

Secure Firewall의 API-Explorer를 통한 탐색 시연

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[FMCAPI 탐색기를 통한 탐색 검토](#)

[FDMAPI 탐색기를 통한 탐색 검토](#)

[문제 해결](#)

소개

이 문서에서는 Cisco FMC 및 Cisco FDM의 API(응용 프로그래밍 인터페이스) 탐색기를 통한 탐색에 대해 설명합니다.

사전 요구 사항

REST API에 대한 기본 이해

요구 사항

이 데모에서는 이 FMC(Firepower 관리 센터)에서 관리하는 하나 이상의 디바이스가 있는 FMC(Firepower 관리 센터) GUI에 액세스해야 합니다. 이 데모의 FDM 파트에서는 로컬에서 관리되는 FTD(Firepower Threat Defense)가 있어야 FDM GUI에 액세스할 수 있습니다.

사용되는 구성 요소

- FMCv
- FTDv
- FTDv 로컬 관리

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

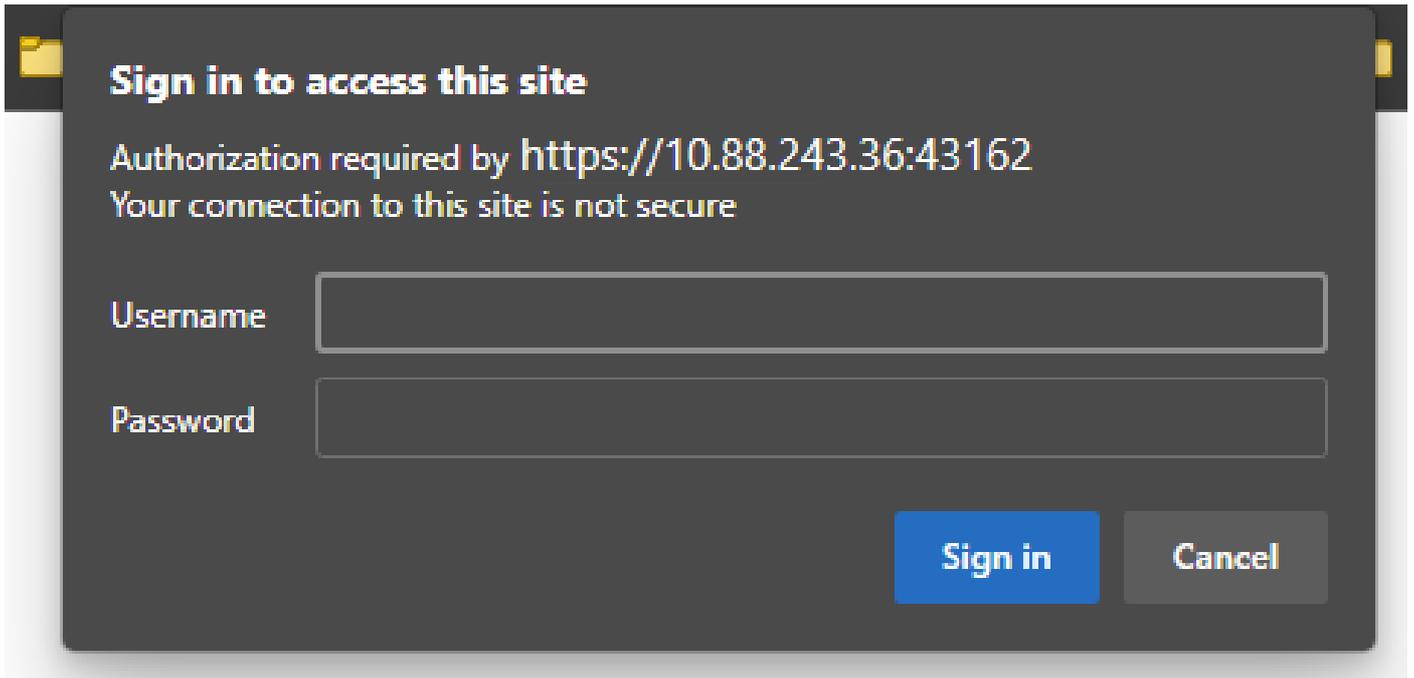
FMC API 탐색기를 통한 탐색 검토

FMC API 탐색기에 액세스하려면 다음 URL로 이동합니다.

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

FMC GUI에 사용된 것과 동일한 자격 증명으로 로그인해야 합니다. 이러한 자격 증명은 API 탐색기

URL을 입력할 때 다음 자격 증명과 유사한 창에 입력됩니다.



Sign in to access this site

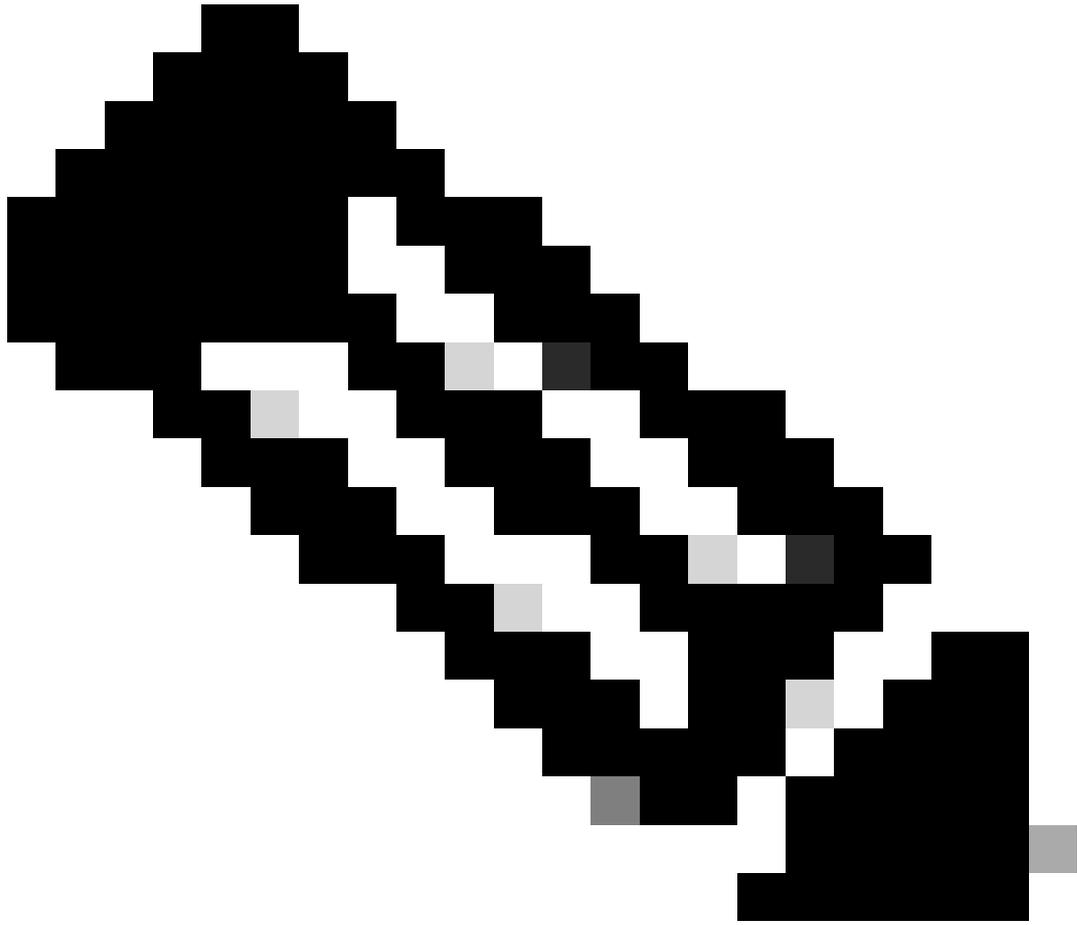
Authorization required by `https://10.88.243.36:43162`
Your connection to this site is not secure

Username

Password

Sign in **Cancel**

로그인하면 API 쿼리는 API를 사용하여 수행할 수 있는 호출에 해당하는 카테고리별로 구분됩니다.



참고: API를 통해 GUI 또는 CLI에서 사용할 수 있는 일부 컨피그레이션 기능은 사용할 수 없습니다.

The screenshot shows the Cisco Firewall Management Center Open API Specification page. The browser address bar shows the URL `https://10.88.243.36:43162/api/api-explorer/`. The page header includes the Cisco logo and links for 'Download OAS 2.0 Spec', 'Download OAS 3.0 Spec', and 'Logout'. The main heading is 'Cisco Firewall Management Center Open API Specification' with a '1.0.0 OAS3' badge. Below the heading, there is a description: '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.' There are also links for 'Cisco Technical Assistance Center (TAC) - Website', 'Send email to Cisco Technical Assistance Center (TAC)', and 'Cisco Firewall Management Center Licensing'. A 'Domains' dropdown menu is set to 'Global'. A list of categories is shown with right-pointing chevrons: Troubleshoot, Backup, Network Map, Devices, Policy Assignments, Device HA Pairs, and Health.

카테고리를 클릭하면 해당 카테고리에 사용할 수 있는 다른 통화가 표시됩니다. 이러한 통화는 해당 REST 메서드 및 해당 통화의 URI(Universal Resource Identifier)와 함께 표시됩니다.

The screenshot shows the API Explorer interface with the 'Policy' category selected and highlighted with a red border. Below the category, several REST API methods are listed with their corresponding URIs and HTTP methods:

- 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}`

다음 예에서는 FMC에 구성된 액세스 정책을 확인하도록 요청합니다. 해당 방법을 클릭하여 확장한 다음 Try it out(테스트 실행) 버튼을 클릭합니다.

강조할 점은 각 API 호출에서 사용 가능한 매개 변수를 사용하여 쿼리를 매개 변수화할 수 있다는 것입니다. 빨간색 별표가 있는 사람만 필수 항목이고 나머지는 비워둘 수 있습니다.

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

예를 들어 domainUUID는 모든 API 호출에 필수이지만 API 탐색기에서는 자동으로 채워집니다. 다음 단계는 Execute(실행)를 클릭하여 이 통화를 수행하는 것입니다.

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

Execute

실행을 클릭하기 전에 통화에 대한 응답 예를 확인하여 요청이 정확한지 여부에 따라 얻을 수 있는 가능한 응답에 대해 알아볼 수 있습니다.

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"
      }
    }
  ]
}

```

API 호출이 실행되면 응답 페이로드와 함께 응답 코드를 얻습니다. 이 경우 200입니다. 이는 OK 요청에 해당합니다. 방금 건 통화의 cURL 및 URL도 가져옵니다. 이 정보는 외부 클라이언트/소프트웨어를 사용하여 이 통화를 하려는 경우에 유용합니다.

가져온 응답은 FMC에 구성된 ACP를 해당 objectID와 함께 반환합니다. 이 경우 다음 이미지의 빨간색 상자에서 이 정보를 볼 수 있습니다.

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

이 objectID는 이 ACP에 대한 참조가 필요한 통화에 입력하는 값입니다. 예를 들어, 이 ACP 내에서

규칙을 생성하려면 다음을 수행합니다.

중괄호 {} 사이의 값을 포함하는 URI는 이 호출을 수행하는 데 필요한 값입니다. domainUUID는 자동으로 채워지는 유일한 값입니다.

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

이러한 통화에 필요한 값은 통화 설명에 지정되어 있습니다. ACP에 대한 규칙을 생성하려면 다음 이미지에서 볼 수 있듯이 policyID가 필요합니다.

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).	

이 policyID는 containerUUID로 지정된 필드에 입력되며, POST 메서드에 또 다른 필수 필드는 페이로드 또는 요청 본문입니다. 제공된 예를 사용하여 요구 사항을 수정할 수 있습니다.

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",

```

수정된 페이로드의 예:

```
{ "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" ] }
```



참고: 사용 가능한 영역은 해당 ID와 함께 다음 쿼리를 사용하여 가져올 수 있습니다.

GET

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

이전 통화를 실행하면 201 응답 코드가 나타나며, 이는 요청이 성공하여 리소스를 생성했음을 나타냅니다.

```

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": [

```

마지막으로, ACP가 수정된 FTD에 이러한 변경 사항이 적용되도록 구축해야 합니다.

이를 위해서는 변경 사항을 구축할 준비가 된 장비 목록을 가져와야 합니다.

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

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

이 예에는 High Availability에 구성된 디바이스 쌍이 포함되어 있습니다. 이 HA의 ID를 가져와야 합니다. 독립형 디바이스인 경우 해당 디바이스의 ID를 가져와야 합니다.

```

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
  }
}

```

HA의 디바이스 ID를 가져오는 데 필요한 쿼리는 다음과 같습니다.

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.

디바이스 ID와 구축 버전 번호를 사용하여 다음 통화 예제의 페이로드를 수정하여 이 구축을 수행하기 위해 호출할 수 있습니다.

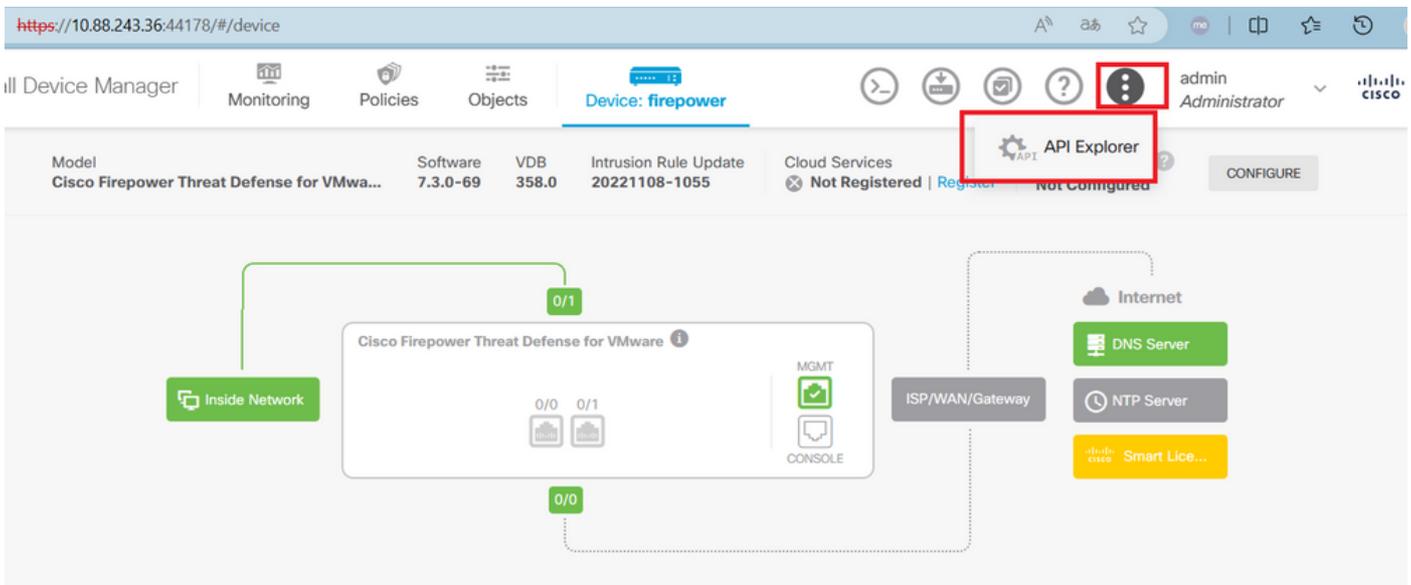
POST /api/fmc_config/v1/domain/{domainUUID}/deployment/deploymentrequests

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

이 호출이 실행되면 모든 것이 정확하면 코드 202로 응답을 받습니다.

FDM API 탐색기를 통한 탐색 검토

FDM API 탐색기에 액세스하려면 다음 이미지에 표시된 것처럼 FDM GUI의 버튼을 사용하여 직접 이동할 수 있습니다.



API 탐색기에서 쿼리는 카테고리로도 구분됩니다.

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

카테고리를 확장하려면 카테고리를 클릭해야 하며, 그런 다음 각 작업을 클릭하여 확장할 수 있습니다. 각 작업 내에서 가장 먼저 발견되는 것은 이 통화에 대한 OK 응답의 예입니다.

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>

다음으로 보이는 것은 통화의 응답을 제한하는 데 사용할 수 있는 매개변수입니다. 필수로 표시된 필드만 해당 통화를 수행하는 데 필수입니다.

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

마지막으로, 이 통화에서 반환할 수 있는 응답 코드를 찾습니다.

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>						

이 전화를 걸려면 **Try It Out**(테스트 아웃)을 클릭해야 합니다. 이 버튼은 각 통화의 맨 아래에 위치하므로 찾을 때까지 아래로 스크롤해야 이 버튼을 찾을 수 있습니다.

520

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

TRY IT OUT!

Try It Out(발신 시도) 버튼을 클릭하면 추가 필드가 필요하지 않은 통화인 경우 즉시 실행되며 응답이 제공됩니다.

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
```

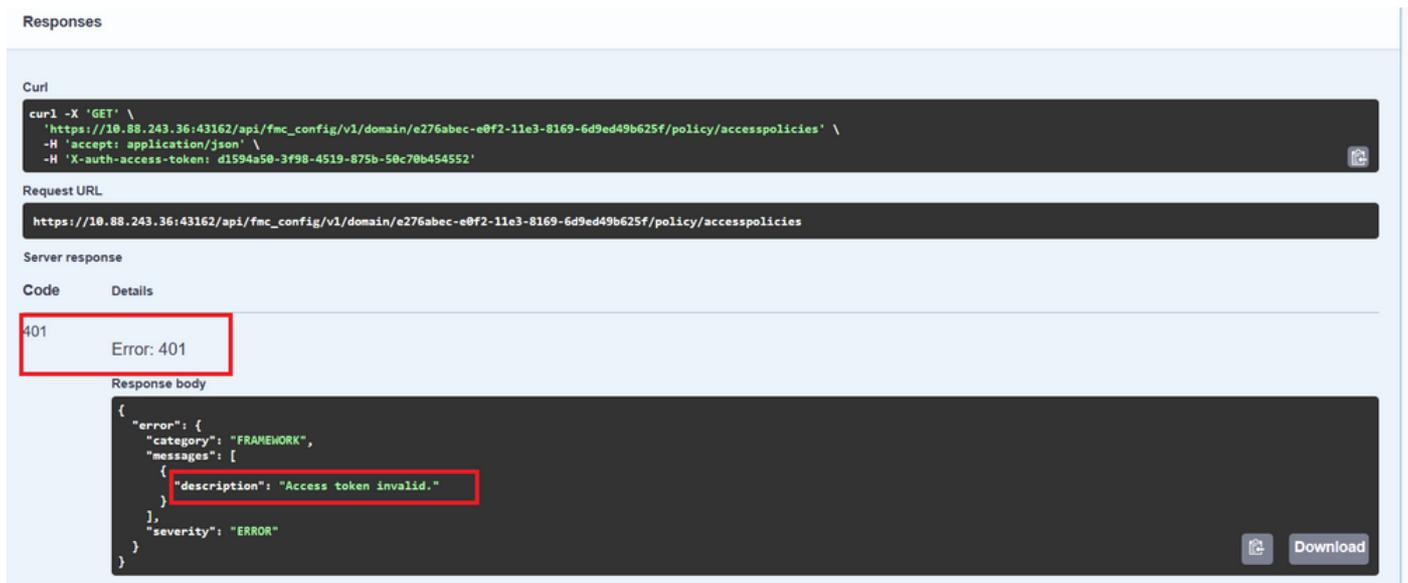
Response Body

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

문제 해결

각 호출은 HTTP 응답 코드 및 응답 본문을 생성합니다. 이렇게 하면 오류가 발생한 위치를 식별할 수 있습니다.

다음은 세션이 만료되었을 때 발생하는 일반적인 오류이며, 이는 토큰이 만료되었기 때문에 유효하지 않음을 나타냅니다.



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

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

Code	Details
401	Error: 401
- Response body:**

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

다음은 호출에서 반환할 수 있는 HTTP 응답 코드의 예입니다.

- 2xx 시리즈: 성공. 여러 상태 코드가 있습니다. 200(GET 및 PUT), 201(POST), 202, 204(DELETE). 이는 성공적인 API 호출을 나타냅니다.
- 30x 시리즈: 리디렉션. 클라이언트가 원래 HTTP를 사용하고 HTTPS로 리디렉션된 경우 사용할 수 있습니다.
- 4xx 시리즈: 클라이언트에서 서버로 전송된 API 호출의 클라이언트측 오류입니다. 두 가지 예로는 세션이 인증되지 않았음을 나타내는 401 상태 코드와 금지된 액세스 시도를 나타내는 403 코드가 있습니다.
- 5xx 시리즈: 서버, 디바이스 또는 서비스 측 오류입니다. 이는 디바이스 API 서비스가 비활성화되었거나 IP 네트워크를 통해 액세스할 수 없기 때문일 수 있습니다

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.