

Dimostrare la navigazione attraverso Secure Firewall API-Explorer

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Esplorazione delle revisioni tramite Esplora FMC API](#)

[Esplora FDM API](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come esplorare Cisco FMC e Cisco FDM tramite l'API (Application Programming Interface).

Prerequisiti

Conoscenze base dell'API REST.

Requisiti

Per questa dimostrazione è necessario avere accesso all'interfaccia utente di Firepower Management Center (FMC) con almeno un dispositivo gestito da questo Firepower Management Center (FMC). Per la parte FDM di questa dimostrazione, è necessario disporre di un Firepower Threat Defense (FTD) gestito localmente per poter accedere alla GUI di FDM.

Componenti usati

- FMCv
- FTDv
- FTDv gestito localmente

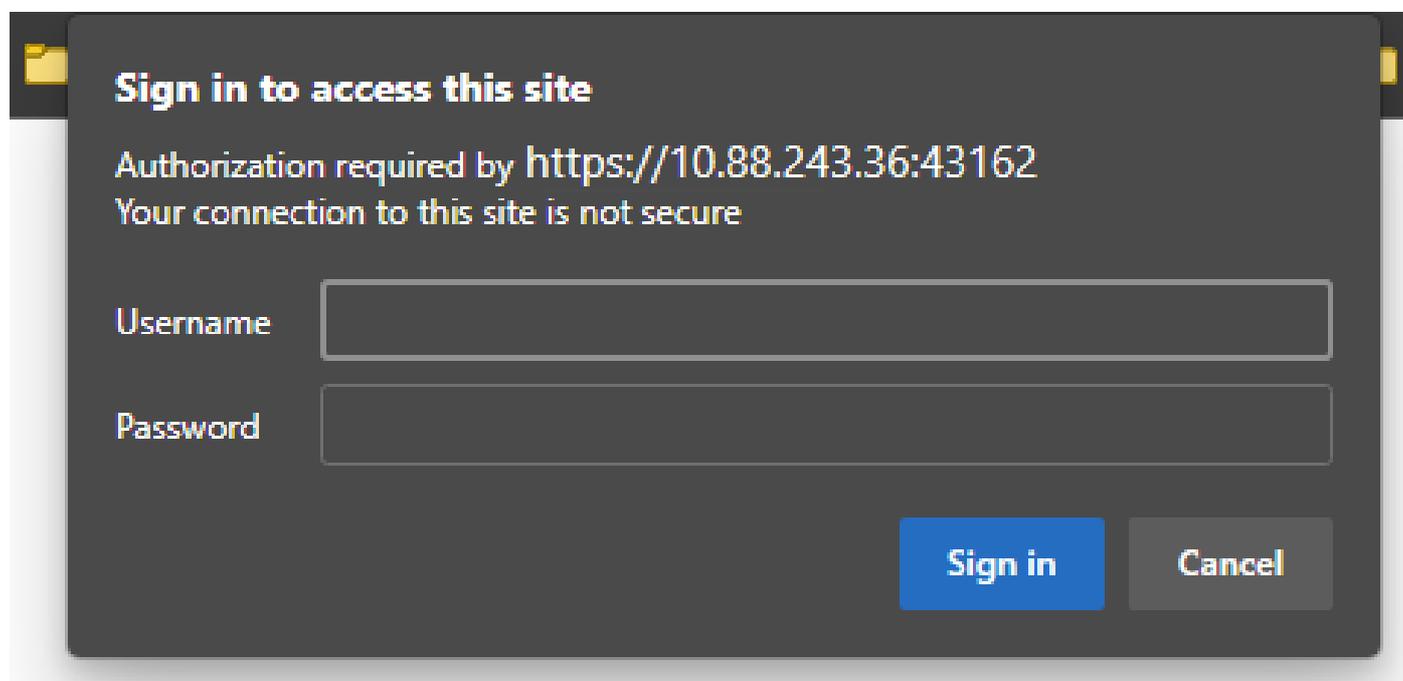
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esplora API di FMC

Per accedere a Esplora API di FMC, passare all'URL successivo:

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

È necessario eseguire l'accesso con le stesse credenziali utilizzate per l'interfaccia utente di FMC. Queste credenziali vengono immesse in una finestra simile a quella successiva quando si immettono gli URL di API Explorer.



Sign in to access this site

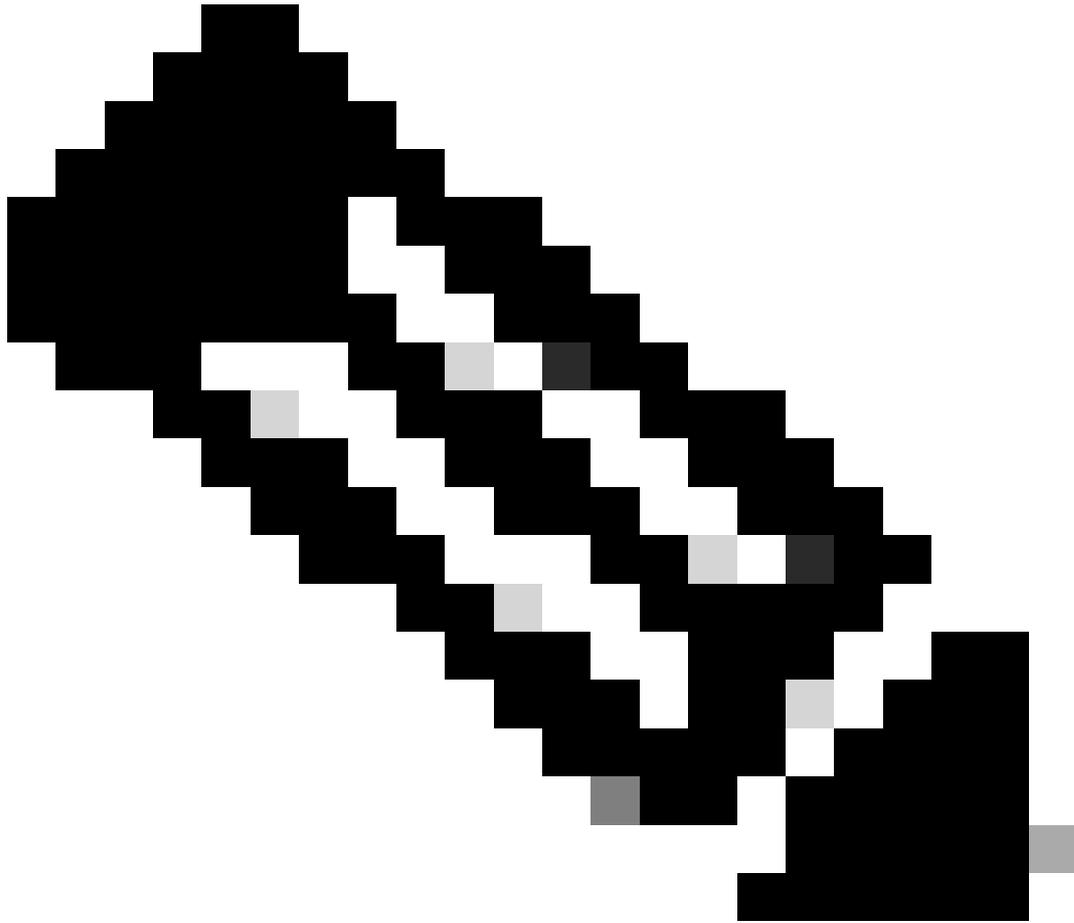
Authorization required by `https://10.88.243.36:43162`
Your connection to this site is not secure

Username

Password

Sign in **Cancel**

Una volta eseguito l'accesso, le query API vengono suddivise in categorie corrispondenti alle chiamate possibili che è possibile effettuare utilizzando le API.



Nota: non tutte le funzioni di configurazione disponibili dalla GUI o dalla CLI sono disponibili tramite le 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 >

Facendo clic su una categoria, si espande per visualizzare le diverse chiamate disponibili per questa categoria. Queste chiamate vengono visualizzate insieme ai rispettivi metodi REST e all'URI (Universal Resource Identifier) di quella chiamata.

- 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}

Nell'esempio seguente viene richiesta la visualizzazione dei criteri di accesso configurati nel FMC. Fare clic sul metodo corrispondente per espanderlo, quindi fare clic sul pulsante Prova.

È importante sottolineare che è possibile parametrizzare le query con i parametri disponibili in ogni chiamata API. Sono obbligatori solo gli asterischi rossi, mentre gli altri possono essere lasciati vuoti.

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="--"/>

Ad esempio, il domainUUID è obbligatorio per tutte le chiamate API, ma in API Explorer viene riempito automaticamente.

Il passaggio successivo consiste nel fare clic su Esegui per effettuare questa chiamata.

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

Prima di fare clic su Esegui, è possibile visualizzare esempi di risposte alle chiamate per avere un'idea delle possibili risposte che è possibile ottenere a seconda che la richiesta sia corretta o meno.

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"
      }
    }
  ]
}

```

Una volta eseguita la chiamata API, si ottiene, insieme al payload della risposta, il codice di risposta. In questo caso, 200, che corrisponde a una richiesta OK. Riceverai anche l'URL cURL e l'URL della chiamata che hai appena fatto. Queste informazioni sono utili se si desidera effettuare la chiamata con un client/software esterno.

La risposta ottenuta restituisce i punti ACP configurati nel CCP insieme al relativo objectID. In questo caso, è possibile visualizzare queste informazioni nella casella rossa dell'immagine seguente:

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

ObjectID è il valore immesso nelle chiamate che richiedono un riferimento a questo punto ACP. Ad esempio, per creare una regola all'interno del punto ACP.

Gli URI che contengono valori tra parentesi graffe {0} sono valori necessari per eseguire questa chiamata. Tenere presente che domainUUID è l'unico valore che viene compilato automaticamente.

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

I valori necessari per queste chiamate sono specificati nella descrizione della chiamata. Per creare regole per un punto ACP, è necessario il policyID, come illustrato nell'immagine seguente:

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).	

Questo PolicyID viene immesso nel campo specificato come containerUUID. Un altro campo obbligatorio per i metodi POST è il payload o il corpo della richiesta. È possibile utilizzare gli esempi forniti per apportare modifiche in base alle proprie esigenze.

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",

```

Esempio di payload modificato:

```
{ "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: è possibile ottenere le zone disponibili e i relativi ID utilizzando la query successiva.

GET

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

Dopo aver eseguito la chiamata precedente, si ottiene un codice di risposta 201, che indica che la richiesta è stata completata e che ha portato alla creazione della risorsa.

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": [
```

Infine, per rendere effettive le modifiche nell'FTD di cui è stato modificato il punto ACP, è necessario eseguire una distribuzione.

A tale scopo, è necessario ottenere l'elenco dei dispositivi con modifiche pronte per la distribuzione.

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

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

L'esempio contiene una coppia di dispositivi configurati in Alta disponibilità. È necessario ottenere l'ID di questa HA. Se si tratta di un dispositivo autonomo, è necessario ottenere l'ID di tale 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
  }
}
```

La query necessaria per ottenere l'ID dispositivo dell'HA è la seguente:

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.

Con l'ID dispositivo e il numero di versione della distribuzione, è possibile modificare il payload dell'esempio di chiamata successivo per effettuare la chiamata per eseguire questa distribuzione.

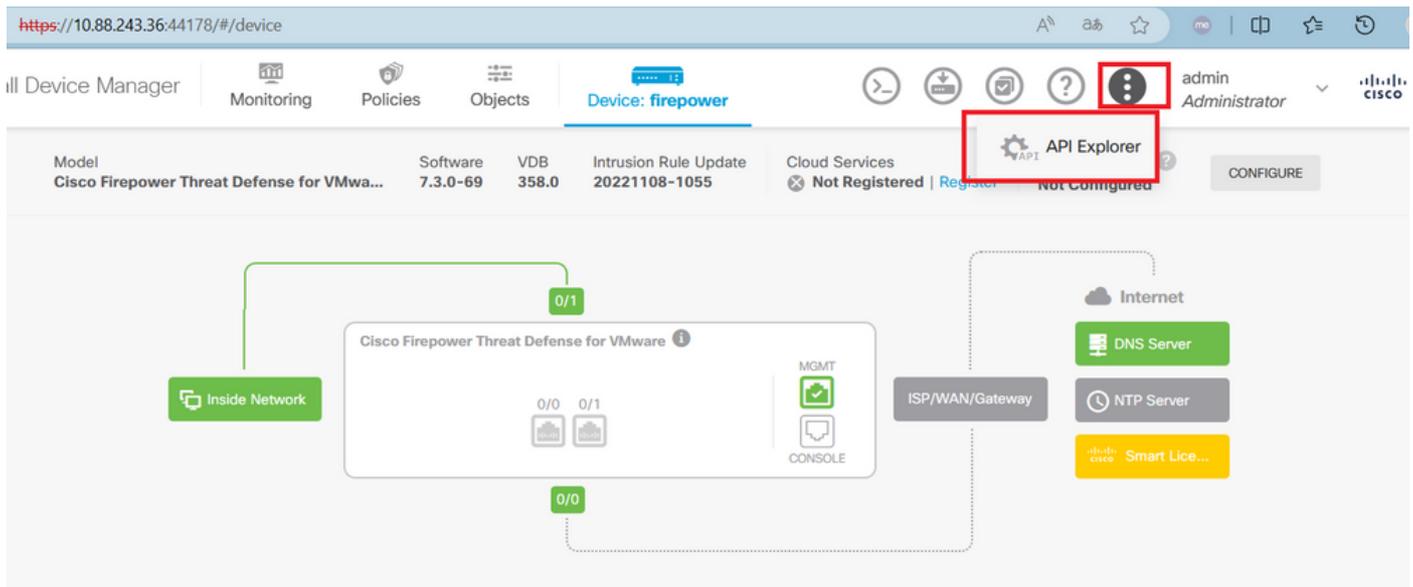
POST /api/fmc_config/v1/domain/{domainUUID}/deployment/deploymentrequests

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

Una volta eseguita questa chiamata, se tutto è corretto, si ottiene una risposta con il codice 202.

Esplorazione delle revisioni tramite Esplora API di FDM

Per accedere a FDM API Explorer, è possibile utilizzare un pulsante sull'interfaccia utente di FDM per passare direttamente a esso, come mostrato nell'immagine seguente:



Una volta in API Explorer, si nota che le query sono anche divise in categorie.

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](#)

Per espandere una categoria, è necessario fare clic su di essa, quindi è possibile espandere ogni operazione facendo clic su una di esse. La prima cosa che si trova all'interno di ciascuna operazione è un esempio di risposta OK per questa chiamata.

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>

Di seguito vengono visualizzati i parametri disponibili per vincolare le risposte della chiamata effettuata. Ricorda che solo i campi contrassegnati come obbligatori sono obbligatori per effettuare una chiamata di questo tipo.

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

Infine, è possibile trovare i possibili codici di risposta restituibili da questa chiamata.

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>						

Se si desidera effettuare questa chiamata, è necessario fare clic su **Prova**. Per trovare questo pulsante, è necessario scorrere verso il basso fino a trovare questo pulsante poiché si trova nella parte inferiore di ogni chiamata.

520

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

TRY IT OUT

Quando si fa clic sul pulsante Prova, se la chiamata non richiede altri campi, viene eseguita immediatamente e viene fornita la risposta.

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

Risoluzione dei problemi

Ogni chiamata genera un codice di risposta HTTP e un corpo di risposta. Ciò consente di identificare la posizione dell'errore.

L'errore seguente si verifica quando la sessione è scaduta e indica che il token non è valido perché è scaduto.

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

- Responses**: The main header of the interface.
- 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 the code `401` and the detail `Error: 401`. Both the code and detail cells are highlighted with a red border.
- 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 border.

Di seguito sono riportati alcuni esempi di codici di risposta HTTP che le chiamate possono restituire:

- Serie 2xx: successo. Sono disponibili diversi codici di stato: 200 (GET e PUT), 201 (POST), 202, 204 (DELETE). Indicano una chiamata API riuscita.
- Serie 30x: Redirection. Può essere utilizzato quando un client originariamente utilizzava HTTP e veniva reindirizzato a HTTPS.
- Serie 4xx: errore lato client nella chiamata API inviata dal client al server. Due esempi includono un codice di stato 401, che indica che la sessione non è autenticata, e un codice 403, che indica un tentativo di accesso vietato.
- Serie 5xx: errore di server, dispositivo o lato servizio. La causa potrebbe essere la disabilitazione del servizio API del dispositivo o l'inaccessibilità della rete IP

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).