Secure Firewall Management Center REST APIs for Access Control Policy

First Published: 2024-01-16

REST APIs for Access Control Policies

Cisco Secure Firewall Management Center APIs can be used to create and manage access policies, access rules, and other access policy objects. This document provides the procedure to manage a basic access control policy. Information about access rules and other policy objects are outside the scope of this document.

The Policy APIs allow you to:

1. Create an access control policy for the managed firewall devices to protect your network from unauthorized access, malware infections, data breaches, and other security threats.
2. (Optional) Lock a policy to ensure that your rules are not overwritten by another user.
3. (Optional) Create a custom policy using the inheritance functionality.
4. (Optional) Delete an access control policy that is obsolete and is no longer needed.
5. Deploy the new or modified policy configurations on the devices whenever you modify the policies.

Endpoints and Methods Used

1 Authenticate Token
2 Refresh Token
3 Create a Basic Access Control Policy
4 Edit an Access Control Policy
5 Lock an Access Control Policy
6 Manage Access Control Policy Inheritance
7 Delete an Access Control Policy
8 Set Target Devices for an Access Control Policy

Important Terms in Management Center REST APIs

- DomainUUID—The Global domain UUID. This ID is always going to be the same in all the management centers, irrespective of their version. If you create a new domain in your management center and a specific

user for the newly created domain, a new domain UUID is displayed on the API console of the management center.

- ContainerUUID—The parent object's UUID that connects the object to the overall schema. For example, to get the physical interfaces, use the device ID as the container UUID in the following URL:

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

- ObjectID—The ID of the target object. For example, to get details about a physical interface, use the interface id as the Object ID in the following URL:

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

Create a Basic Access Control Policy

An access policy comprises the following components:

- Traffic matching criteria—Security Zone, IP Address or Geo Location, Port Number, Protocol, Application Type, URL Pattern, URL Category, URL Reputation, and Users.
- Action on matching traffic—Allow, Block, Trust, Monitor.
- An intrusion prevention policy, a file policy, or both for the Allow action categories.

Note You can assign only one policy to a threat defense device. However, you can assign the same policy to several devices.

Before you begin

Ensure that you have the appropriate authorization to use the REST APIs resource. See the Authentication from a REST API Client section of the Secure Firewall Management Center REST API Quick Start Guide.

Procedure

Create an access control policy using the following URL:

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

Example:

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"
}
```

A policy is created with the specified name and a unique ID.

What to do next

1. Assign policy to target devices. See Set Target Devices for an Access Control Policy, on page 8.
2. Deploy configuration changes. See Deploy a Configuration, on page 13.

Edit an Access Control Policy

Before you begin

Ensure that you have created an access policy that you want to modify or edit. For information about how to create a policy, see Create a Basic Access Control Policy, on page 3.

Procedure

Step 1 To edit an access policy, you require the ID of the policy. To get the ID, use the following URL:

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

Example:

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"
  }
```

Step 2 Edit the access control policy using the following URL:

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

In this example, to edit the Policy 1 parameters, use the policy ID (00505691-AED0-0ed3-0000-004294990861) as the Object ID in the Request body.

Note Ensure that you deploy the modified configuration for the updates to take effect.

What to do next

- Deploy configuration changes. See Deploy a Configuration, on page 13.

Lock an Access Control Policy

By default, access policies are not locked. You can lock them if you do not want any other user to modify the rules or settings.

Before you begin

Ensure that you have created an access policy that you want to lock. For information about how to create a policy, see Create a Basic Access Control Policy, on page 3.

Procedure

Step 1 To lock an access policy, you need the ID of the policy. To get the ID, use the following URL:

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

Step 2 To lock an access policy, use the following URL:

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

Specify the policy ID in the Request body.

Example:

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"
        }
      }
    }
  ]
}
```

To unlock the policy, use the POST method and specify "lock": "false" in the Request body.

The policy is locked and other users cannot modify the policy.

Manage Access Control Policy Inheritance

The inheritance feature allows you to apply some baseline characteristics from one policy to multiple policies. You can use a policy as a base policy for another access control policy.

Procedure

Step 1 To view an existing inheritance setting for a policy, use the following URL:

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

Use the policy ID for the containerUUID and object ID fields in the Request URL

Example:

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"
}
```

Notice that the basePolicy—CorePolicy is inherited by the Policy1 access policy.

Step 2 To modify the inheritance, use the following URL. Use the policy ID, whose base policy you want to change, for the containerUUID and object ID in the Request URL.

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

Specify the policy ID that you want to use as the new base policy in the Request body.

Example:

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"
}
```

The new base policy is applied to Policy1.

Step 3 To test the new inheritance settings for Policy 1, use the following URL:

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

Use the policy ID for the object ID field in the Request URL.

Example:

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"
    },
   ...
   ...
    }
```

What to do next

1. Re-assign policy to target devices. See Set Target Devices for an Access Control Policy, on page 8.
2. Deploy configuration changes. See Deploy a Configuration, on page 13.

Set Target Devices for an Access Control Policy

You can assign only one policy to a device. However, you can assign the same policy to several devices.

Before you begin

- Ensure that you have created the access policy to be assigned to devices. For information about how to create a policy, see Create a Basic Access Control Policy, on page 3.
- Ensure that you have configured the target devices and enabled them.

Procedure

Step 1 To assign a policy to devices, you require the devices IDs and policy ID.

Get the IDs of the devices to which the policy must be assigned using the following URL:

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

Tip Append "?expanded=true" to get all the device details.

Example:

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"
}
```

Use the following URL to get the specific policy ID. The URL returns all policy IDs from which you can identify the ID of the specific policy.

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

Example:

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"
      }
```

Step 2 Create policy assignment using the following URL:

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

Example:

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"
}
```

What to do next

- Deploy configuration changes. See Deploy a Configuration, on page 13.

Delete an Access Control Policy

Before you begin

Ensure that the access policy that you want to delete is unassigned from the target devices. If you proceed to delete the policy, the following error will appear in the Response body:

ERROR 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."`

To sucessfully delete the policy that is assigned to devices, you must reassign the devices with an alternative access policy. For information about how to set the target devices for a policy, see Set Target Devices for an Access Control Policy, on page 8.

Procedure

Step 1 To delete an access policy, you require the ID of the policy. To get the ID, use the following URL:

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

Example:

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"
    }
```

Step 2 Verify if the access policy is assigned to any device using the following URL:

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

Specify the policy ID in the Request URL.

Example:

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
    }
```

Here, you can see that a device is assigned to the policy that you want to delete. If no devices are mapped to the policy, go to Step 4.

Step 3 Reassign another policy, for example, Policy 1 to the target device using the following URL:

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

Use the ID of the alternative policy as the Object ID in the Request URL.

Example:

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"
    }
  ]
}
```

Step 4 Delete the policy using the following URL:

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

Use the ID of the policy that you want to delete as the Object ID in the Request URL.

Example:

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"
}
```


Deploy a Configuration

To deploy a new or modified configuration, you require the device ID and version.

Procedure

Step 1 Procure the deployable device version using the following URL:

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

Example:

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"
    }
```

Step 2 Deploy the configuration changes:

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

Use the version ID and device ID to deploy the configuration in the Request body.

Example:

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"
}
```