アクセス コントロール ポリシー用の Cisco Secure Firewall Management Center REST API

初版：2024 年 1 月 16 日

アクセス コントロール ポリシーの REST API

Cisco Secure Firewall Management Center API を使用して、アクセスポリシー、アクセスルール、およびその他のアクセス ポリシー オブジェクトを作成および管理できます。このドキュメントでは、基本的なアクセス コントロール ポリシーを管理する手順について説明します。アクセスルールおよびその他のポリシーオブジェクトに関する情報は、このドキュメントの範囲外です。

ポリシー API を使用すると、次のことができます。

1. 管理対象ファイアウォールデバイスのアクセス コントロール ポリシーを作成して、不正アクセス、マルウェア感染、データ侵害、およびその他のセキュリティ脅威からネットワークを保護します。
2. （任意）ポリシーをロックして、ルールが別のユーザーによって上書きされないようにします。
3. （任意）継承機能を使用してカスタムポリシーを作成します。
4. （任意）廃止され、不要になったアクセス コントロール ポリシーを削除します。
5. ポリシーを変更するたびに、新しいポリシー設定または変更されたポリシー設定をデバイスに展開します。

使用されるエンドポイントとメソッド

1 認証トークン
2 更新トークン
3 基本的なアクセス コントロール ポリシーの作成
4 アクセス コントロール ポリシーの編集
5 アクセス コントロール ポリシーのロック
6 アクセス コントロール ポリシー継承の管理
7 アクセス コントロール ポリシーの削除
8 アクセス コントロール ポリシーのターゲットデバイスの設定

Management Center REST API の重要な用語

- DomainUUID：グローバルドメイン UUID。この ID は、バージョンに関係なく、すべての Management Center で常に同じになります。Management Center で新しいドメインを作成し、新しく作成したドメインの特定のユーザーを作成すると、新しいドメイン UUID が Management Center の API コンソールに表示されます。
- ContainerUUID：オブジェクトをスキーマ全体に接続する親オブジェクトの UUID。たとえば、物理インターフェイスを取得するには、次の URL でデバイス ID をコンテナ UUID として使用します。

  GET /api/fmc_config/v1/domain/{domain_UUID}/devices/devicerecords/{container_UUID}/fpphysicalinterfaces
- ObjectID：ターゲットオブジェクトの ID。たとえば、物理インターフェイスの詳細を取得するには、次の URL でインターフェイス ID をオブジェクト ID として使用します。

  GET /api/fmc_config/v1/domain/{domain_UUID}/devices/devicerecords/{container_UUID}/fpphysicalinterfaces/{objectId}

基本的なアクセス コントロール ポリシーの作成

アクセスポリシーは、次のコンポーネントで構成されます。

- トラフィック一致基準：セキュリティゾーン、IP アドレスまたは位置情報、ポート番号、プロトコル、アプリケーションタイプ、URL パターン、URL カテゴリ、URL レピュテーション、およびユーザー。
- 一致するトラフィックに対するアクション：許可、ブロック、信頼、モニター。
- [許可（Allow）] アクションカテゴリの侵入防御ポリシー、ファイルポリシー、またはその両方。

（注） Threat Defense デバイスに割り当てることができるポリシーは 1 つだけです。ただし、複数のデバイスに同じポリシーを割り当てることができます。

始める前に

REST API リソースを使用するための適切な許可があることを確認します。『Secure Firewall Management Center REST API Quick Start Guide』の「Authentication from a REST API Client」セクションを参照してください。

手順

次の URL を使用してアクセス コントロール ポリシーを作成します。

```
POST api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies
```

例：

Request body

```
{
  "type": "AccessPolicy",
  "name": "Policy1",
  "defaultAction": {
    "action": "BLOCK"
  }
}
```

Response body

```
{
  "metadata": {
    "inherit": false,
    "lockingStatus": {
      "status": "UNLOCKED"
    },
    "domain": {
      "name": "Global",
      "id": "e276abec-e0f2-11e3-8169-6d9ed49b625f",
      "type": "Domain"
    }
  },
  "type": "AccessPolicy",
  "links": {
    "self": "https://..."
  },
  "rules": {
    "refType": "list",
    "type": "AccessRule",
    "links": {
      "self": "https://...."
    }
  },
  "name": "Policy1",
  "id": "00505691-AED0-0ed3-0000-004294990861"
}
```

指定した名前と一意の ID でポリシーが作成されます。

次のタスク

1. ターゲットデバイスにポリシーを割り当てます。「アクセス コントロール ポリシーのターゲットデバイスの設定 （9 ページ）」を参照してください。
2. 設定変更を展開します。「構成の展開 （14 ページ）」を参照してください。

アクセス コントロール ポリシーの編集

始める前に

変更または編集するアクセスポリシーが作成されていることを確認します。ポリシーを作成する方法については、「基本的なアクセス コントロール ポリシーの作成 （3 ページ）」を参照してください。

手順

ステップ 1 アクセスポリシーを編集するには、ポリシーの ID が必要です。ID を取得するには、次の URL を使用します。

```
GET /api/fmc_config/v1/domain/{domainUUID} /policy/accesspolicies
```

例：

Request URL

```
https://<management_center_IP_or_name>/api/fmc_config/v1/domain/<domainUUID>/policy/accesspolicies
```

Response Body

```
{
  "links": {
    "self": "https://...."
  },
  "items": [
    {
      "type": "AccessPolicy",
      "links": {
        "self": "https://..."
      },
      "name": "Policy1",
      "id": "00505691-AED0-0ed3-0000-004294990861"
    },
    {
      "type": "AccessPolicy",
      "links": {
        "self": "https://..."
      },
      "name": "Policy2",
      "id": "00505691-64F9-0ed3-0000-004294969027"
    }
```

ステップ 2 次の URL を使用してアクセス コントロール ポリシーを編集します。

```
PUT /api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{objectId}
```

この例では、Policy 1 のパラメータを編集するために、要求本文のオブジェクト ID としてポリシー ID（00505691-AED0-0ed3-0000-004294990861）を使用します。

（注） 更新を有効にするには、変更した設定を展開してください。

次のタスク

- 設定変更を展開します。「構成の展開 （14 ページ）」を参照してください。

アクセス コントロール ポリシーのロック

デフォルトでは、アクセスポリシーはロックされていません。他のユーザーがルールまたは設定を変更できないようにする場合は、それらをロックできます。

始める前に

ロックするアクセスポリシーが作成されていることを確認します。ポリシーを作成する方法については、「基本的なアクセス コントロール ポリシーの作成 （3 ページ）」を参照してください。

手順

ステップ 1 アクセスポリシーをロックするには、ポリシーの ID が必要です。ID を取得するには、次の URL を使用します。

```
GET /api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies
```

ステップ 2 アクセスポリシーをロックするには、次の URL を使用します。

```
POST
/api/fmc_config/v1/domain/{domainUUID}/policy/operational/policylocks
```

要求本文でポリシー ID を指定します。

例：

Request body

```
{
  "policies": [
    {
      "lock": "true",
      "policy": {
        "id": "00505691-AED0-0ed3-0000-004294990861",
        "type": "AccessPolicy"
      }
    }
  ]
}
```

Response body

```
{
  "policies": [
    {
      "type": "PolicyLock",
      "policy": {
        "name": "Policy1",
        "id": "00505691-AED0-0ed3-0000-004294990861",
        "type": "AccessPolicy",
        "links": {
          "self": "https://..."
        }
      },
      "status": "LOCKED",
      "metadata": {
        "lockedByUser": {
          "name": "apiuser"
        }
      }
    }
  ]
}
```

ポリシーのロックを解除するには、POST メソッドを使用し、要求本文で "lock": "false" を指定します。

ポリシーはロックされ、他のユーザーはポリシーを変更できません。

アクセス コントロール ポリシー継承の管理

継承機能を使用すると、1 つのポリシーの一部のベースライン特性を複数のポリシーに適用できます。ポリシーを別のアクセス コントロール ポリシーの基本ポリシーとして使用できます。

手順

ステップ 1 ポリシーの既存の継承設定を表示するには、次の URL を使用します。

```
GET api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/ {containerUUID}
/inheritancesettings/{objectId}
```

要求 URL の containerUUID フィールドとオブジェクト ID フィールドにポリシー ID を使用します。

例：

Request URL

```
https://<management_center_IP_or_name>/api/fmc_config/v1/domain/<domainUUID>
/policy/accesspolicies/00505691-AED0-0ed3-0000-004294990861/inheritancesettings/00505691-AED0-0ed3-0000-004294990861
```

Response body

```
 {
  "links": {
    "self": ….
  },
  "basePolicy": {
    "name": "CorePolicy",
    "id": "00505691-AED0-0ed3-0000-004294980190",
    "type": "AccessPolicy",
    "links": {
      "self": "https://...."
    }
  },
  "id": "00505691-AED0-0ed3-0000-004294990861",
  "type": "AccessPolicyInheritanceSetting"
}
```

basePolicy—CorePolicy は Policy1 アクセスポリシーによって継承されることに注意してください。

ステップ 2 継承を変更するには、次の URL を使用します。要求 URL の containerUUID とオブジェクト ID に、変更する基本ポリシーのポリシー ID を使用します。

```
PUT api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}
/inheritancesettings/{objectId}
```

要求本文で新しい基本ポリシーとして使用するポリシー ID を指定します。

例：

Request body

```
{
  "type": "AccessPolicyInheritanceSetting",
  "id": "00505691-AED0-0ed3-0000-004294990861",
  "basePolicy": {
    "type": "AccessPolicy",
    "id": "00505691-AED0-0ed3-0000-004294999105"
  }
}
```

Response body

```
 "links": {
    "self": "https://..."
  },
  "basePolicy": {
    "id": "00505691-AED0-0ed3-0000-004294999105",
    "type": "AccessPolicy",
    "links": {
      "self": "https://..."
    }
  },
  "id": "00505691-AED0-0ed3-0000-004294990861",
  "type": "AccessPolicyInheritanceSetting"
}
```

新しい基本ポリシーが Policy1 に適用されます。

ステップ 3 Policy 1 の新しい継承設定をテストするには、次の URL を使用します。

```
GET /api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{objectId}
```

要求 URL のオブジェクト ID フィールドにポリシー ID を使用します。

例：

Request URL

```
https://<management_center_IP_or_name>/api/fmc_config/v1/domain/<domainUUID>/policy
/accesspolicies/00505691-AED0-0ed3-0000-004294990861
```

Response body

```
{
  "metadata": {
    "inherit": true,
    "parentPolicy": {
      "name": "NewCorePolicy",
      "id": "00505691-AED0-0ed3-0000-004294999105",
      "type": "AccessPolicy"
    },
    "lockingStatus": {
      "status": "UNLOCKED"
    },
   ...
   ...
    }
```

次のタスク

1. ターゲットデバイスにポリシーを再割り当てします。「アクセス コントロール ポリシーのターゲットデバイスの設定 （9 ページ）」を参照してください。

2. 設定変更を展開します。「構成の展開 （14 ページ）」を参照してください。

アクセス コントロール ポリシーのターゲットデバイスの設定

デバイスに割り当てることができるポリシーは1つだけです。ただし、複数のデバイスに同じポリシーを割り当てることができます。

始める前に

- デバイスに割り当てるアクセスポリシーが作成されていることを確認します。ポリシーを作成する方法については、「基本的なアクセス コントロール ポリシーの作成 （3 ページ）」を参照してください。
- ターゲットデバイスが設定され、有効になっていることを確認します。

手順

ステップ 1 ポリシーをデバイスに割り当てるには、デバイス ID とポリシー ID が必要です。

次の URL を使用して、ポリシーを割り当てる必要があるデバイスの ID を取得します。

```
GET api/fmc_config/v1/domain/{domainUUID}/devices/devicerecords
```

ヒント すべてのデバイスの詳細を取得するには、"?expanded=true" を追加します。

例：

Request URL

```
https://<management_center_IP_or_name>/api/fmc_config/v1/domain/<domainUUID>/devices/devicerecords?expanded=true
```

Response body

```
{
  "links": {
    "self": ….
  },
  "items": [
    {
      "id": "f862a198-e4b9-11ed-8e1d-cd2f06e0848a",
      "type": "Device",
      "links": {
        "self": "https://…"
      },
      "name": "10.10.0.67"
    },
    {
      "id": "fcf18d38-e4b8-11ed-9380-cb4dda45fa18",
      "type": "Device",
      "links": {
        "self": "https://..."
      },
      "name": "10.10.0.66"
}
```

特定のポリシー ID を取得するには、次の URL を使用します。この URL は、特定のポリシーの ID を識別できるすべてのポリシー ID を返します。

```
GET api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies
```

例：

Request URL

https://*<management_center_IP_or_name>*/api/fmc_config/v1/domain/*<domainUUID>*/policy/accesspolicies

Response body

```
{
  "links": {
    "self": "https://...."
  },
  "items": [
    {
      "type": "AccessPolicy",
      "links": {
        "self": "https://..."
      },
      "name": "Policy1",
      "id": "00505691-AED0-0ed3-0000-004294990861"
      }
```

ステップ 2 次の URL を使用してポリシー割り当てを作成します。

```
POST api/fmc_config/v1/domain/{domainUUID}/assignment/policyassignments
```

例：

Request body

```
{
  "type": "PolicyAssignment",
  "policy": {
    "type": "AccessPolicy",
    "name": "Policy1",
    "id": "00505691-AED0-0ed3-0000-004294990861"
  },
  "targets": [
    {
      "id": " f862a198-e4b9-11ed-8e1d-cd2f06e0848a",
      "type": "Device",
      "name": "10.10.0.67"
    },
    {
      "id": " fcf18d38-e4b8-11ed-9380-cb4dda45fa18",
      "type": "Device",
      "name": "10.10.0.68"
    }
  ]
}
```

Response body

```
{
  "links": {
    "self": "https://..."
  },
  "type": "PolicyAssignment",
  "policy": {
    "type": "AccessPolicy",
    "name": "Policy1",
    "defaultAction": {
      "type": "AccessPolicyDefaultAction"
    },
```

```
    "id": "00505691-AED0-0ed3-0000-004294990861"
  },
  "targets": [
    {
      "id": "fcf18d38-e4b8-11ed-9380-cb4dda45fa18",
      "name": "10.10.0.66",
      "keepLocalEvents": false
    },
    {
      "id": "f862a198-e4b9-11ed-8e1d-cd2f06e0848a",
      "name": "10.10.0.67",
      "keepLocalEvents": false
    }
  ],
  "name": "Policy1",
  "id": "00505691-AED0-0ed3-0000-004294990861"
}
```


次のタスク

- 設定変更を展開します。「構成の展開 （14 ページ）」を参照してください。

アクセス コントロール ポリシーの削除

始める前に

削除するアクセスポリシーがターゲットデバイスから割り当て解除されていることを確認します。ポリシーの削除を続行すると、応答本文に次のエラーが表示されます。

エラー 400：`"Policy In Use Policy Policy 1 or its children is assigned to a device in current domain or sub-domain. Please remove the assignments before attempting to delete."`

デバイスに割り当てられているポリシーを正常に削除するには、代替アクセスポリシーを使用してデバイスを再割り当てする必要があります。ポリシーのターゲットデバイスを設定する方法については、「アクセス コントロール ポリシーのターゲットデバイスの設定 （9ページ）」を参照してください。

手順

ステップ 1 アクセスポリシーを削除するには、ポリシーの ID が必要です。ID を取得するには、次の URL を使用します。

```
GET /api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies
```

例：

Request URL

https://*<management_center_IP_or_name>*/api/fmc_config/v1/domain/*<domainUUID>*/policy/accesspolicies

Response body


```
{
```

```
  "links": {
    "self": "https://...."
  },
  "items": [
    {
      "type": "AccessPolicy",
      "links": {
        "self": "https://..."
      },
      "name": "Policy1",
      "id": "00505691-AED0-0ed3-0000-004294990861"
    },
    {
      "type": "AccessPolicy",
      "links": {
        "self": "https://..."
      },
      "name": "Policy2",
      "id": "00505691-64F9-0ed3-0000-004294969027"
    }
```

ステップ 2 次の URL を使用して、アクセスポリシーがデバイスに割り当てられているかどうかを確認します。

```
GET api/fmc_config/v1/domain/{domainUUID}/assignment/policyassignments/{objectId}
```

[要求URL（Request URL）] でポリシー ID を指定します。

例：

Request URL

https://*<management_center_IP_or_name>*/api/fmc_config/v1/domain/*<domainUUID>*/assignment/policyassignments/{objectId}

Response body

```
{
  "links": {
    "self": "https://...."
  },
  "type": "PolicyAssignment",
  "policy": {
    "type": "AccessPolicy",
    "id": "00505691-64F9-0ed3-0000-004294969027",
    "name": "Policy2"
  },
  "targets": [
    {
      "id": "931837d8-8cef-11ee-9dd7-82aa44a9ed90",
      "type": "Device",
      "name": "10.10.0.6",
      "keepLocalEvents": false
    }
```

ここで、削除するポリシーにデバイスが割り当てられていることを確認できます。ポリシーにマッピングされているデバイスがない場合は、ステップ 4 に進みます。

ステップ 3 次の URL を使用して、別のポリシー（たとえば、Policy 1）をターゲットデバイスに再割り当てします。

```
PUT api/fmc_config/v1/domain/{domainUUID}/assignment/policyassignments/{objectId}
```

代替ポリシーの ID を要求 URL のオブジェクト ID として使用します。

例：

Request URL

https://*<management_center_IP_or_name>*/api/fmc_config/v1/domain/*<domainUUID>*/assignment/policyassignments/00505691-AED0-0ed3-0000-004294990861

Response body

```
{
  "type": "PolicyAssignment",
  "id": "policyassignmentUUID",
  "policy": {
    "type": "AccessPolicy",
    "name": "Policy1",
    "id": "00505691-AED0-0ed3-0000-004294990861"
  },
  "targets": [
    {
      "id": "931837d8-8cef-11ee-9dd7-82aa44a9ed90",
      "type": "Device",
      "name": "10.10.0.6"
    }
  ]
}
```

ステップ 4 次の URL を使用してポリシーを削除します。

```
DELETE api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{objectId}
```

要求 URL のオブジェクト ID として、削除するポリシーの ID を使用します。

例：

Request URL

https://*<management_center_IP_or_name>*/api/fmc_config/v1/domain/*<domainUUID>*/policy/accesspolicies/00505691-64F9-0ed3-0000-004294969027

Response body

```
{
  "metadata": {
    "inherit": false,
    "lockingStatus": {
      "status": "UNLOCKED"
    },
    "timestamp": 1702489999184,
    "lastUser": {
      "name": "user"
    },
    "domain": {
      "name": "Global",
      "id": "e276abec-e0f2-11e3-8169-6d9ed49b625f",
      "type": "Domain"
    }
  },
  "type": "AccessPolicy",
  "links": {
    "self": "https://...."
  },
  "rules": {
    "refType": "list",
    "links": {
      "self": "https://..."
    },
    "type": "AccessRule"
```

```
  },
  "securityIntelligence": {
    "id": "00505689-14EC-0ed3-0000-004294970406",
    "type": "SecurityIntelligencePolicy",
    "links": {
      "self": "https://...."
    }
  },
  "prefilterPolicySetting": {
    "id": "4897c8f4-e211-4661-b0a4-25b0826cded9",
    "type": "PrefilterPolicy",
    "name": "Default Prefilter Policy"
  },
  "defaultAction": {
    "enableSyslog": false,
    "sendEventsToFMC": false,
    "logBegin": false,
    "logEnd": false,
    "type": "AccessPolicyDefaultAction",
    "action": "BLOCK",
    "id": "00505689-14EC-0ed3-0000-000268434433"
  },
  "name": "Policy2",
  "id": "00505691-64F9-0ed3-0000-004294969027"
}
```


構成の展開

新規または変更された設定を展開するには、デバイス ID とバージョンが必要です。

手順

ステップ 1 次の URL を使用して、展開可能なデバイスのバージョンを取得します。

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

例：

Request URL

https://*<management_center_IP_or_name>*/api/fmc_config/v1/domain/*<domainUUID>*/deployment/deployabledevices

Response body


```
{
  "links": {
    "self": "https://..."
  },
  "items": [
    {
      "version": "1688031258587",
      "name": "192.168.0.155",
      "type": "DeployableDevice"
    },
    {
      "version": "1688031258587",
      "name": "192.168.0.124",
      "type": "DeployableDevice"
    }
```

ステップ 2 設定変更を展開します。

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

バージョン ID とデバイス ID を使用して、要求本文に設定を展開します。

例：

Request body

```
{
  "type": "DeploymentRequest",
  "version": "1688031258587",
  "forceDeploy": false,
  "ignoreWarning": true,
  "deviceList": [
    "9670dd78-13e5-11ee-a01c-995c31db76ce",
"9aaf35ec-13e5-11ee-b58e-b9c3aa43807a"
  ],
  "deploymentNote": "deploying access policies"
}
```

Response body

```
{
  "version": "1688031258587",
  "metadata": {
    "task": {
      "id": "4295001488",
      "links": {
        "self": "https://..."
      }
    }
  },
  "deviceList": [
    "9670dd78-13e5-11ee-a01c-995c31db76ce",
    "9aaf35ec-13e5-11ee-b58e-b9c3aa43807a"
  ],
  "forceDeploy": false,
  "ignoreWarning": true,
  "deploymentNote": "deploying access policies",
  "type": "DeploymentRequest"
}
```

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。