Dimostrare la navigazione attraverso Secure Firewall API-Explorer

Sommario

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

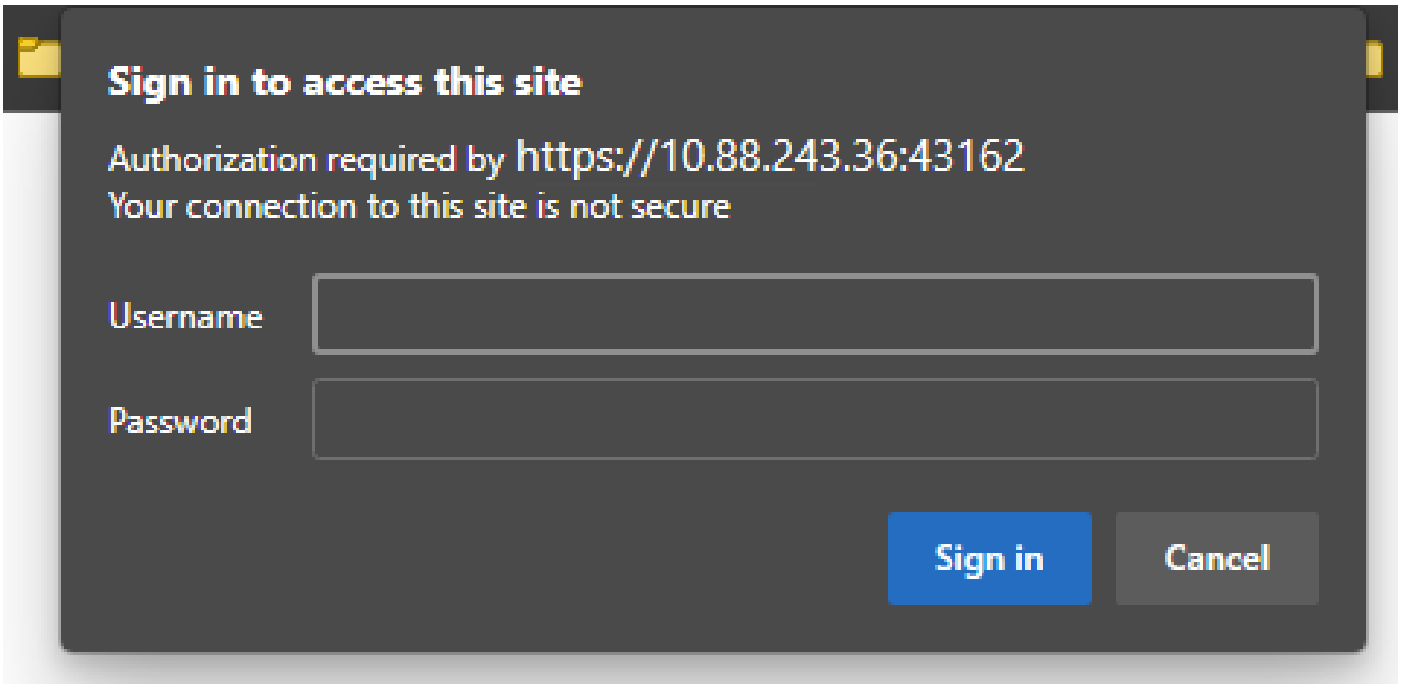
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Esplora API di FMC

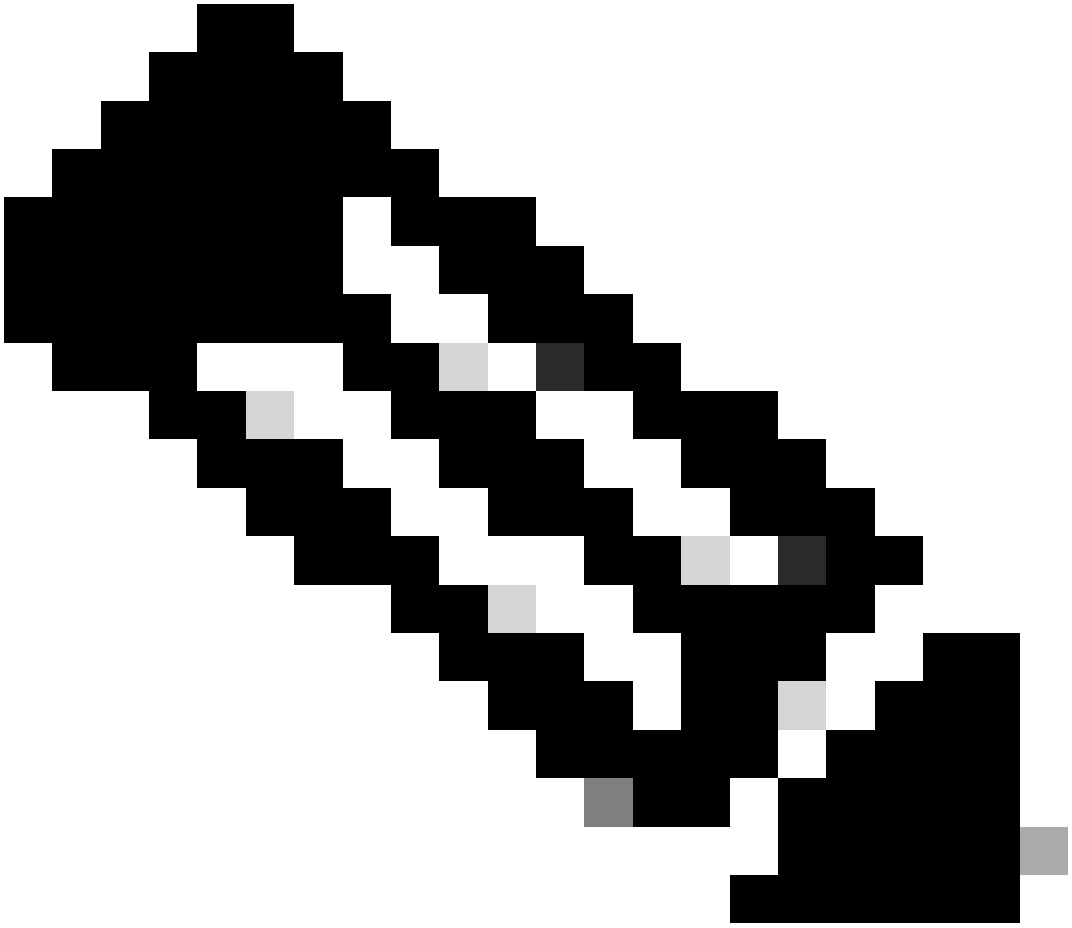
Per accedere a Esplora API di FMC, passare all'URL successivo:

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

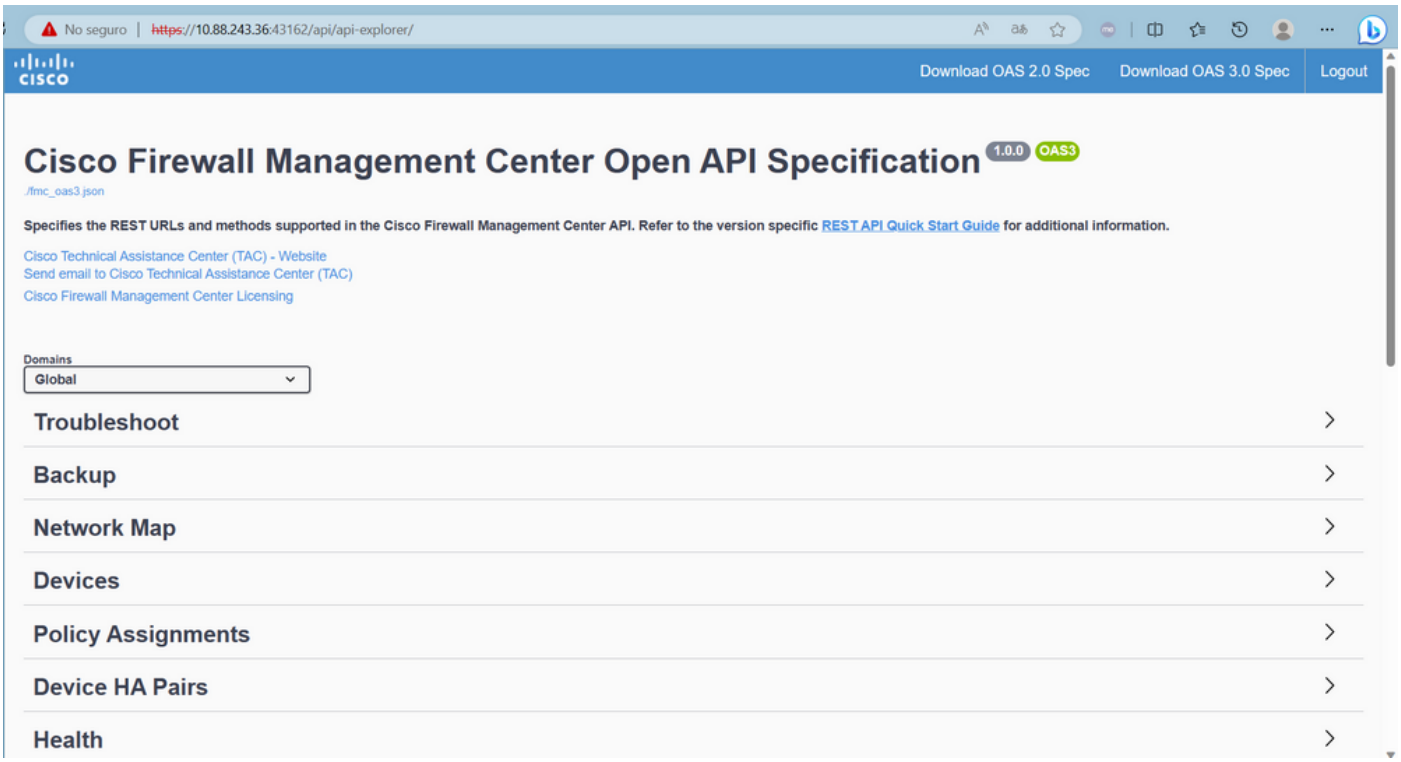
È necessario eseguire l'accesso con le stesse credenziali utilizzate per l'interfaccia utente di FMC. Queste credenziali vengono immesse in una finestra simile a quella successiva quando si immettono gli URL di API Explorer.



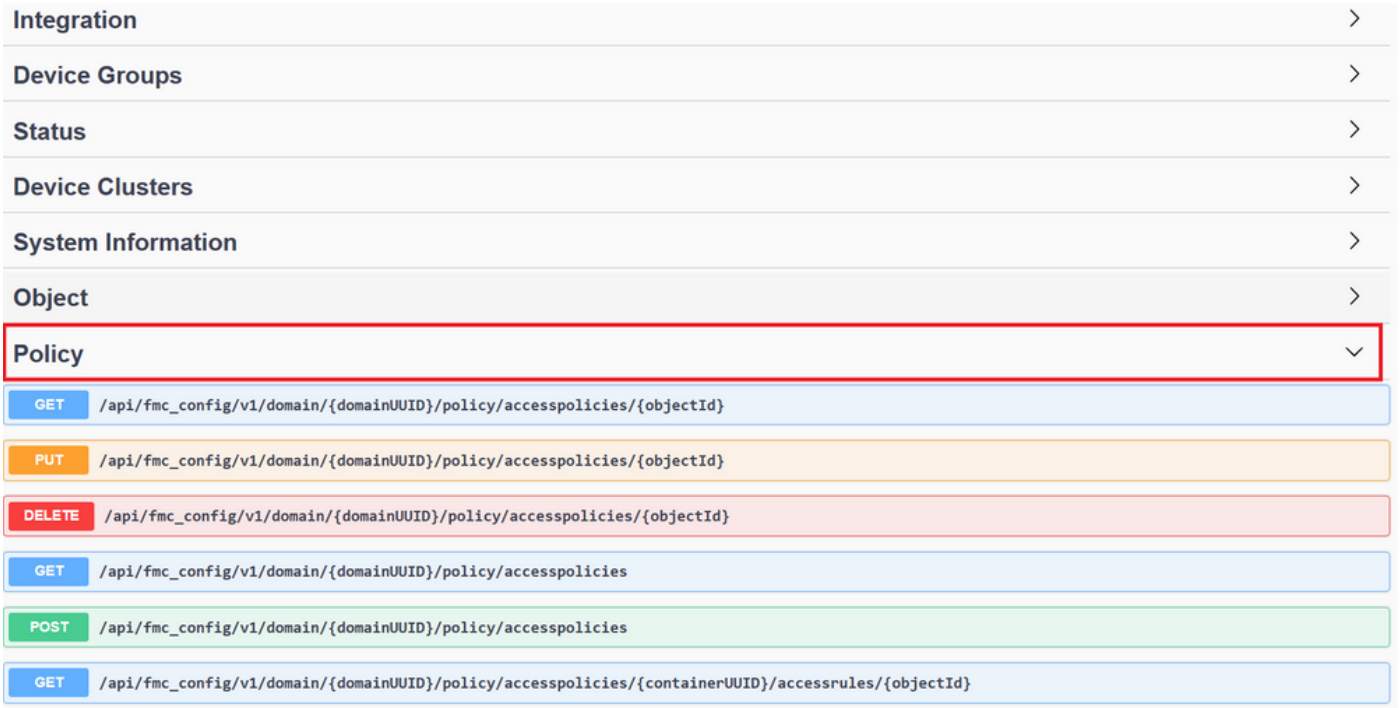
Una volta eseguito l'accesso, le query API vengono suddivise in categorie corrispondenti alle chiamate possibili che è possibile effettuare utilizzando le API.



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

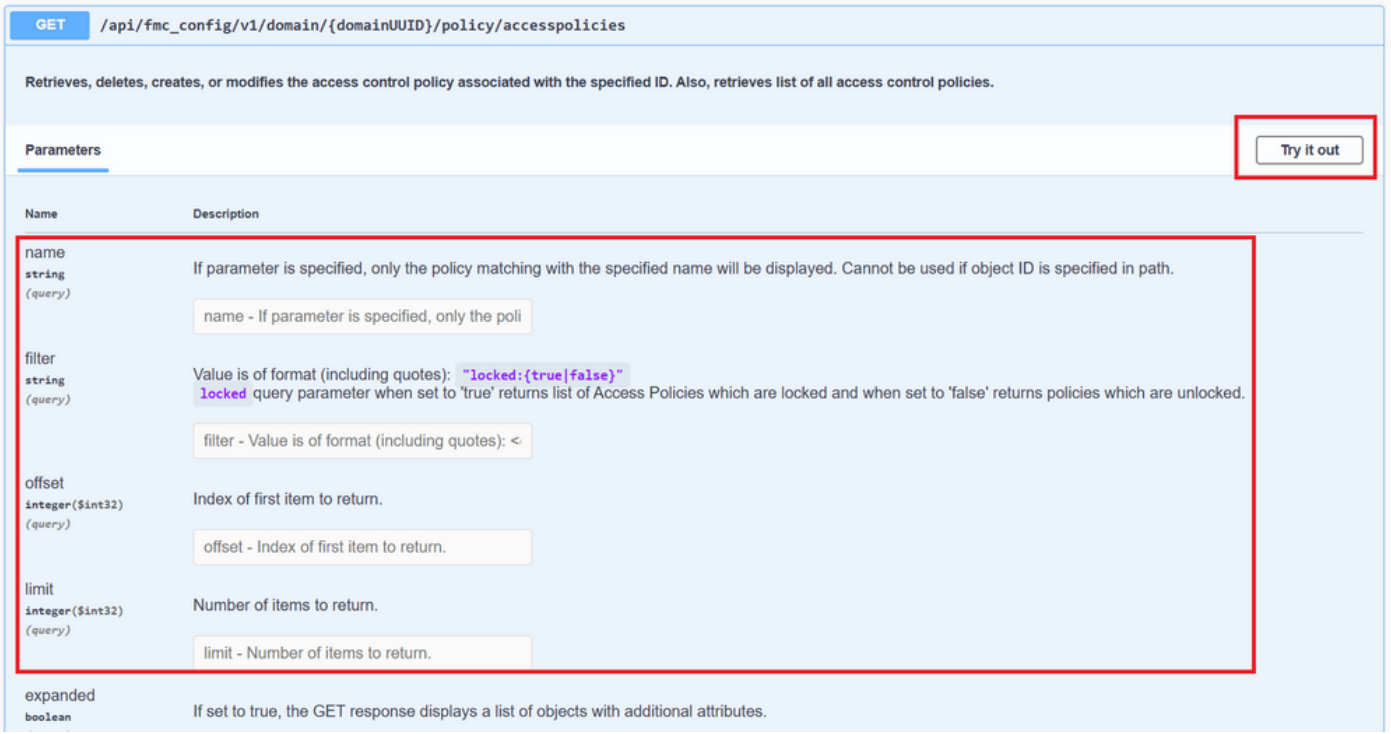


Facendo clic su una categoria, si espande per visualizzare le diverse chiamate disponibili per questa categoria. Queste chiamate vengono visualizzate insieme ai rispettivi metodi REST e all'URI (Universal Resource Identifier) di quella chiamata.



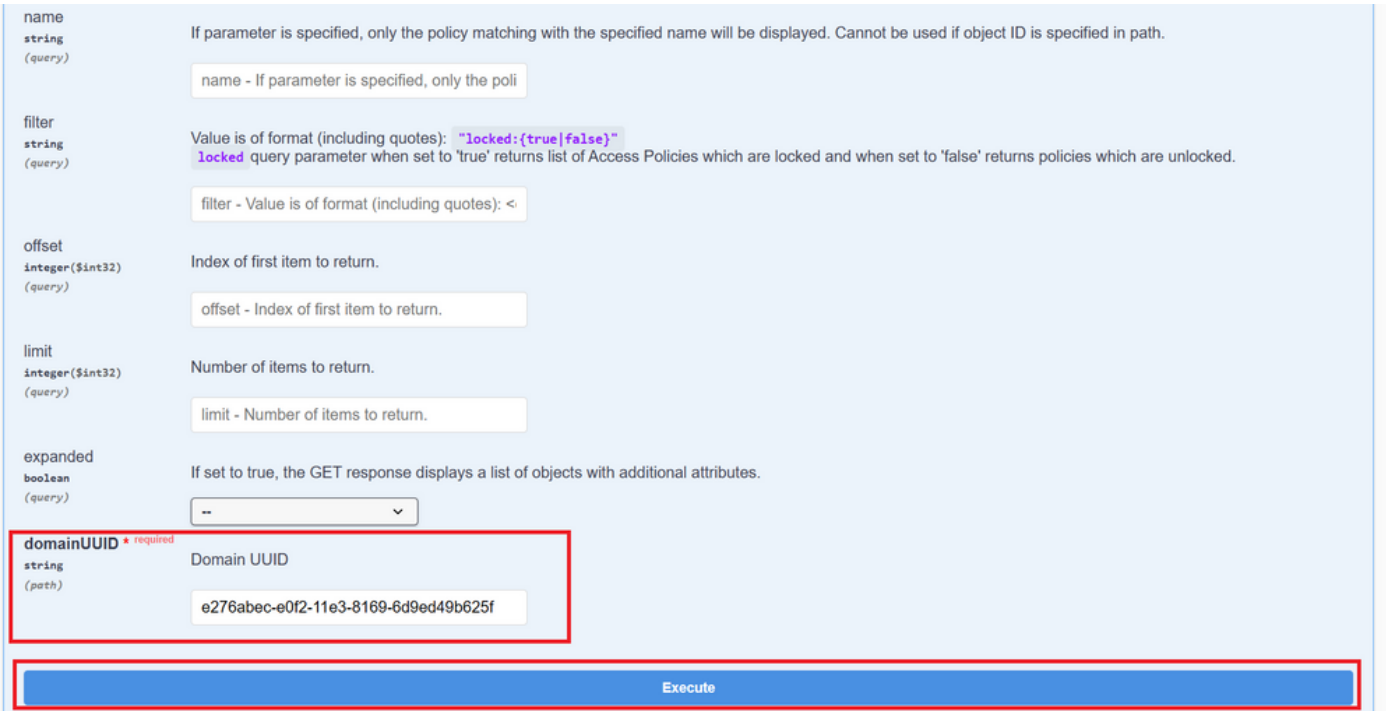
Nell'esempio seguente viene richiesta la visualizzazione dei criteri di accesso configurati nel FMC. Fare clic sul metodo corrispondente per espanderlo, quindi fare clic sul pulsante Prova.

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.

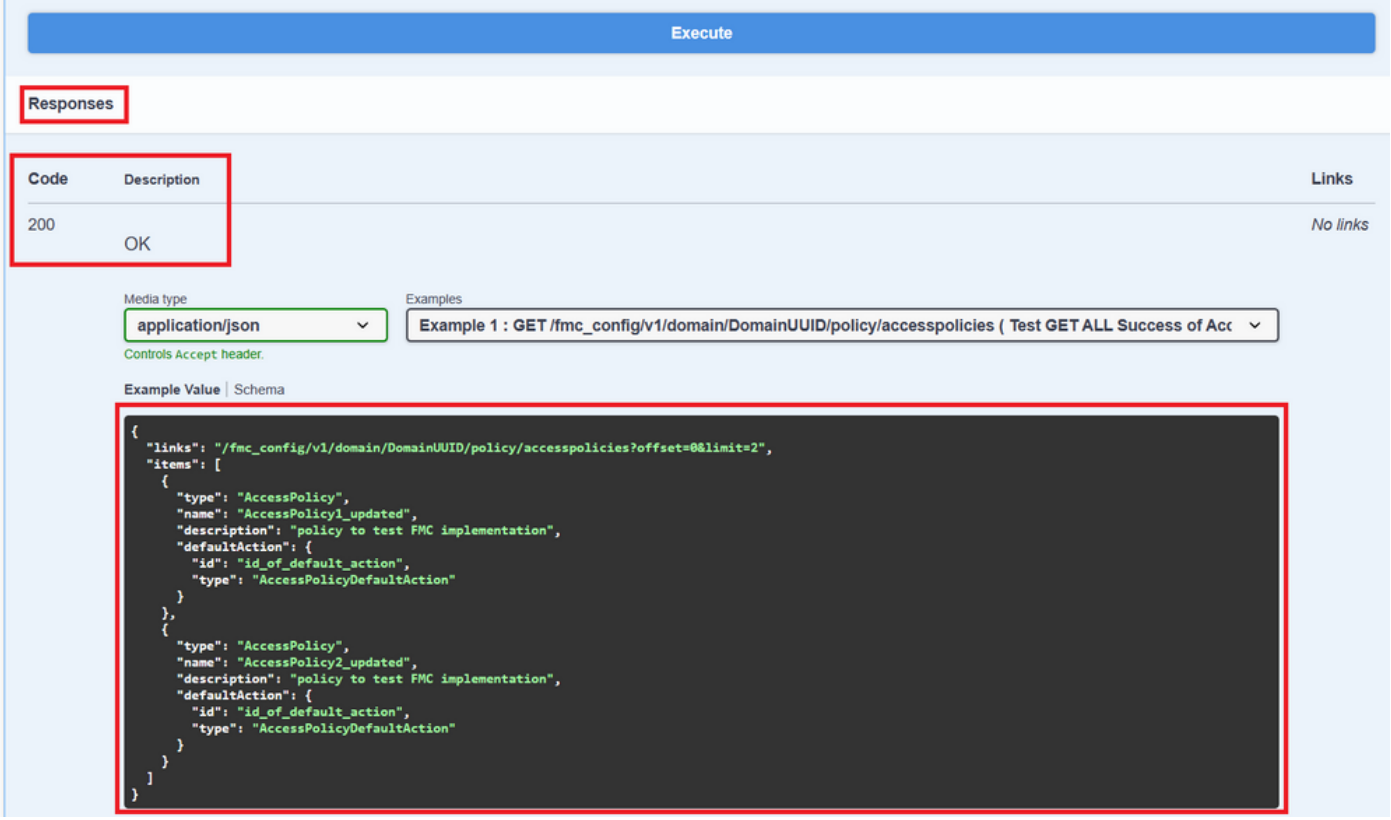


Ad esempio, il domainUUID è obbligatorio per tutte le chiamate API, ma in API Explorer viene riempito automaticamente.

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

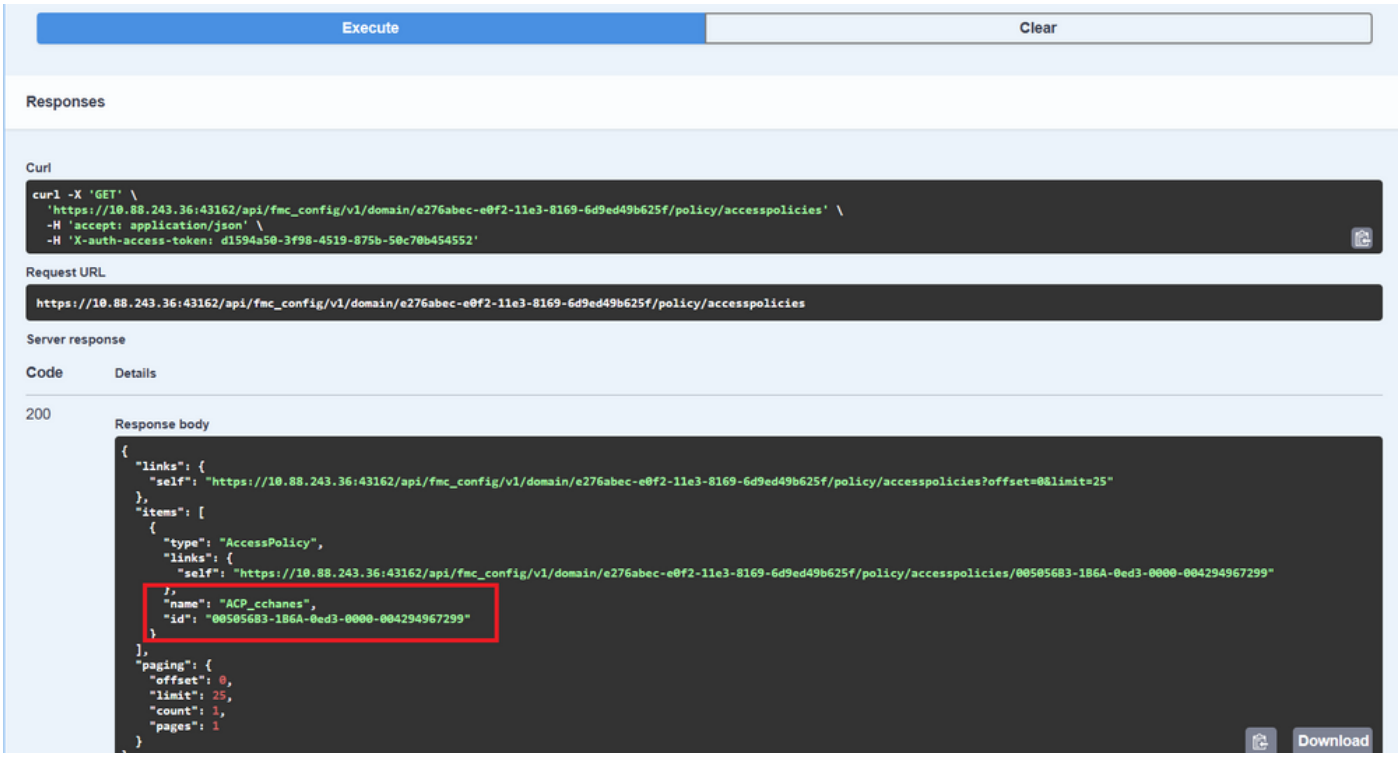


Prima di fare clic su Esegui, è possibile visualizzare esempi di risposte alle chiamate per avere un'idea delle possibili risposte che è possibile ottenere a seconda che la richiesta sia corretta o meno.



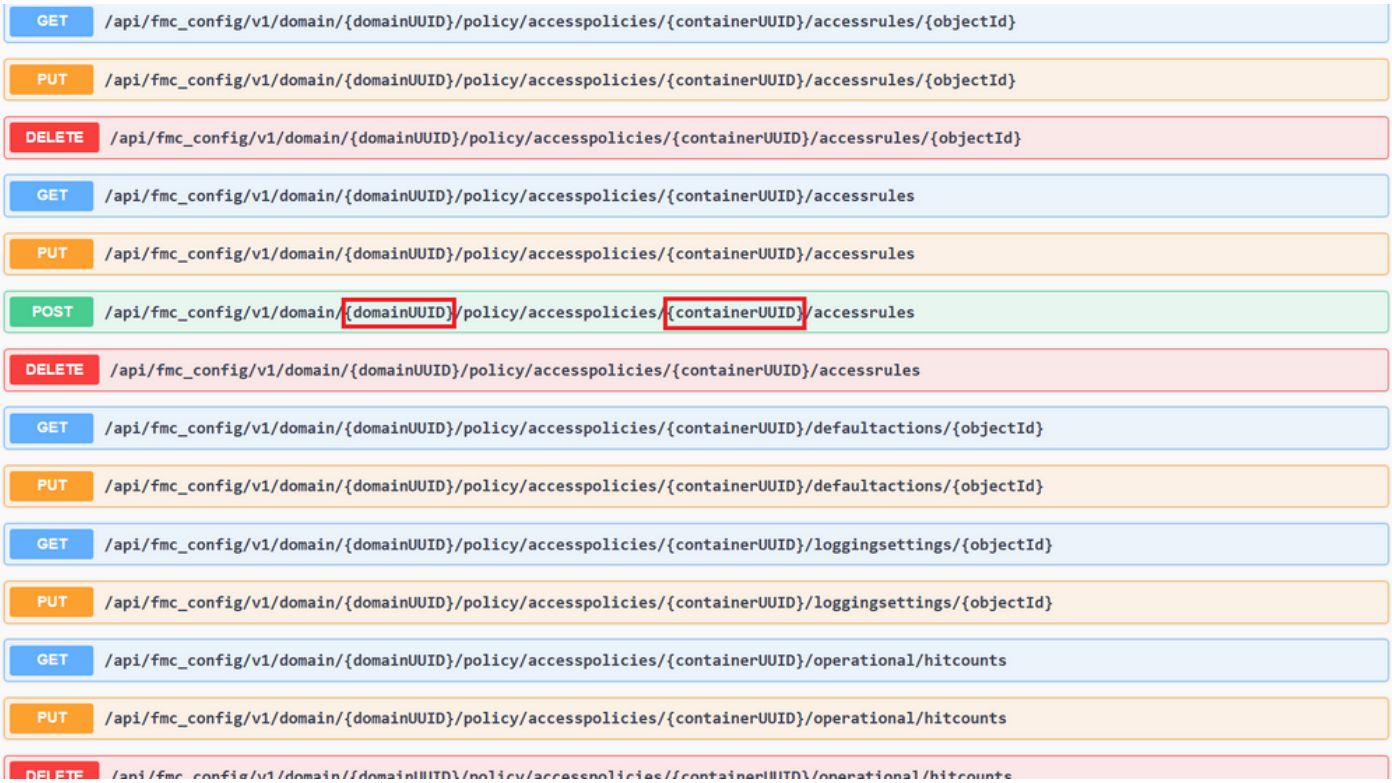
Una volta eseguita la chiamata API, si ottiene, insieme al payload della risposta, il codice di risposta. In questo caso, 200, che corrisponde a una richiesta OK. Riceverai anche l'URL cURL e l'URL della chiamata che hai appena fatto. Queste informazioni sono utili se si desidera effettuare la chiamata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

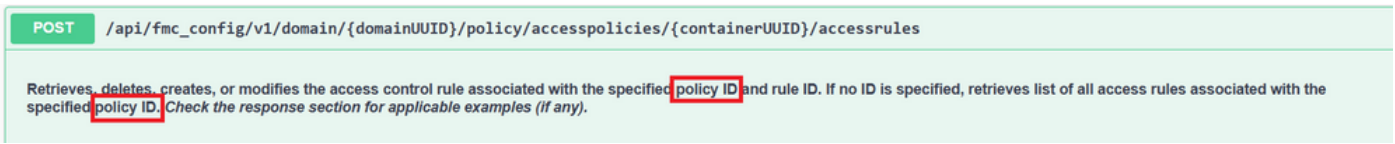


ObjectID è il valore immesso nelle chiamate che richiedono un riferimento a questo punto ACP. Ad esempio, per creare una regola all'interno del punto ACP.

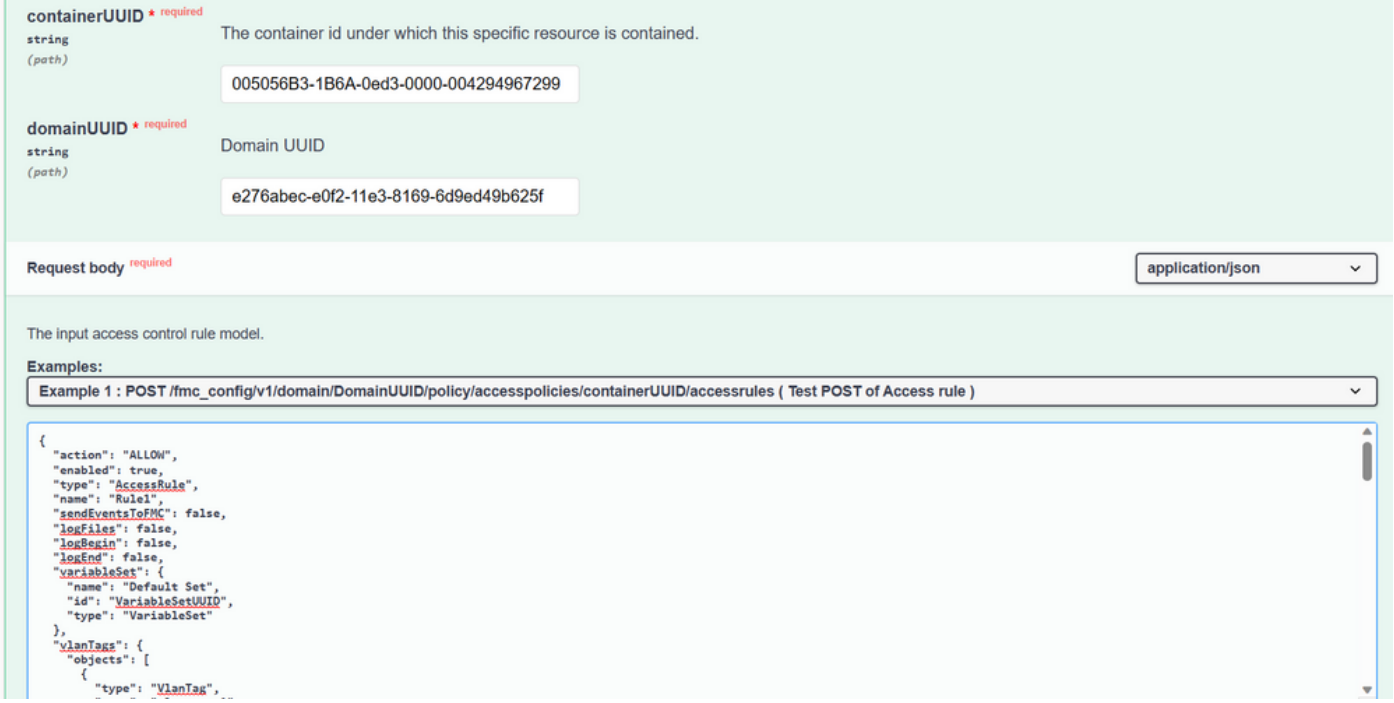
Gli URI che contengono valori tra parentesi graffe {0} sono valori necessari per eseguire questa chiamata. Tenere presente che domainUUID è l'unico valore che viene compilato automaticamente.



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:

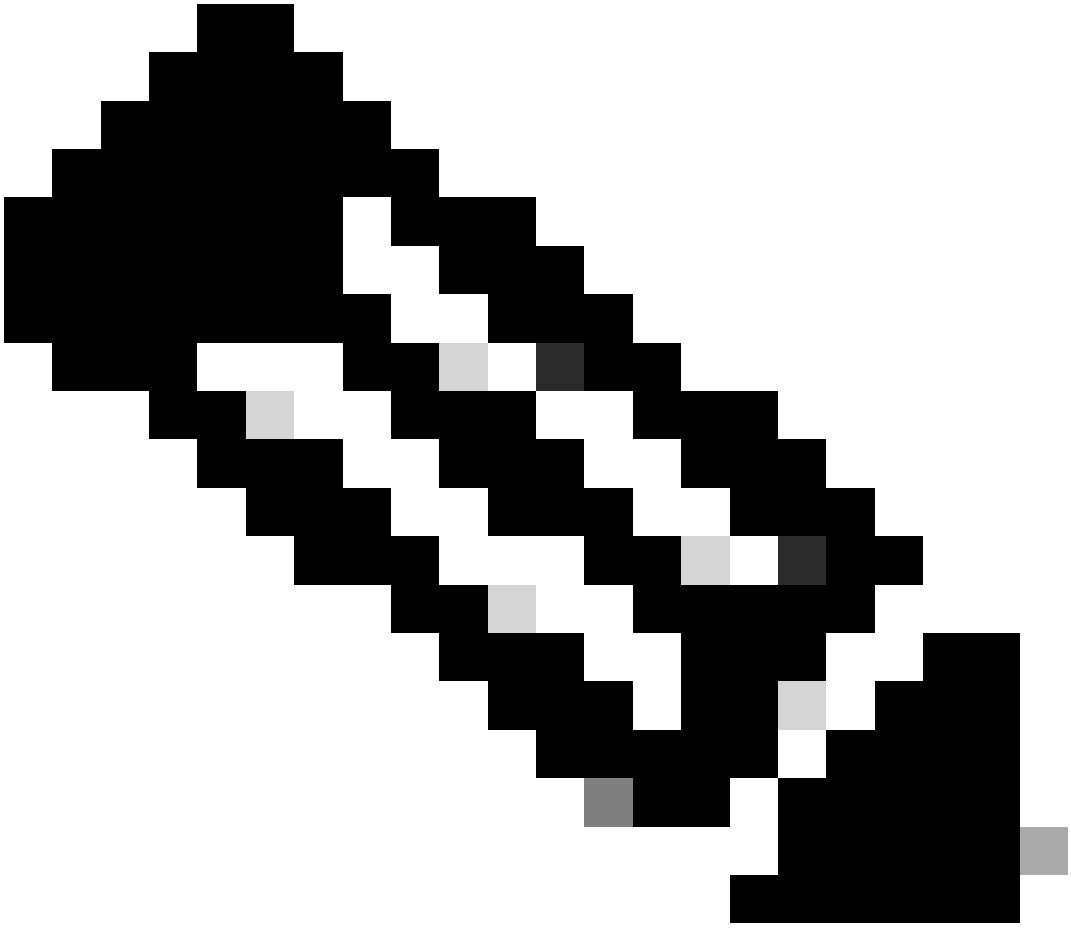


Questo PolicyID viene immesso nel campo specificato come containerUUID. Un altro campo obbligatorio per i metodi POST è il payload o il corpo della richiesta. È possibile utilizzare gli esempi forniti per apportare modifiche in base alle proprie esigenze.



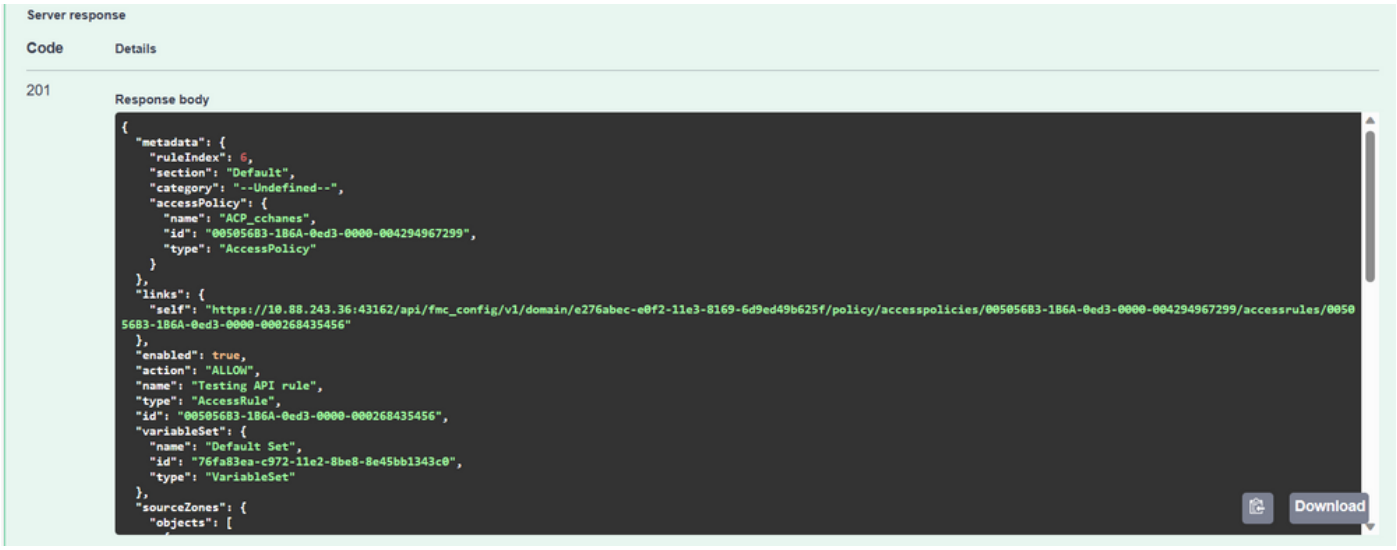
Esempio di payload modificato:

{ "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"] }



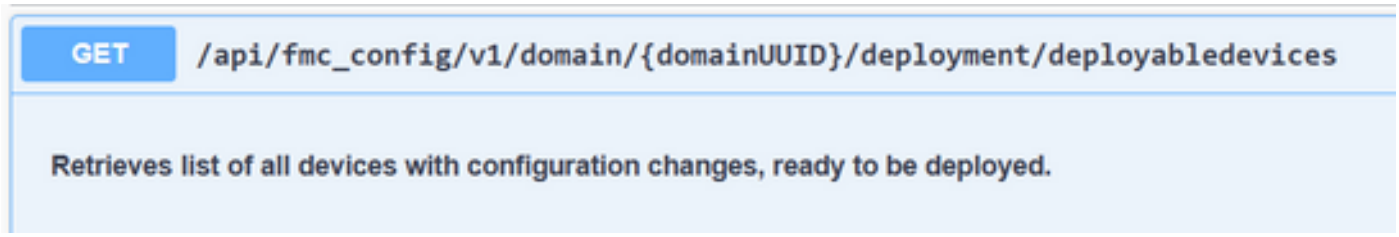
Nota: è possibile ottenere le zone disponibili e i relativi ID utilizzando la query successiva.

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.

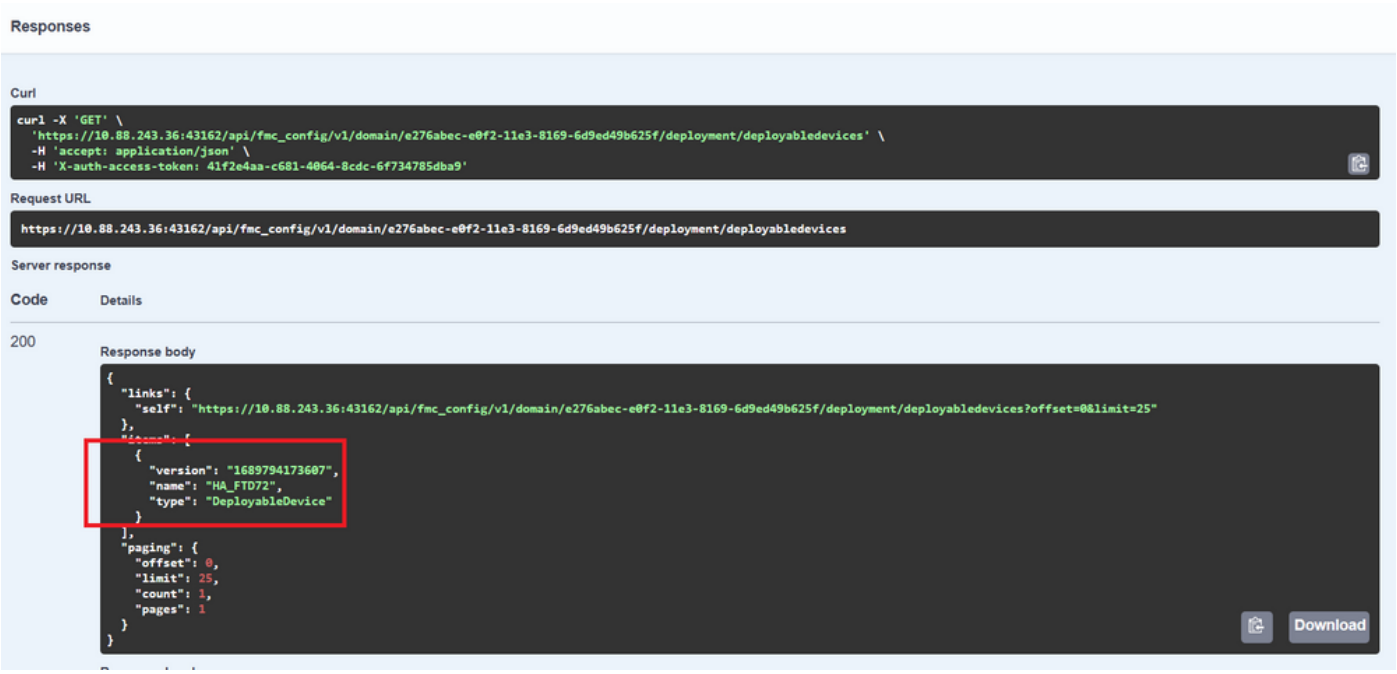


Infine, per rendere effettive le modifiche nell'FTD di cui è stato modificato il punto ACP, è necessario eseguire una distribuzione.

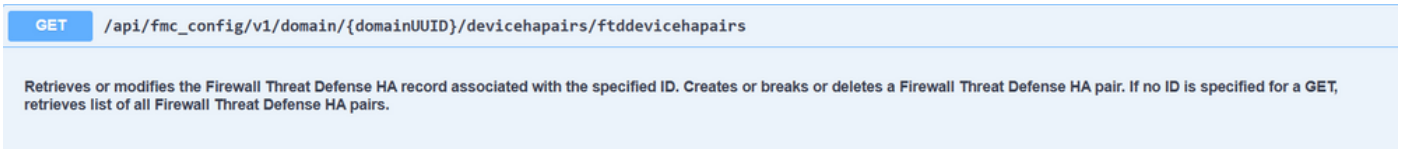
A tale scopo, è necessario ottenere l'elenco dei dispositivi con modifiche pronte per la distribuzione.



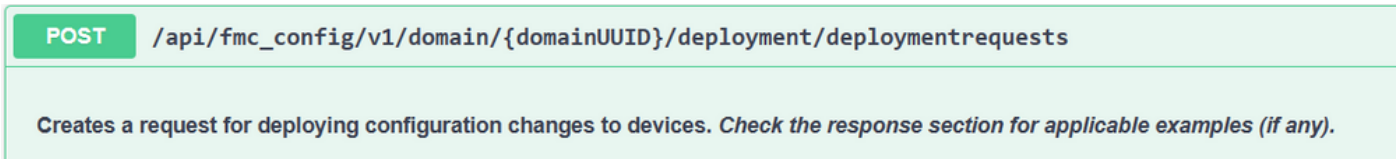
L'esempio contiene una coppia di dispositivi configurati in Alta disponibilità. È necessario ottenere l'ID di questa HA. Se si tratta di un dispositivo autonomo, è necessario ottenere l'ID di tale dispositivo.



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



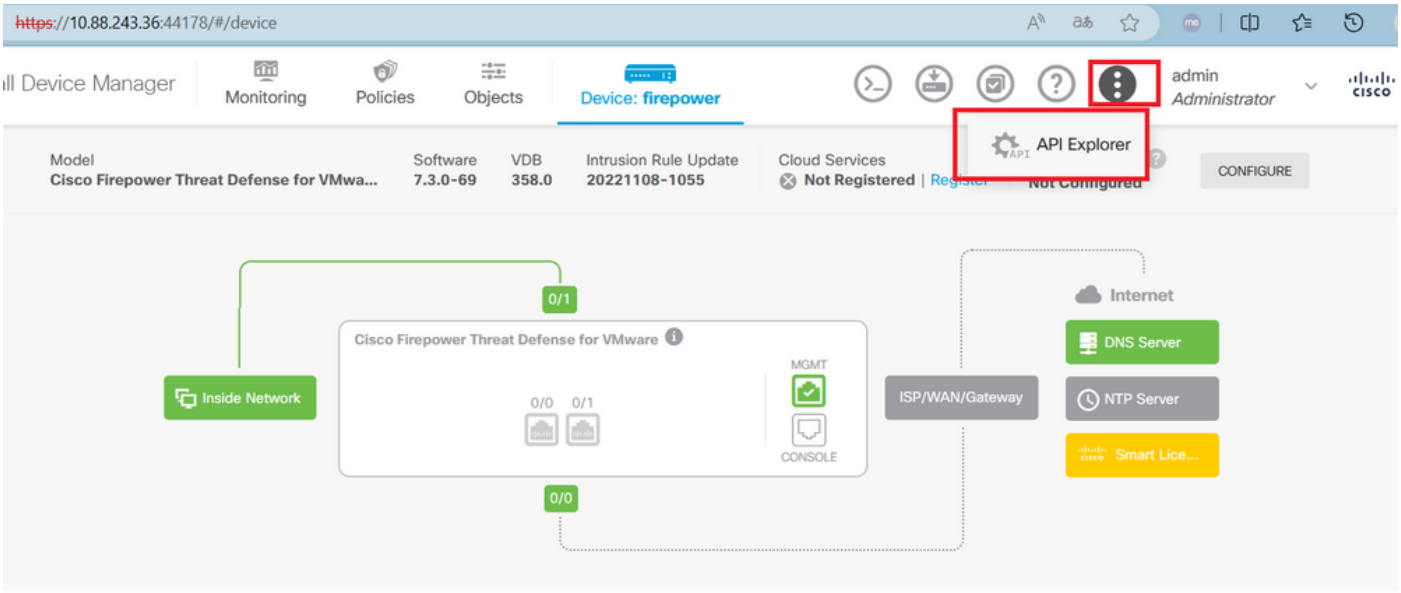
Con l'ID dispositivo e il numero di versione della distribuzione, è possibile modificare il payload dell'esempio di chiamata successivo per effettuare la chiamata per eseguire questa distribuzione.



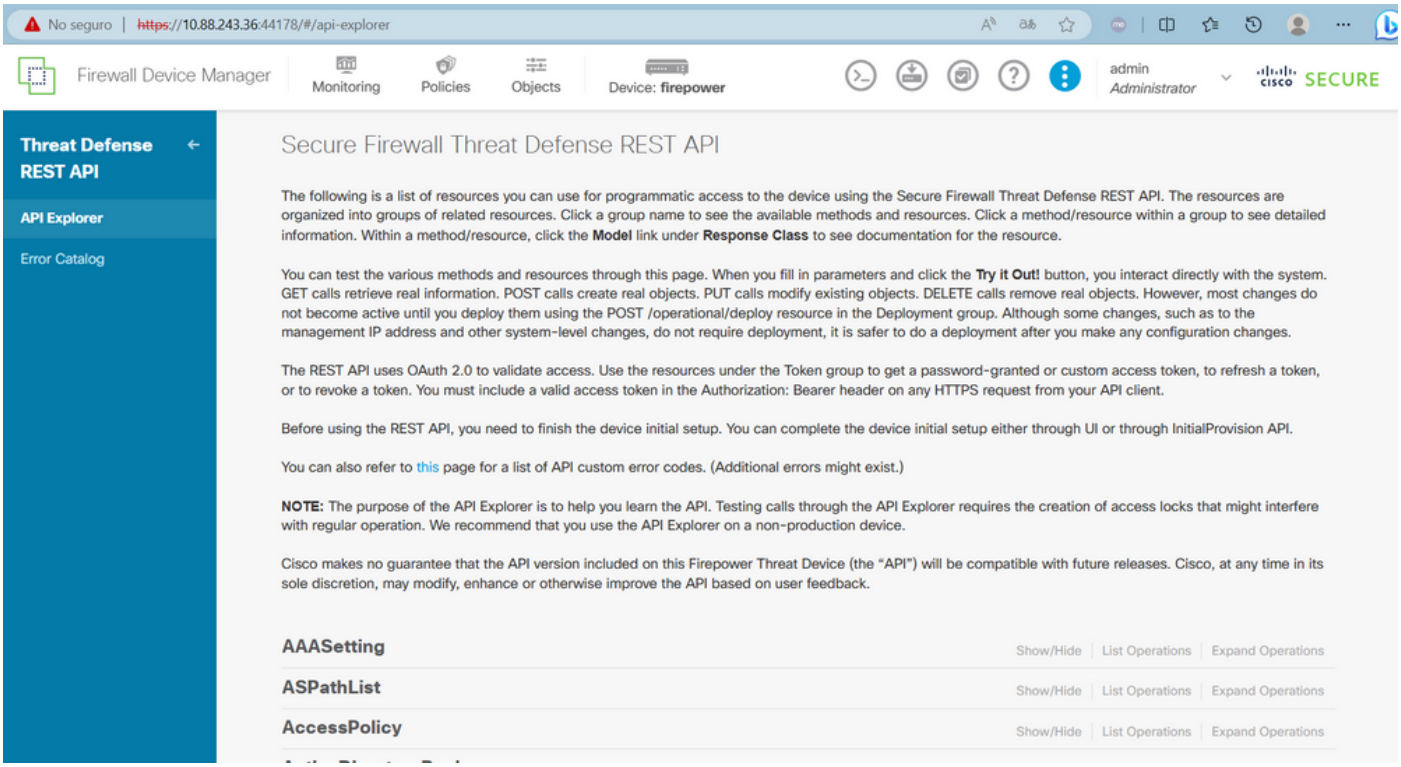
Una volta eseguita questa chiamata, se tutto è corretto, si ottiene una risposta con il codice 202.

Esplorazione delle revisioni tramite Esplora API di FDM

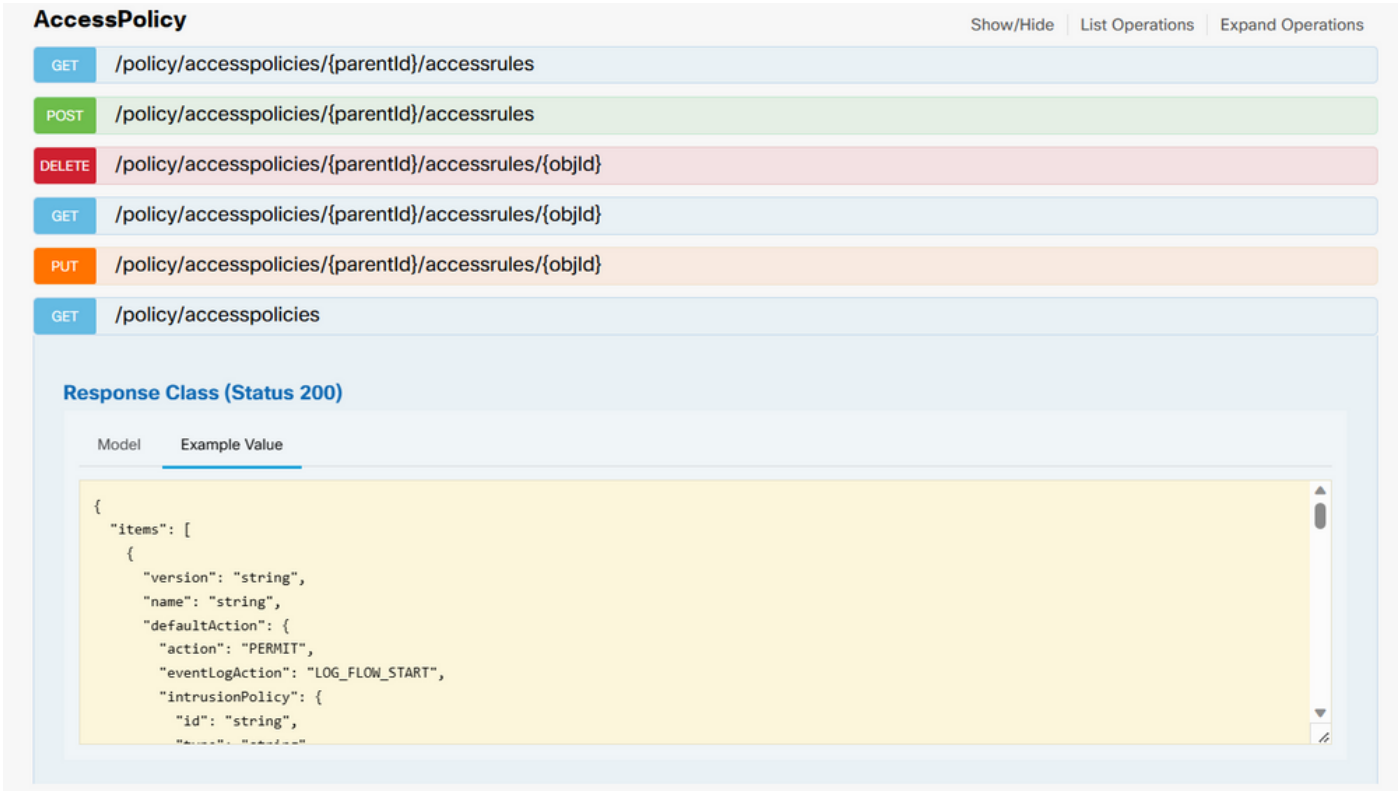
Per accedere a FDM API Explorer, è possibile utilizzare un pulsante sull'interfaccia utente di FDM per passare direttamente a esso, come mostrato nell'immagine seguente:



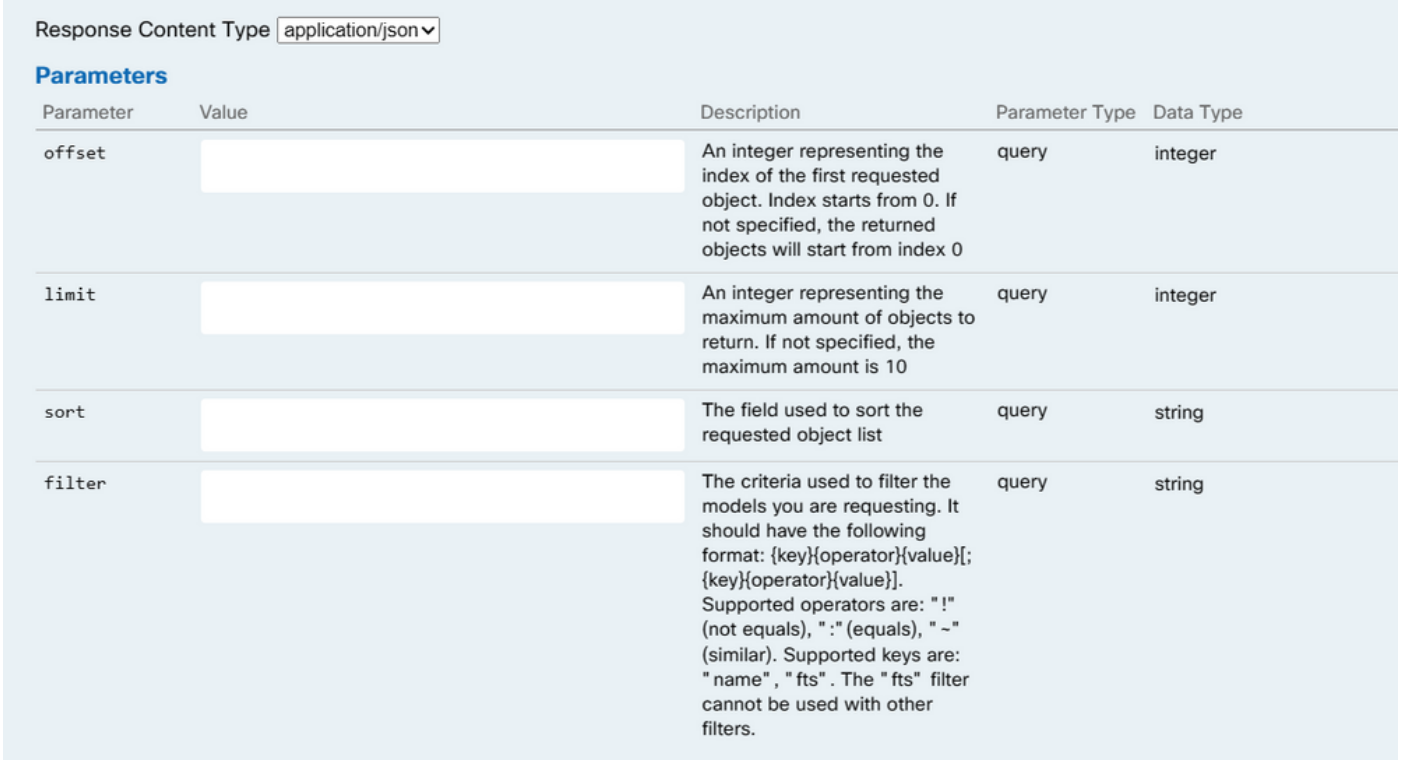
Una volta in API Explorer, si nota che le query sono anche divise in categorie.



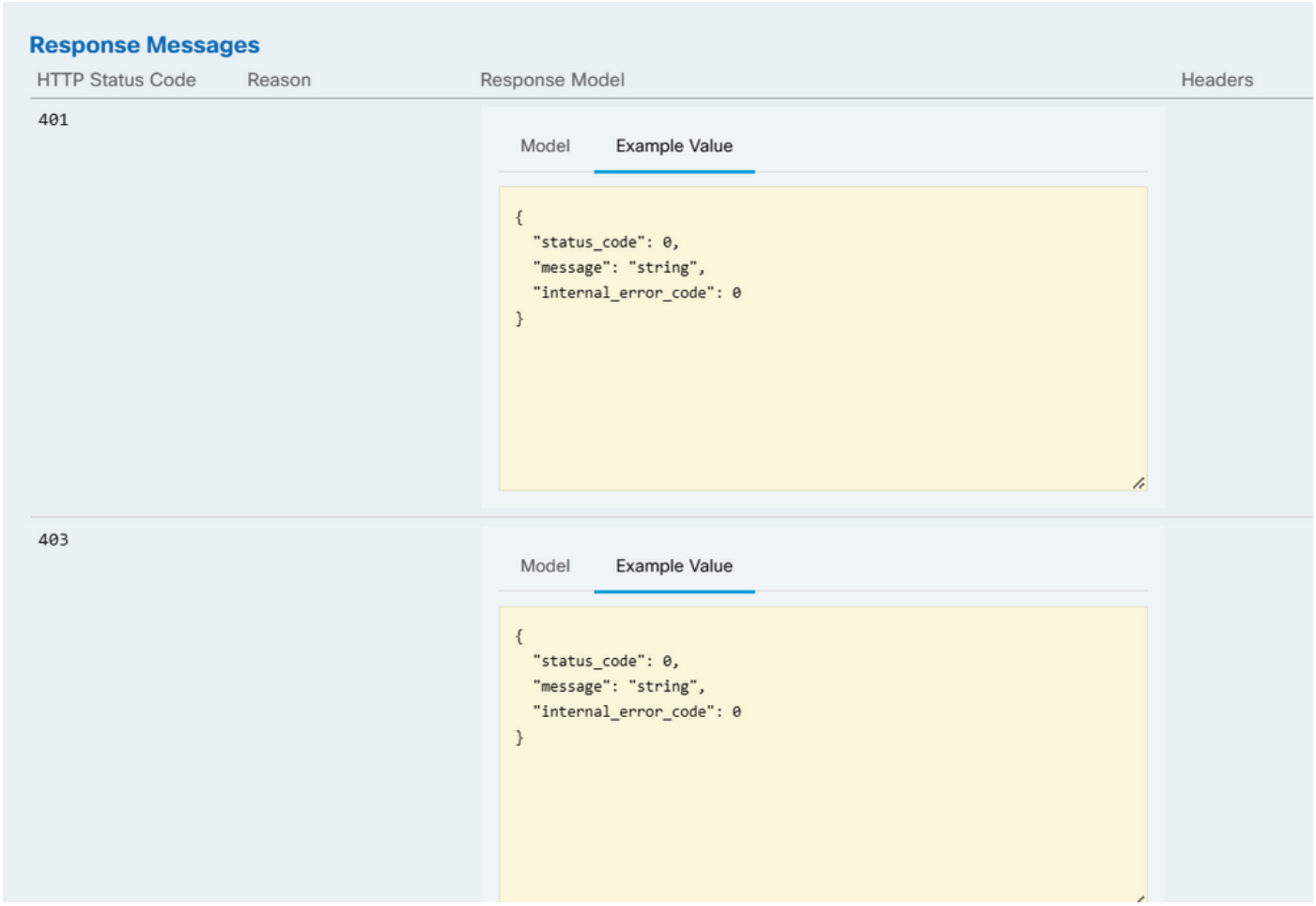
Per espandere una categoria, è necessario fare clic su di essa, quindi è possibile espandere ogni operazione facendo clic su una di esse. La prima cosa che si trova all'interno di ciascuna operazione è un esempio di risposta OK per questa chiamata.



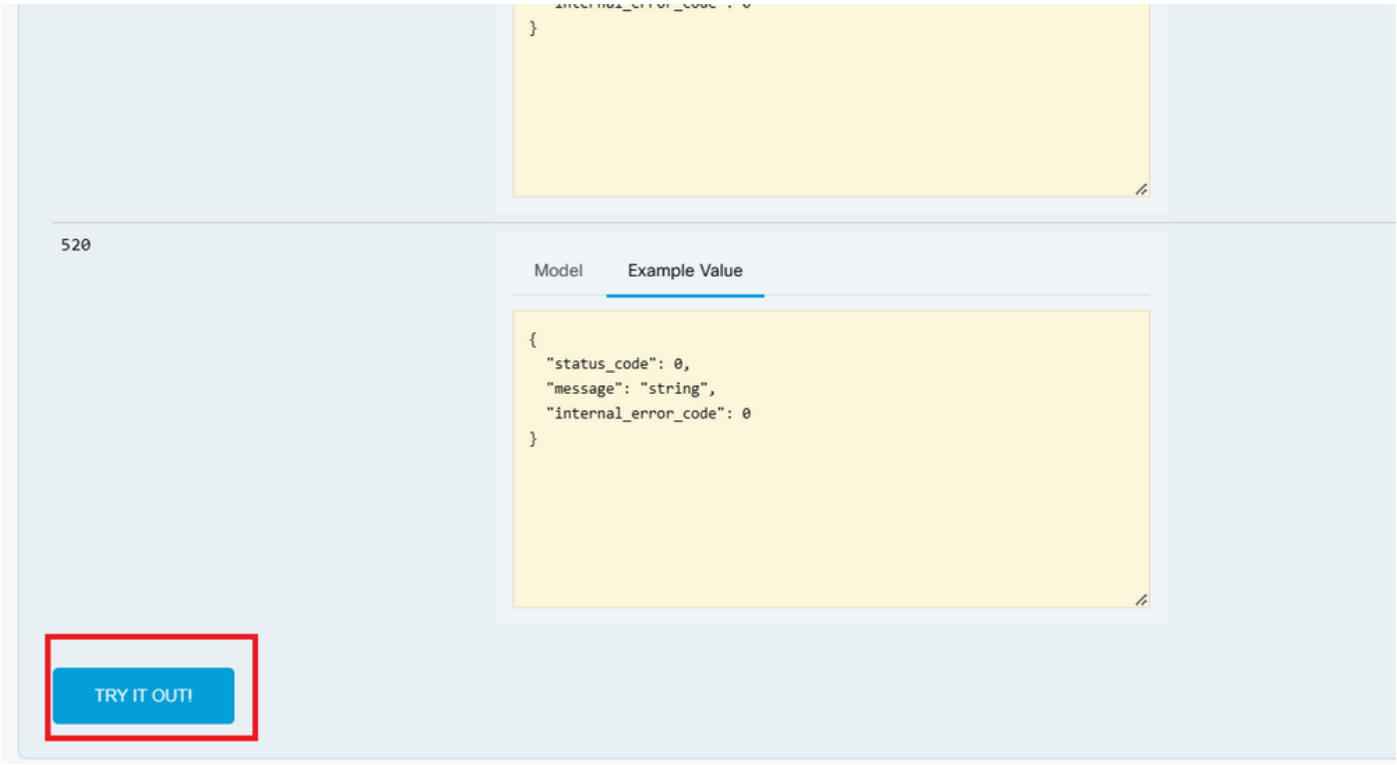
Di seguito vengono visualizzati i parametri disponibili per vincolare le risposte della chiamata effettuata. Ricorda che solo i campi contrassegnati come obbligatori sono obbligatori per effettuare una chiamata di questo tipo.



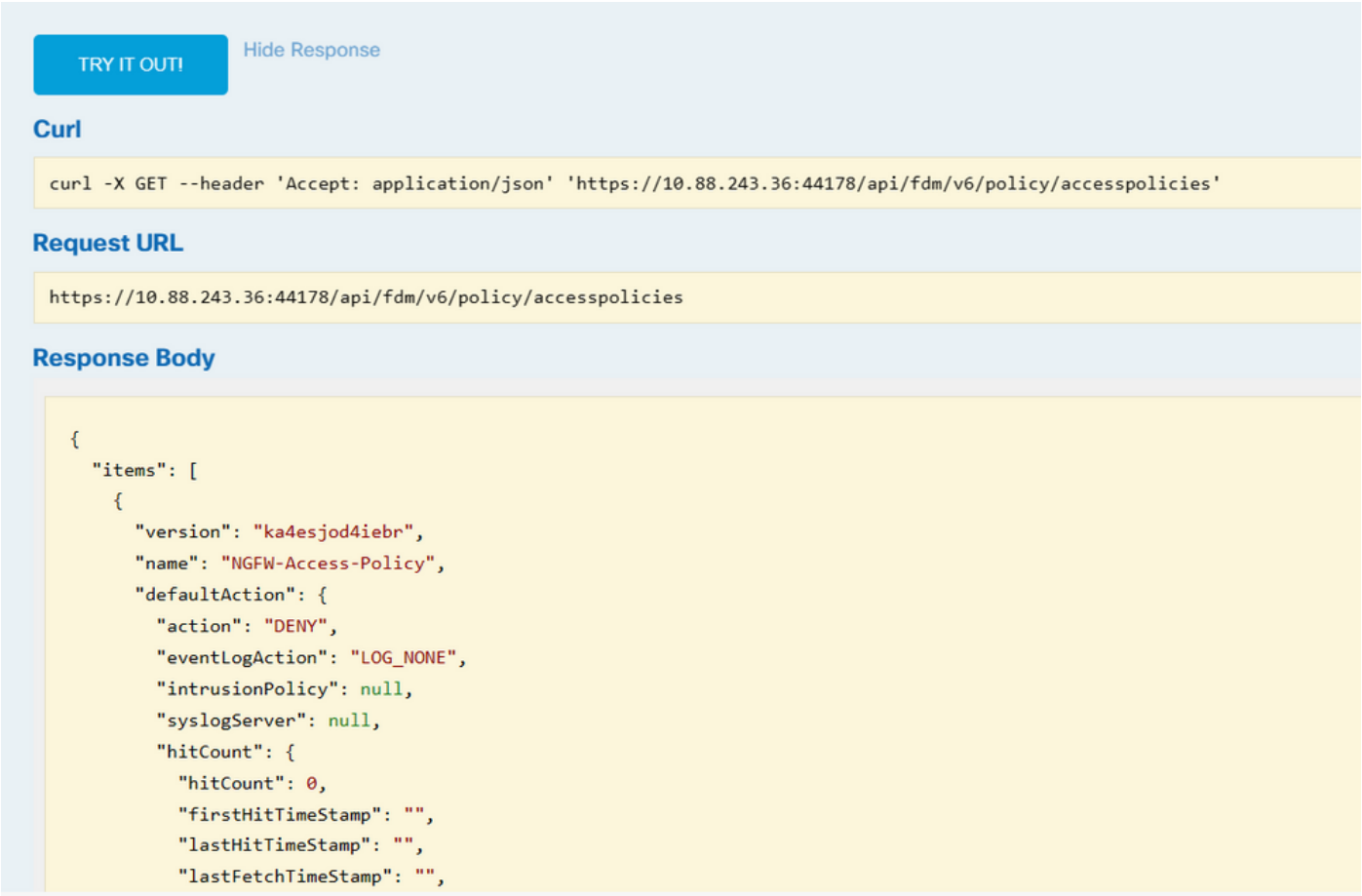
Infine, è possibile trovare i possibili codici di risposta restituibili da questa chiamata.



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.



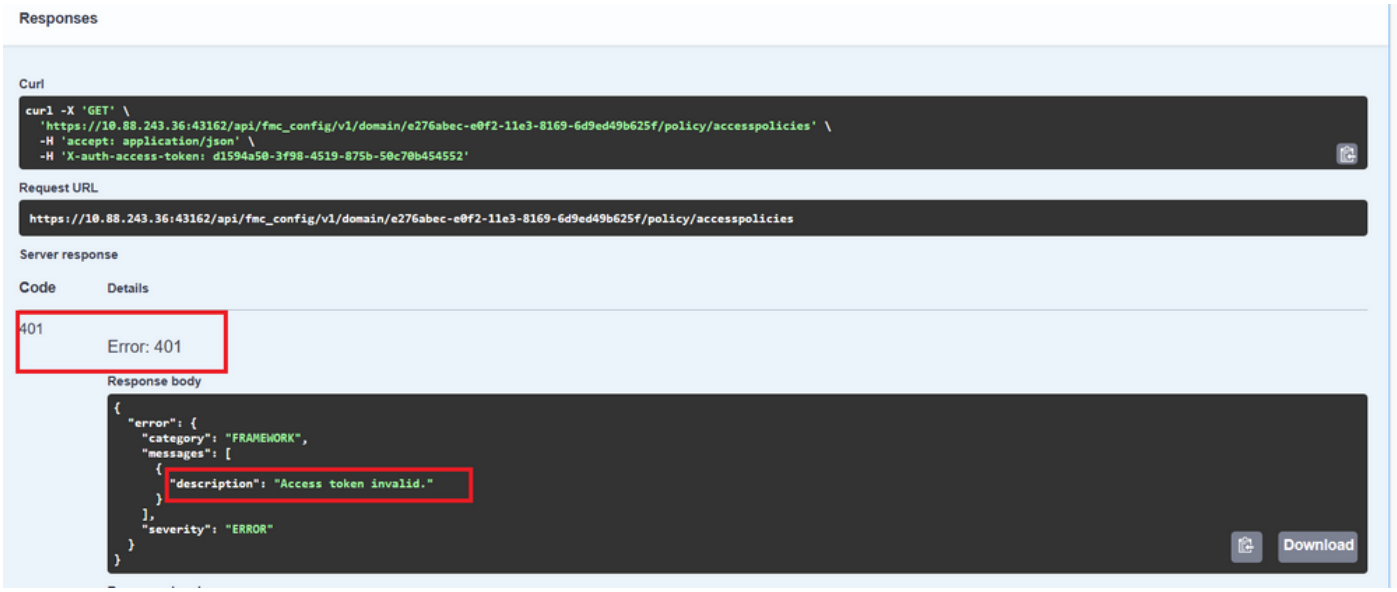
Quando si fa clic sul pulsante Prova, se la chiamata non richiede altri campi, viene eseguita immediatamente e viene fornita la risposta.



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.



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).