen können.



Hinweis: Nicht alle über die GUI oder CLI verfügbaren Konfigurationsfunktionen sind über die APIs verfügbar.

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

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 >

Wenn Sie auf eine Kategorie klicken, wird sie erweitert und zeigt Ihnen die verschiedenen Aufrufe an, die für diese Kategorie verfügbar sind. Diese Aufrufe werden zusammen mit den jeweiligen REST-Methoden und dem URI (Universal Resource Identifier) dieses Aufrufs angezeigt.

- 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}

Im nächsten Beispiel fordern Sie an, die im FMC konfigurierten Zugriffsrichtlinien anzuzeigen. Klicken Sie auf die entsprechende Methode, um sie zu erweitern, und klicken Sie dann auf die Schaltfläche "Try it out".

Hervorzuheben ist, dass Sie Ihre Abfragen mit den verfügbaren Parametern in jedem API-Aufruf parametrisieren können. Nur solche mit roten Sternchen sind obligatorisch, die anderen können

leer gelassen werden.

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

Die domainUUID ist beispielsweise für alle API-Aufrufe obligatorisch, wird jedoch im API-Explorer automatisch ausgefüllt.

Als Nächstes klicken Sie auf Ausführen, um diesen Anruf zu tätigen.

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

Execute

Bevor Sie auf "Ausführen" klicken, werden Ihnen Beispiele von Antworten auf die Anrufe angezeigt, um einen Eindruck davon zu erhalten, welche Antworten Sie erhalten können, je nachdem, ob die Anfrage richtig ist oder nicht.

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

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"
      }
    }
  ]
}

```

Nachdem der API-Aufruf ausgeführt wurde, erhalten Sie zusammen mit der Antwortnutzlast den Antwortcode. In diesem Fall 200, was einer OK-Anfrage entspricht. Sie erhalten auch die cURL und die URL des Aufrufs, den Sie gerade getätigt haben. Diese Informationen sind nützlich, wenn Sie diesen Aufruf mit einem externen Client/einer externen Software tätigen möchten.

Die erhaltene Antwort gibt die im FMC konfigurierten ACPs zusammen mit ihrer Objekt-ID zurück. In diesem Fall werden diese Informationen im roten Feld im nächsten Bild angezeigt:

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

Diese objectID ist der Wert, den Sie in Aufrufen eingeben, die einen Verweis auf diesen ACP erfordern. Zum Beispiel, um eine Regel innerhalb dieses ACP zu erstellen.

Die URIs, die Werte zwischen geschweiften Klammern enthalten {}, sind Werte, die für diesen Aufruf erforderlich sind. Denken Sie daran, dass domainUUID der einzige Wert ist, der automatisch gefüllt wird.

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

Die für diese Aufrufe erforderlichen Werte sind in der Aufrufbeschreibung angegeben. Um Regeln für einen ACP zu erstellen, benötigen Sie die policy-ID, wie im nächsten Bild zu sehen ist:

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).	

Diese policyID wird in das als containerUUID angegebene Feld eingegeben. Ein weiteres erforderliches Feld für POST-Methoden ist der Payload- oder Anforderungstext. Anhand der Beispiele können Sie Ihre Anforderungen anpassen.

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",

```

Beispiel für eine geänderte Nutzlast:

```
{ "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" ] }
```



Hinweis: Die verfügbaren Zonen können zusammen mit ihren IDs mit der nächsten Abfrage abgerufen werden.

GET

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

Wenn Sie den vorherigen Aufruf ausführen, erhalten Sie einen Antwortcode 201, der angibt, dass die Anforderung erfolgreich war und zur Erstellung der Ressource geführt hat.

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": [

```

Schließlich müssen Sie eine Bereitstellung vornehmen, damit diese Änderungen in der FTD wirksam werden, deren ACP geändert wurde.

Dazu müssen Sie eine Liste der Geräte abrufen, für die Änderungen bereitgestellt werden können.

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

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

Das Beispiel enthält ein Gerätepaar, das in Hochverfügbarkeit konfiguriert ist. Sie müssen die ID dieser HA erhalten. Wenn Sie ein eigenständiges Gerät sind, müssen Sie die ID dieses Geräts erhalten.

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
  }
}
```

Die Abfrage, die zum Abrufen der Geräte-ID der HA erforderlich ist, lautet wie folgt:

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.

Mit der Geräte-ID und der Bereitstellungsversionsnummer können Sie die Nutzlast des nächsten Anrufbeispiels ändern, um den Anruf für diese Bereitstellung zu tätigen.

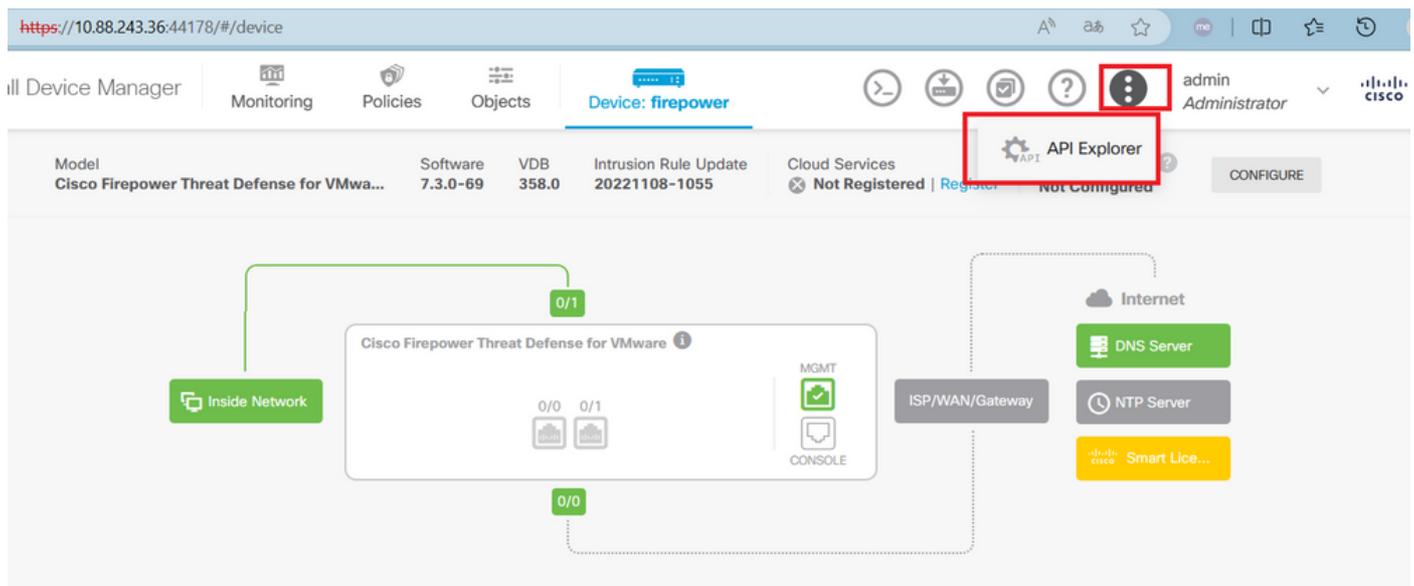
POST /api/fmc_config/v1/domain/{domainUUID}/deployment/deploymentrequests

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

Sobald dieser Aufruf ausgeführt wird, wenn alles korrekt ist, erhalten Sie eine Antwort mit Code 202.

Navigation in FDM API Explorer überprüfen

Um auf den FDM API Explorer zuzugreifen, können Sie eine Schaltfläche auf der FDM-GUI verwenden, um direkt darauf zuzugreifen, wie im folgenden Bild gezeigt:



Sobald Sie den API Explorer aufgerufen haben, werden die Abfragen auch in Kategorien unterteilt.

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

Um eine Kategorie zu erweitern, müssen Sie auf sie klicken. Anschließend können Sie jede der Operationen durch Klicken auf eine der Kategorien erweitern. Das erste, was in jeder Operation gefunden wird, ist ein Beispiel für eine OK-Antwort für diesen Anruf.

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>

Als Nächstes sehen Sie die verfügbaren Parameter, mit denen Sie die Antworten auf Ihren Anruf beschränken können. Denken Sie daran, dass nur die als erforderlich markierten Felder für einen solchen Anruf erforderlich sind.

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

Schließlich finden Sie die möglichen Antwortcodes, die dieser Anruf zurückgeben kann.

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>						

Wenn Sie diesen Anruf tätigen möchten, klicken Sie auf **Try It Out**. Um diese Schaltfläche zu finden, müssen Sie nach unten blättern, bis Sie diese Schaltfläche finden, da sie sich am unteren Ende jedes Anrufs befindet.

```
internal_error_code": 0
}
```

520

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

TRY IT OUT!

Wenn Sie auf die Schaltfläche "Try It Out" klicken und es sich um einen Anruf handelt, für den keine weiteren Felder erforderlich sind, wird der Anruf sofort ausgeführt, und Sie erhalten eine Antwort.

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

Jeder Aufruf generiert einen HTTP-Antwortcode und einen Antworttext. So können Sie leichter erkennen, wo der Fehler liegt.

Der nächste Fehler tritt häufig auf, wenn die Sitzung abgelaufen ist. Er weist darauf hin, dass das Token ungültig ist, da es abgelaufen ist.

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

- Responses**: Header section.
- 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**: 401
 - Details**: Error: 401
 - Response body**:

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

Im Folgenden finden Sie Beispiele für HTTP-Antwortcodes, die Aufrufe zurückgeben können:

- Serie 2xx: Erfolg Es gibt mehrere Statuscodes: 200 (GET und PUT), 201 (POST), 202, 204 (DELETE). Sie zeigen einen erfolgreichen API-Aufruf an.
- 30x-Serie: Umleitung. Kann verwendet werden, wenn ein Client ursprünglich HTTP verwendet hat und zu HTTPS umgeleitet wurde.
- 4xx-Serie: Client-seitiger Fehler im API-Aufruf, der vom Client an den Server gesendet wurde. Zwei Beispiele umfassen einen 401-Statuscode, der angibt, dass die Sitzung nicht authentifiziert ist, und einen 403-Code, der einen unzulässigen Zugriffsversuch anzeigt.
- 5xx-Serie: Server-, Geräte- oder serviceseitiger Fehler. Dies kann daran liegen, dass der Geräte-API-Dienst deaktiviert wurde oder über das IP-Netzwerk nicht darauf zugegriffen werden kann.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.