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

Table des matières

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

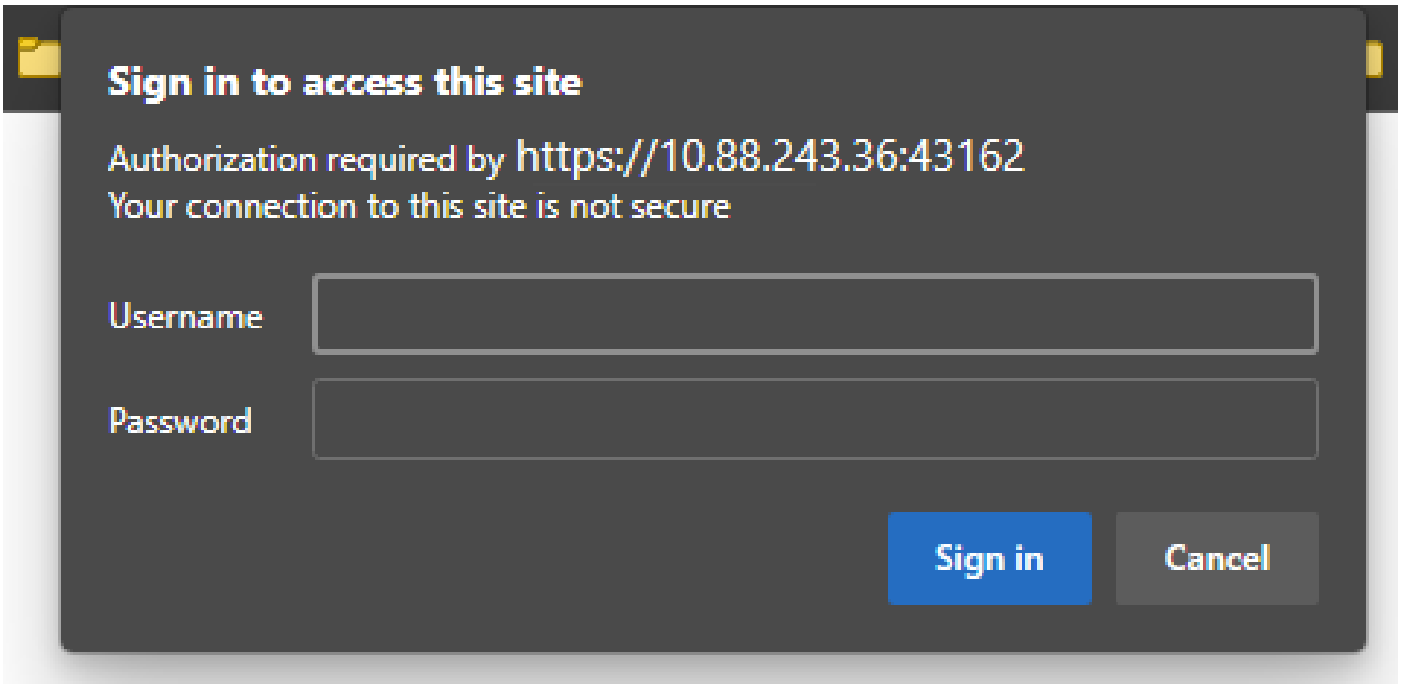
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Vérifier la navigation via l'Explorateur d'API FMC

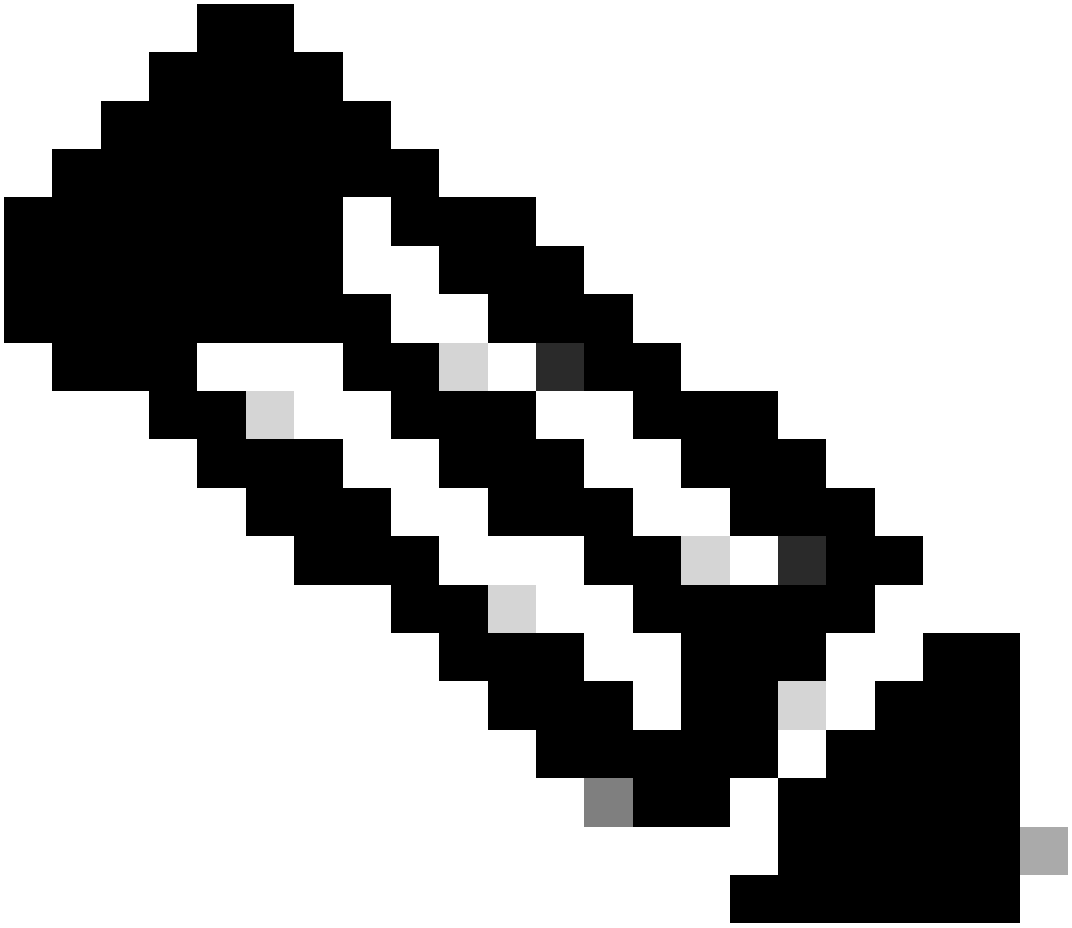
Pour accéder à l'explorateur d'API FMC, accédez à l'URL suivante :

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

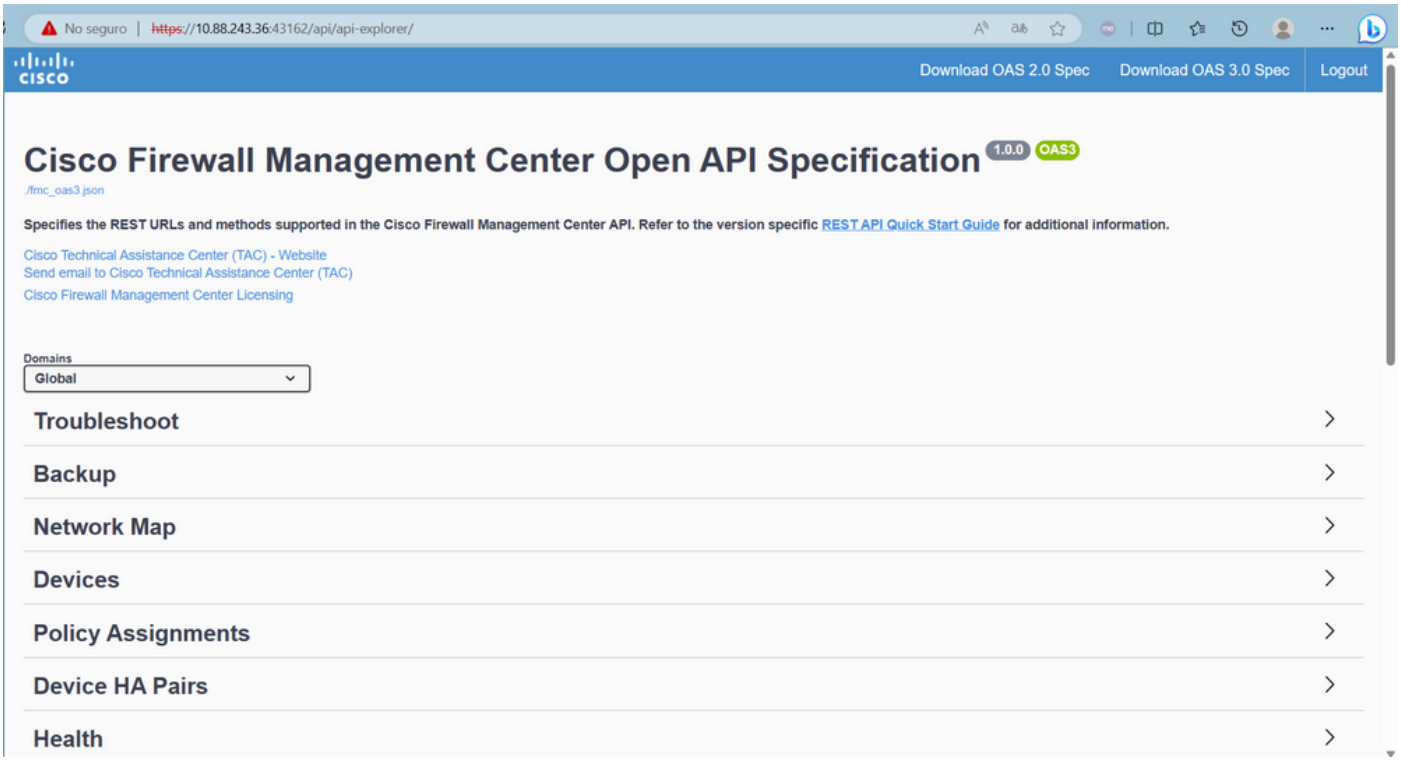
Vous devez vous connecter avec les mêmes informations d'identification que celles utilisées pour l'interface utilisateur graphique FMC. Ces informations d'identification sont entrées dans une fenêtre semblable à la suivante lorsque vous entrez les URL de l'explorateur d'API.



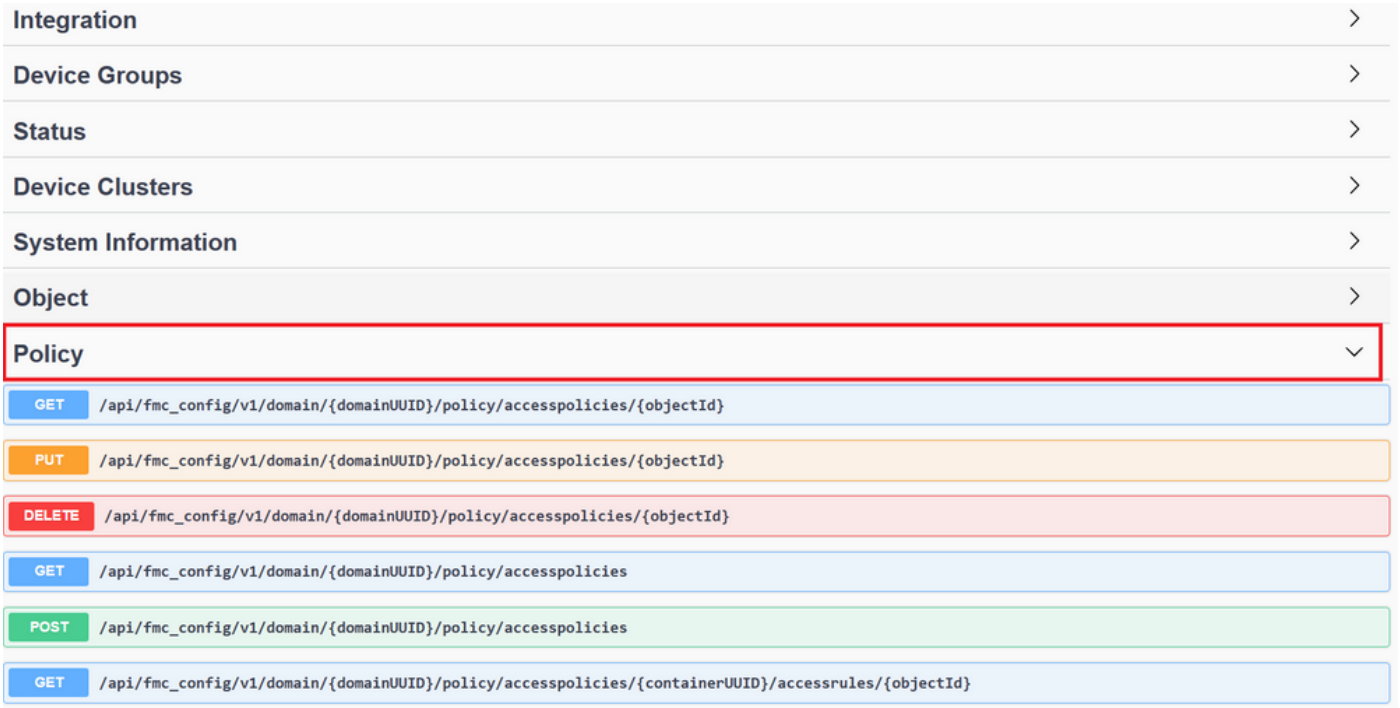
Une fois connectées, les requêtes API sont divisées en catégories correspondant aux appels possibles que vous pouvez effectuer à l'aide des API.



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.

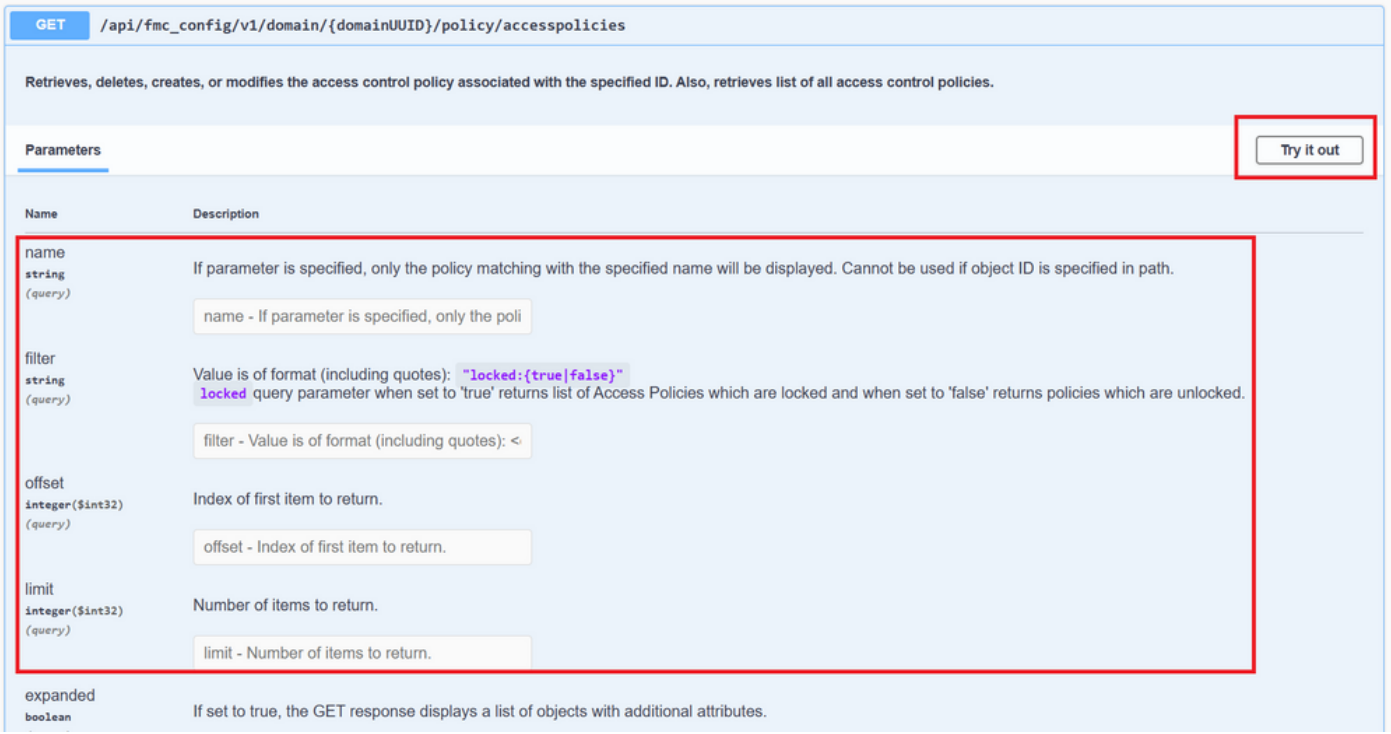


Lorsque vous cliquez sur une catégorie, elle se développe et vous affiche les différents appels disponibles pour cette catégorie. Ces appels sont affichés avec leurs méthodes REST respectives et l'URI (Universal Resource Identifier) de cet appel.



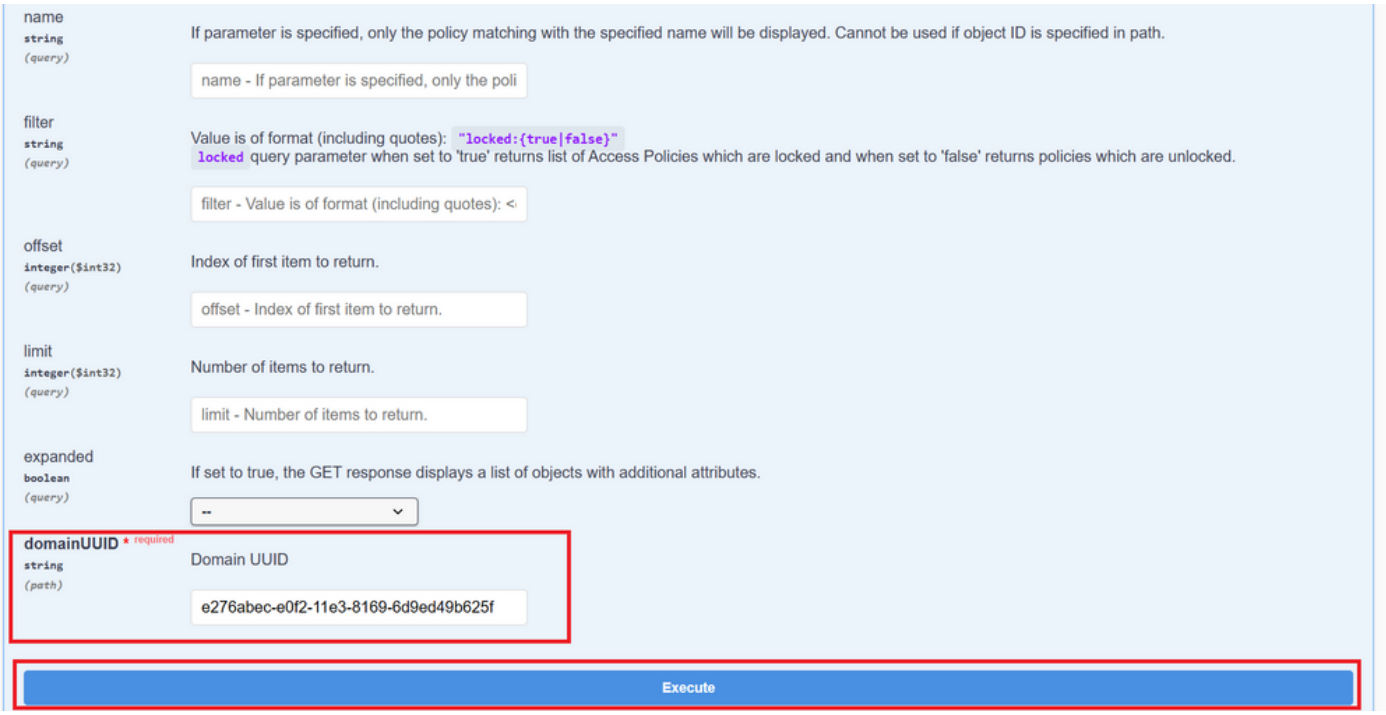
Dans l'exemple suivant, vous demandez à voir les stratégies d'accès configurées dans le FMC. Cliquez sur la méthode correspondante pour la développer, puis cliquez sur le bouton Try it out.

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.

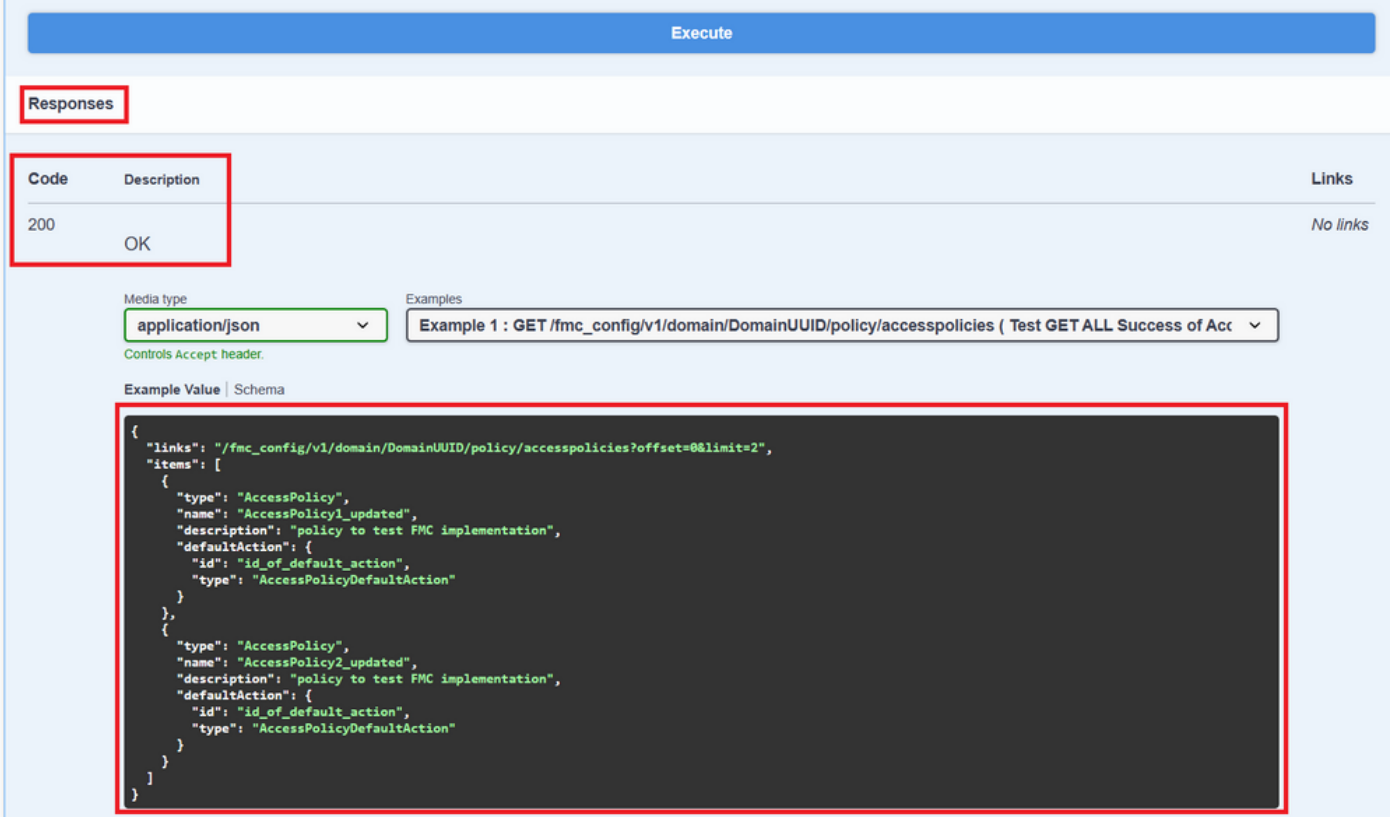


Par exemple, domainUUID est obligatoire pour tous les appels d'API, mais dans l'Explorateur d'API, il remplit automatiquement.

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

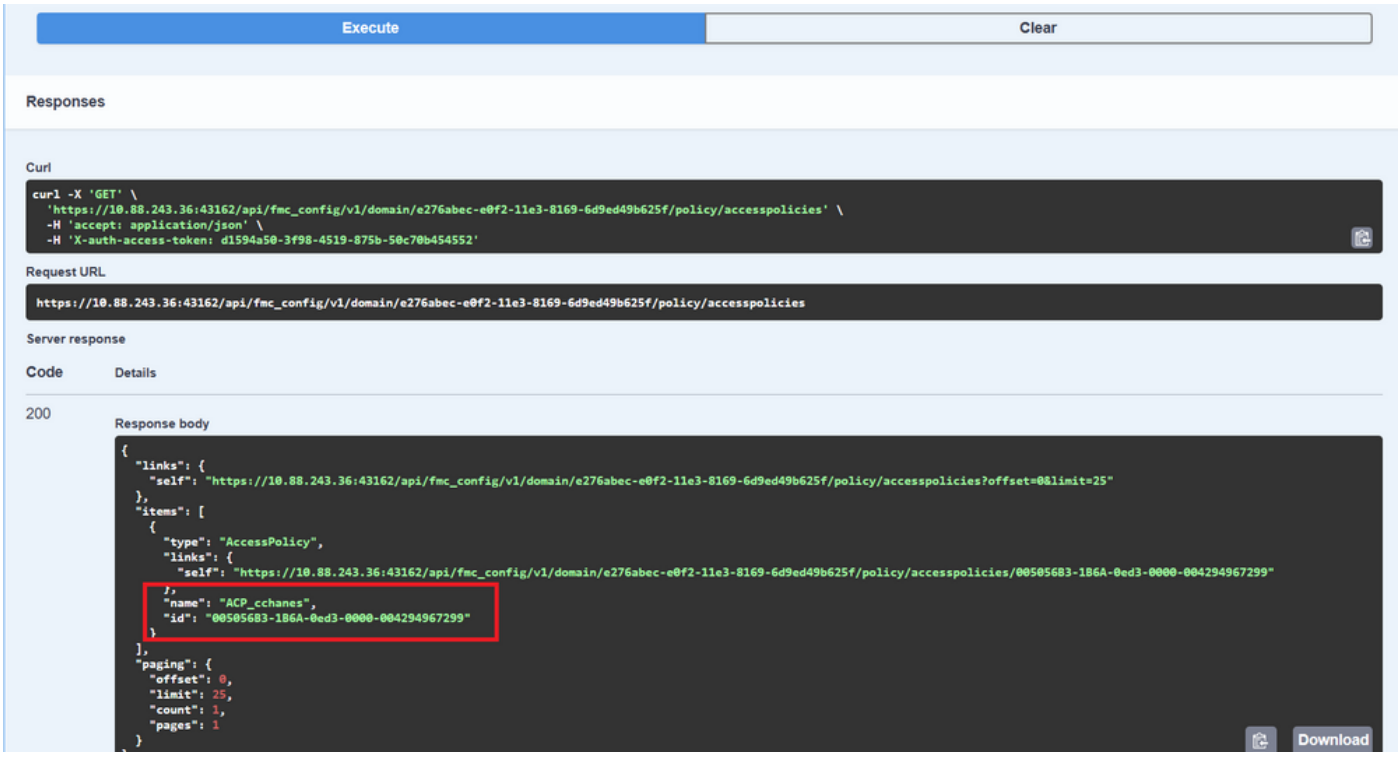


Avant de cliquer sur Exécuter, vous pouvez voir des exemples de réponses aux appels pour avoir une idée des réponses possibles que vous pouvez obtenir selon que la demande est correcte ou non.



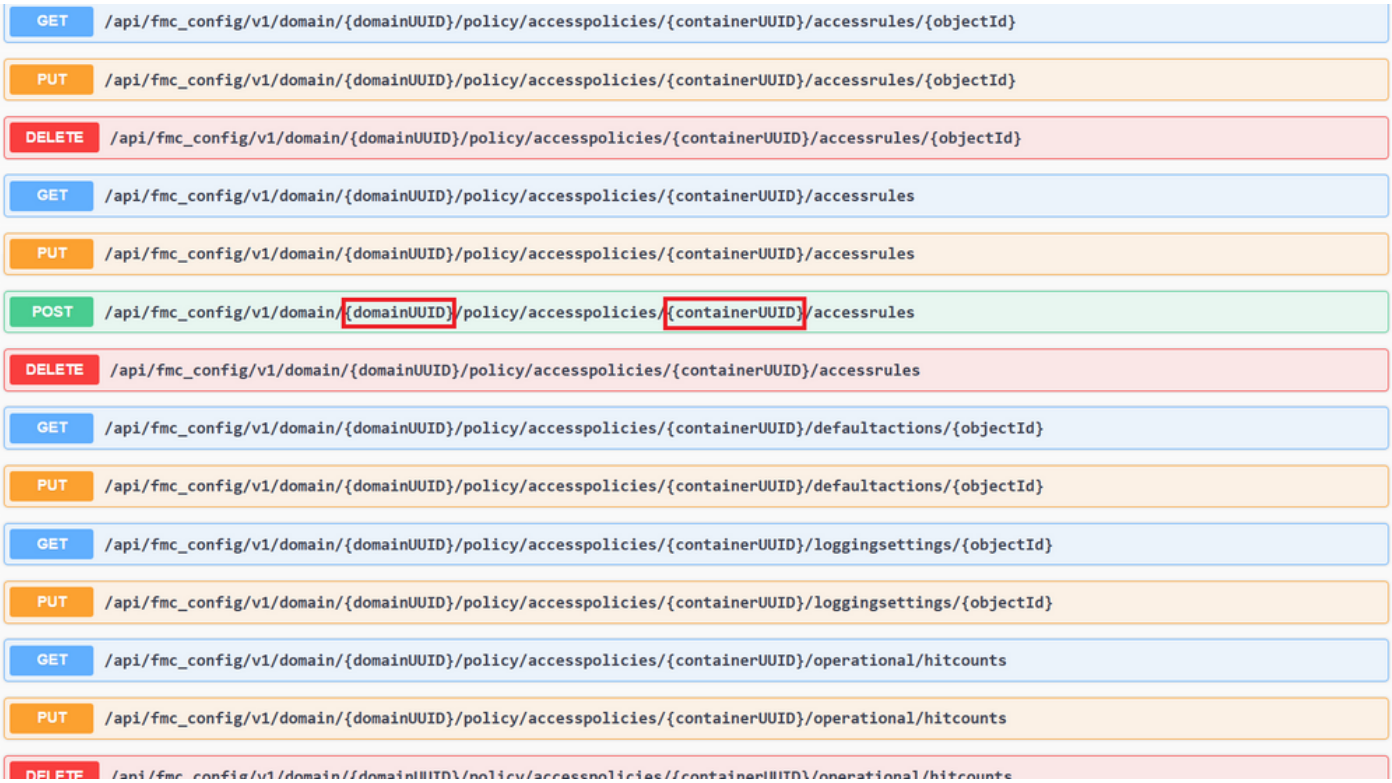
Une fois l'appel d'API exécuté, vous obtenez, avec la charge utile de réponse, le code de réponse. Dans ce cas 200, ce qui correspond à une requête OK. Vous obtenez également l'URLc et l'URL de l'appel que vous venez de passer. Ces informations sont utiles si vous souhaitez passer cet appel avec un client/logiciel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

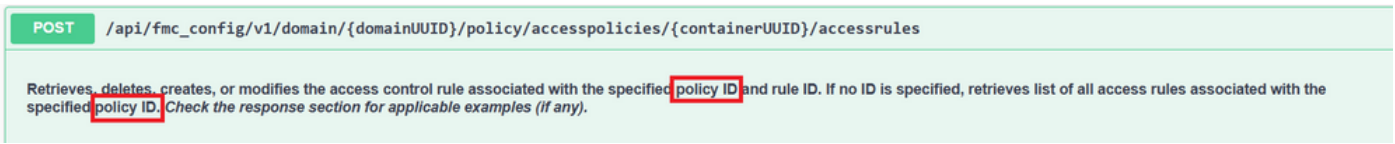


Cet objectID est la valeur que vous entrez dans les appels qui nécessitent une référence à cet ACP. Par exemple, pour créer une règle dans cet ACP.

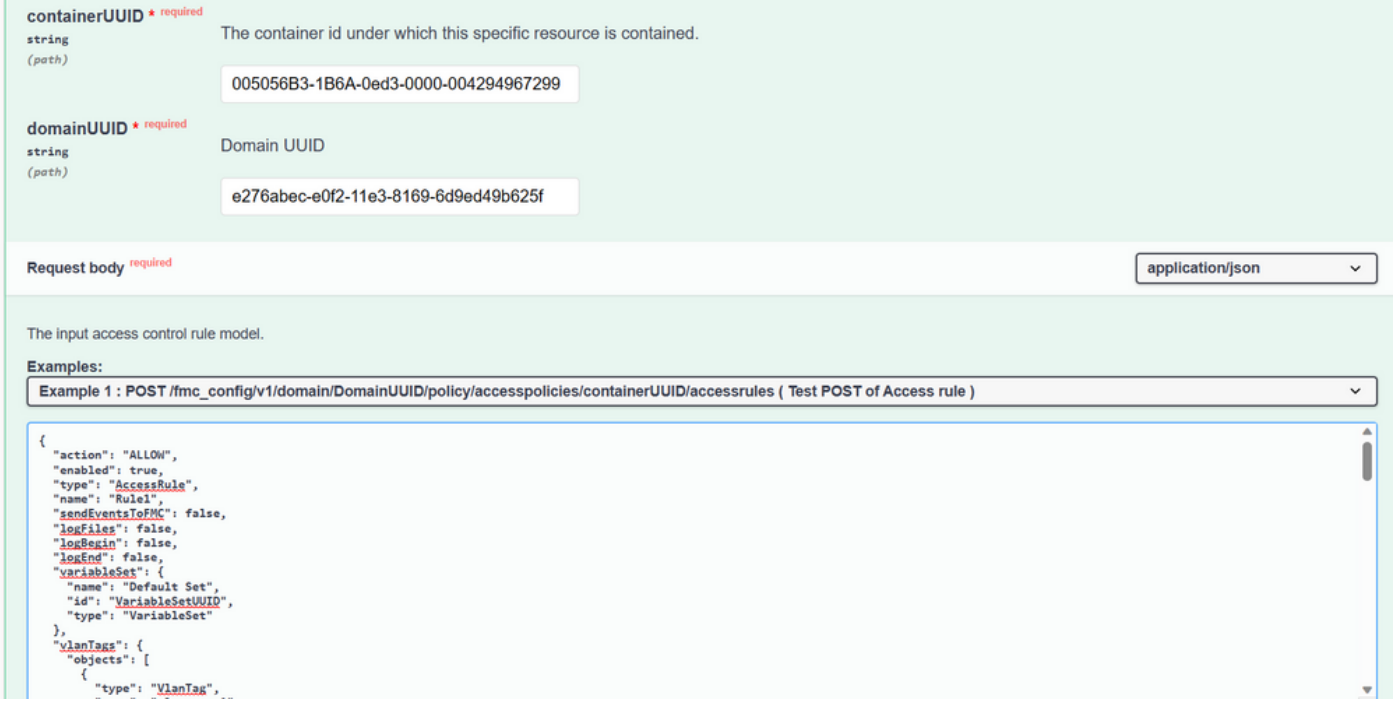
Les URI qui contiennent des valeurs entre accolades {} sont des valeurs requises pour effectuer cet appel. N'oubliez pas que domainUUID est la seule valeur qui est automatiquement remplie.



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 :

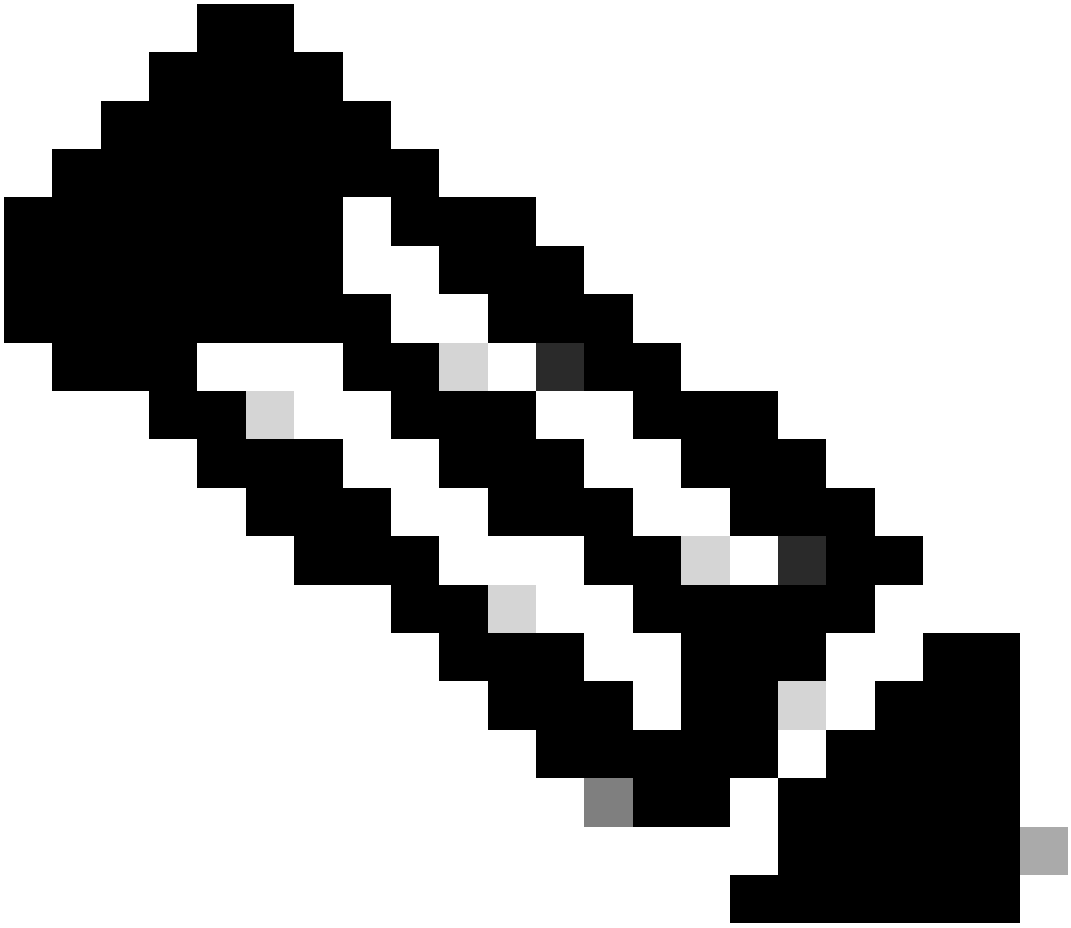


Ce policyID est entré dans le champ spécifié comme containerUID, un autre champ requis pour les méthodes POST est la charge utile ou le corps de la requête. Vous pouvez utiliser les exemples donnés pour modifier selon vos besoins.



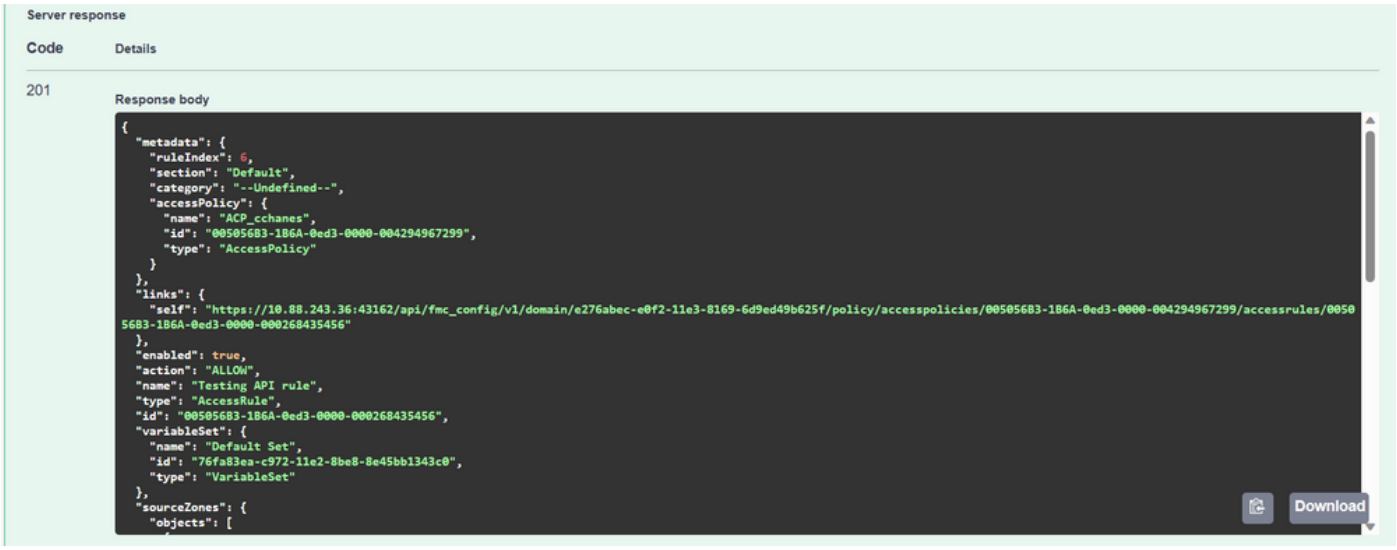
Exemple de charge utile modifiée :

{ "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"] }



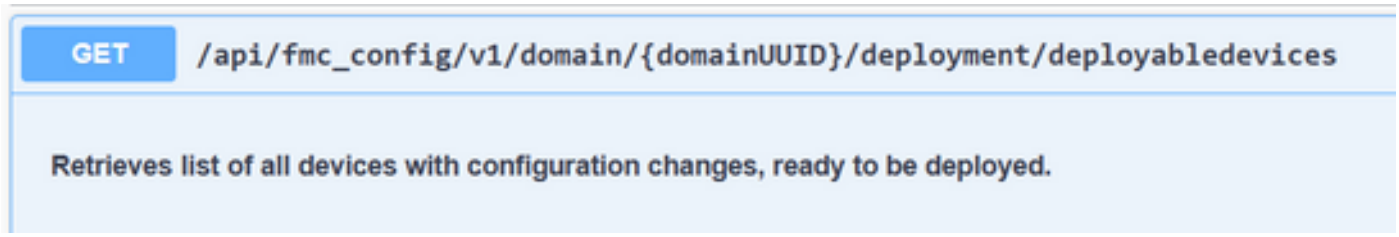
Remarque : les zones disponibles, ainsi que leurs ID, peuvent être obtenues à l'aide de la requête suivante.

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.

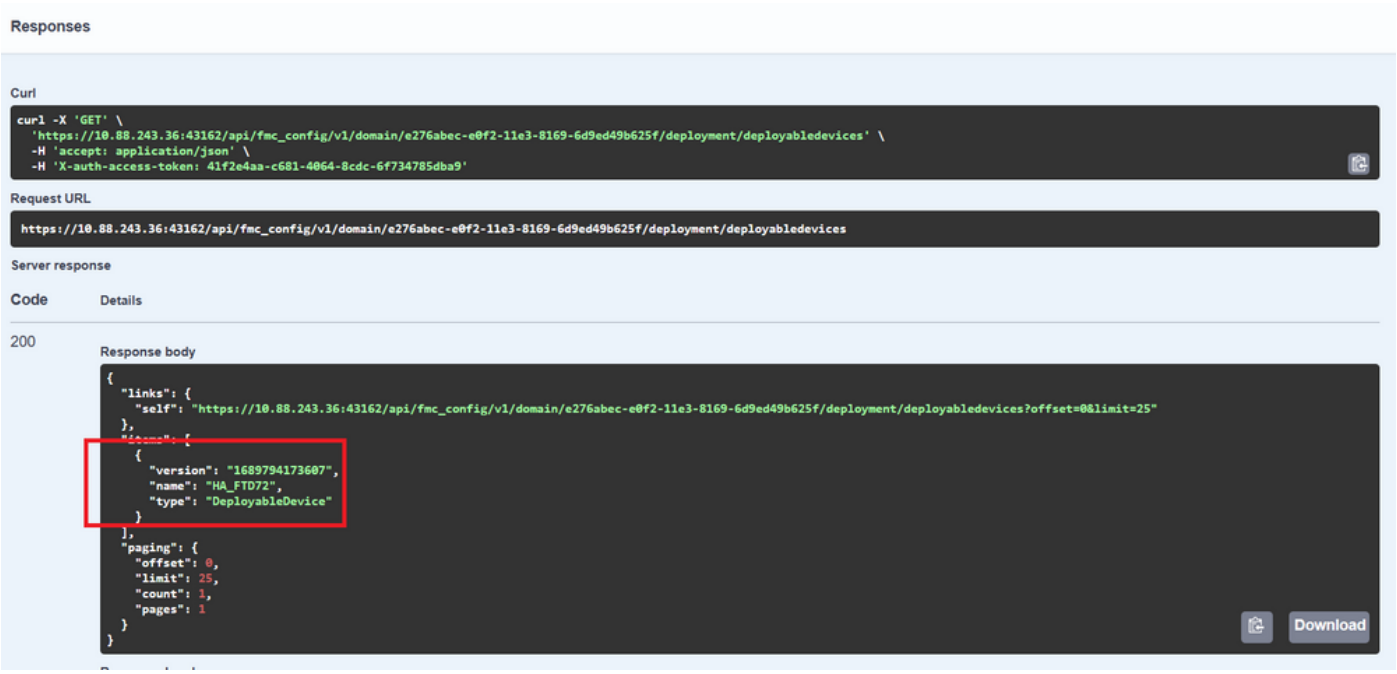


Enfin, vous devez effectuer un déploiement pour que ces modifications prennent effet dans le FTD dont l'ACP a été modifié.

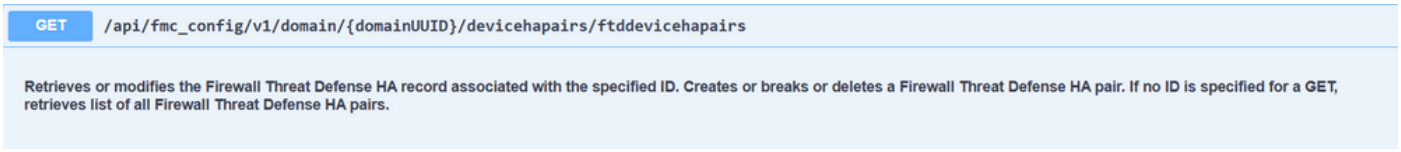
Pour cela, vous devez obtenir la liste des périphériques dont les modifications sont prêtes à être déployées.



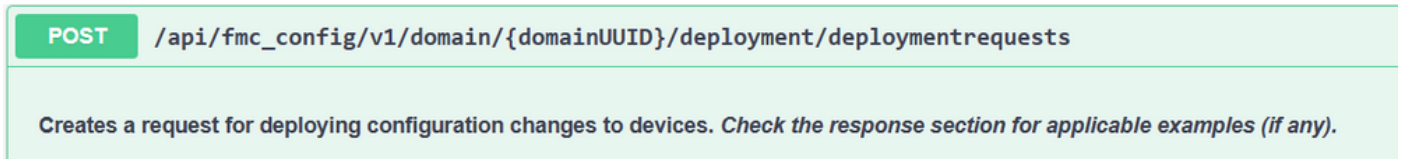
L'exemple contient une paire de périphériques configurés en haute disponibilité. Vous devez obtenir l'ID de cette haute disponibilité. Dans le cas d'un périphérique autonome, vous devez obtenir l'ID de ce périphérique.



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



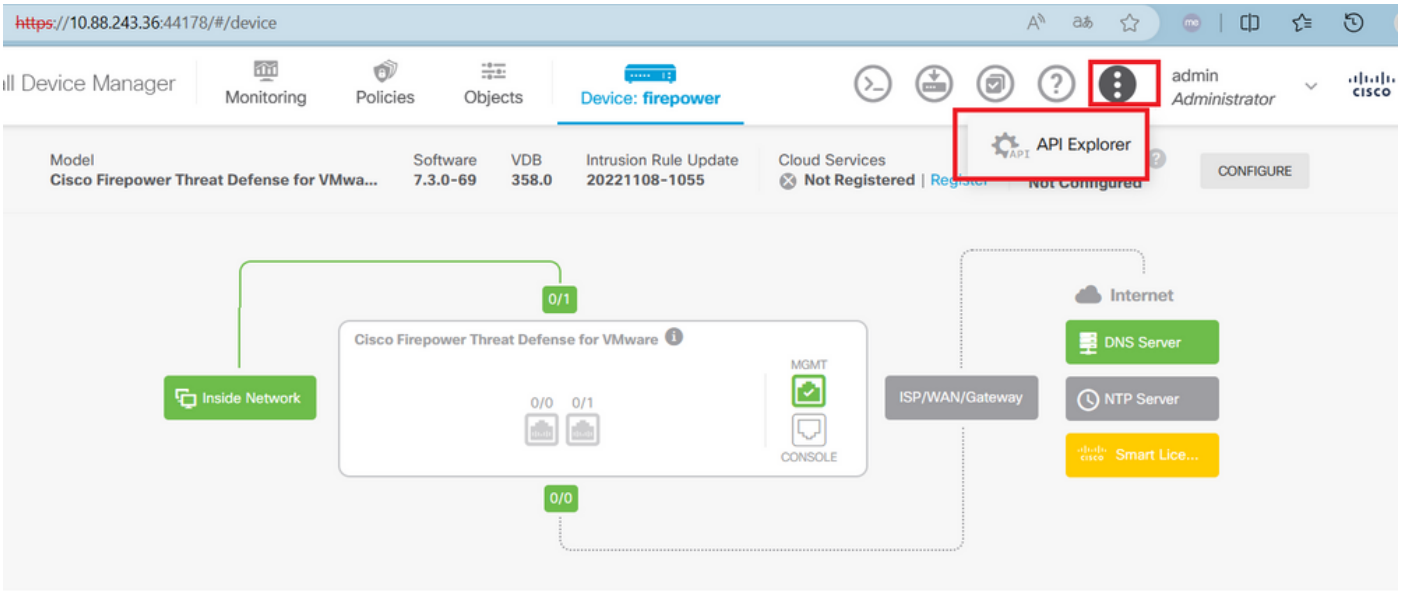
Avec l'ID de périphérique et le numéro de version du déploiement, vous pouvez modifier la charge utile de l'exemple d'appel suivant pour passer l'appel pour effectuer ce déploiement.



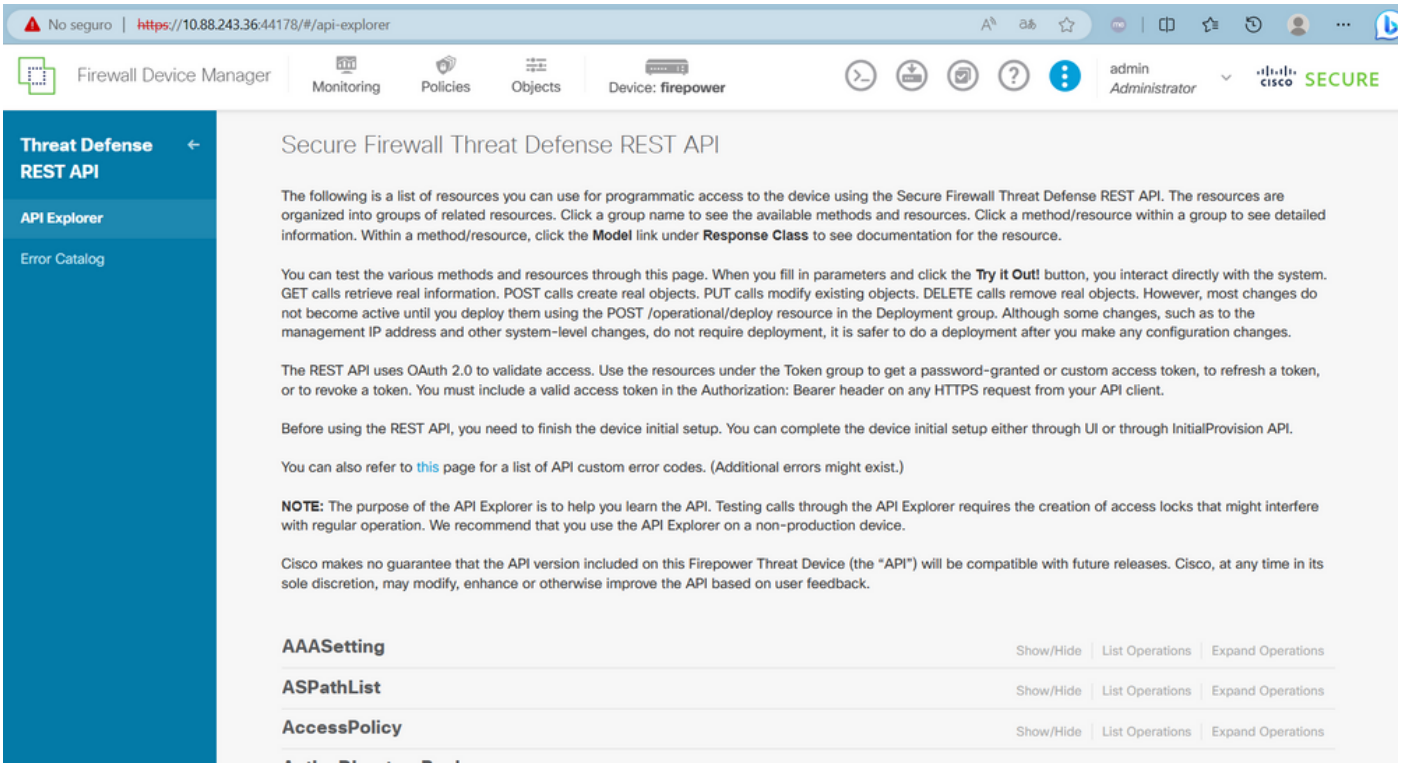
Une fois cet appel exécuté, si tout est correct, vous obtenez une réponse avec le code 202.

Vérifier la navigation via l'Explorateur d'API FDM

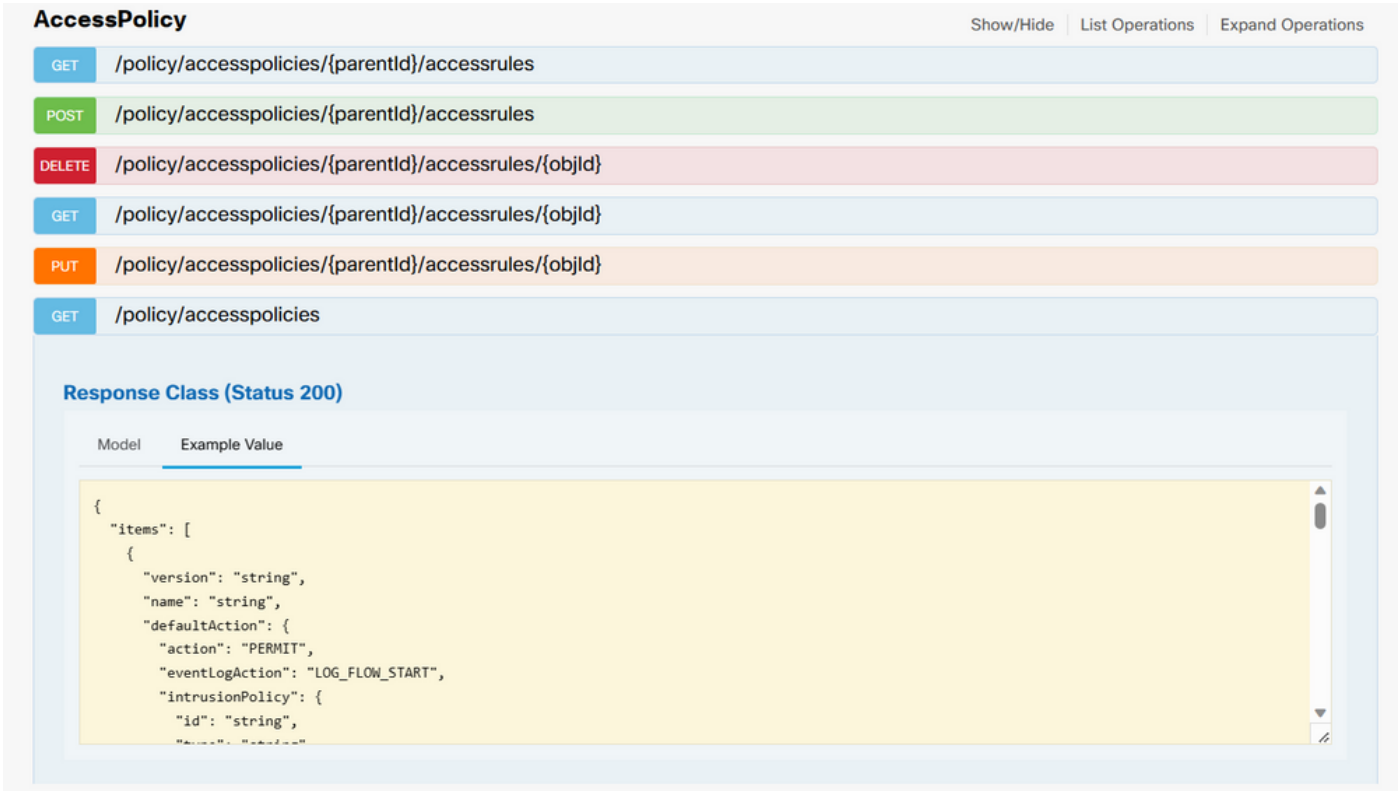
Pour accéder à l'explorateur d'API FDM, il est possible d'utiliser un bouton de l'interface utilisateur graphique FDM pour y accéder directement, comme illustré dans l'image suivante :



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



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.



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 application/json

Parameters

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

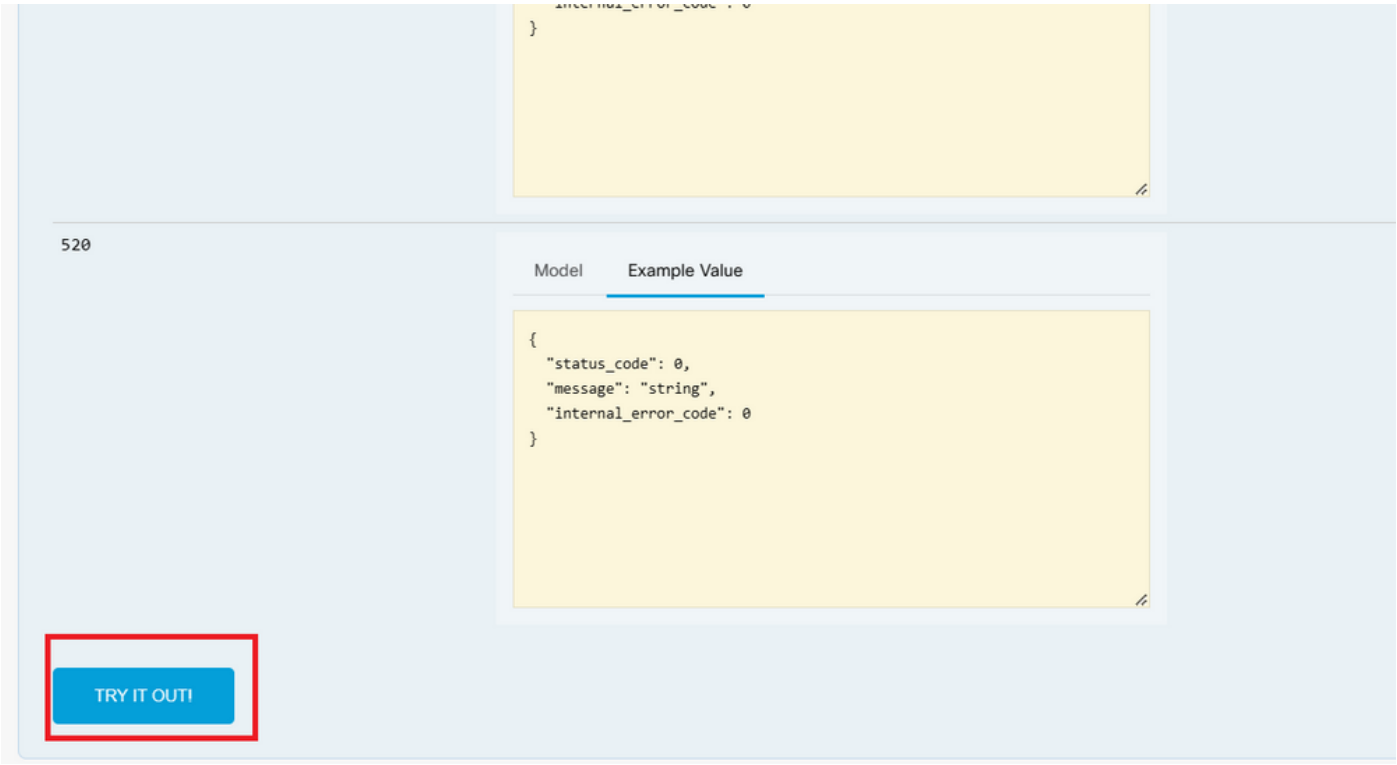
Enfin, vous trouverez les codes de réponse possibles que cet appel peut renvoyer.

Response Messages

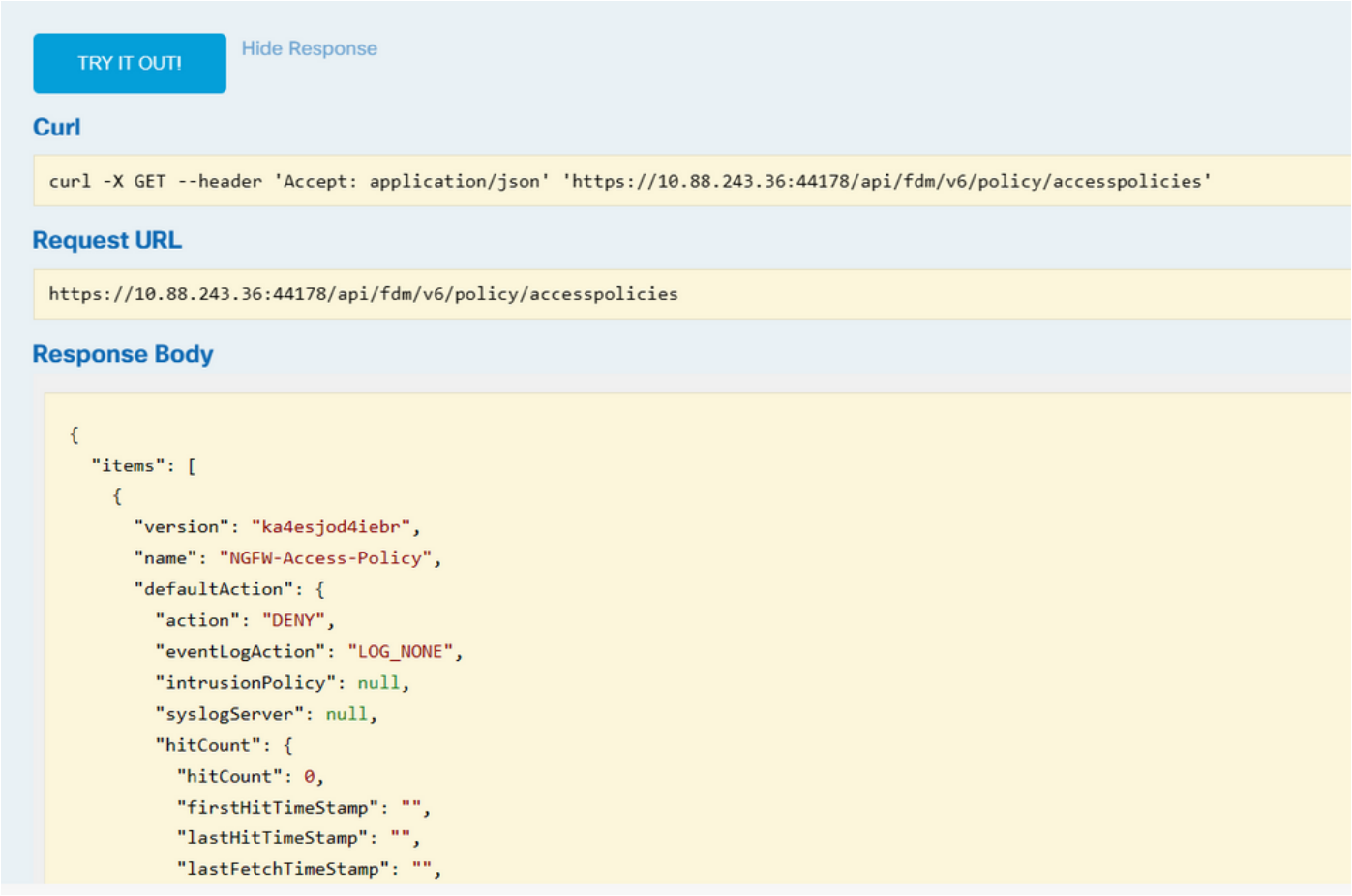
HTTP Status Code	Reason	Response Model	Headers
401		Model / Example Value	
403		Model / Example Value	

```
{
  "status_code": 0,
  "message": "string",
  "internal_error_code": 0
}
```

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.



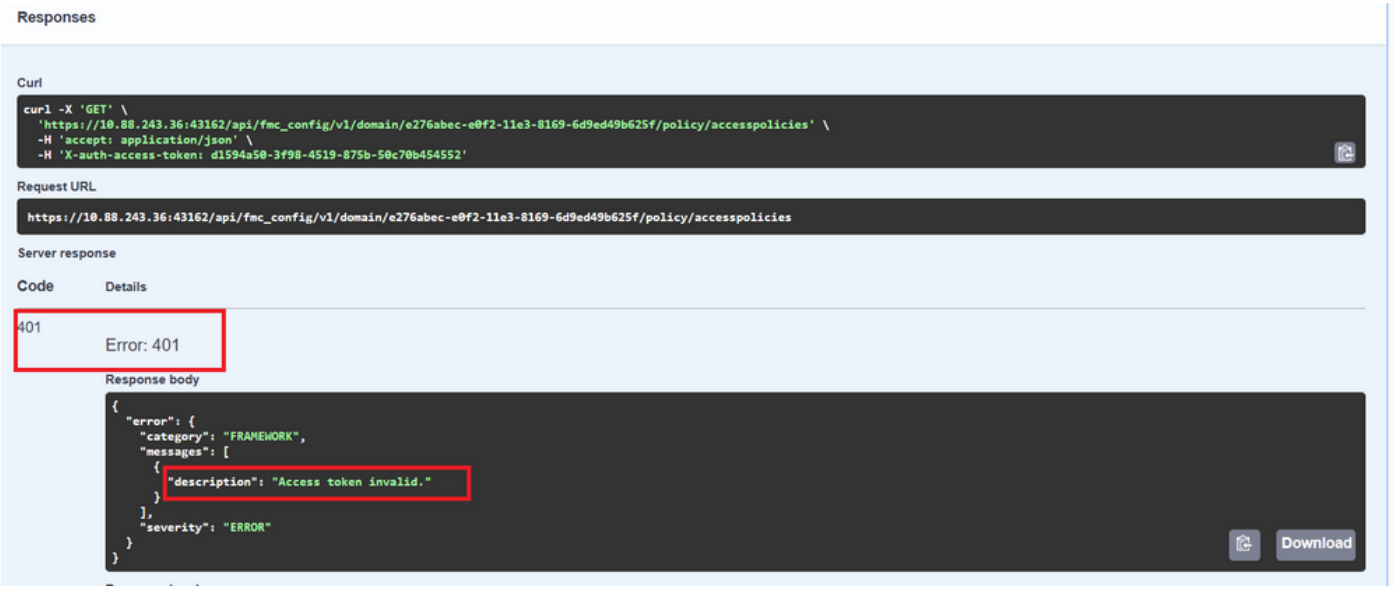
Lorsque vous cliquez sur le bouton Try It Out, s'il s'agit d'un appel qui ne nécessite pas plus de champs, il s'exécute immédiatement et vous donne la réponse.



Dépannage

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.



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.