Configure a Time-Based Access Control Rule on FDM with Rest API

Contents

Introduction

This document describes how to configure and validate a Time-Based access control rule on the FTD managed by FDM with Rest API.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Secure Firewall Threat Defense (FTD)
- Firepower Device Management (FDM)
- Knowledge of Representational State Transfer Application Programming Interface (REST API)
- Access Control List (ACL)

Components Used

The information in this document is based on FTD version 7.1.0.

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. If your network is live, ensure that you understand the potential impact of any command.

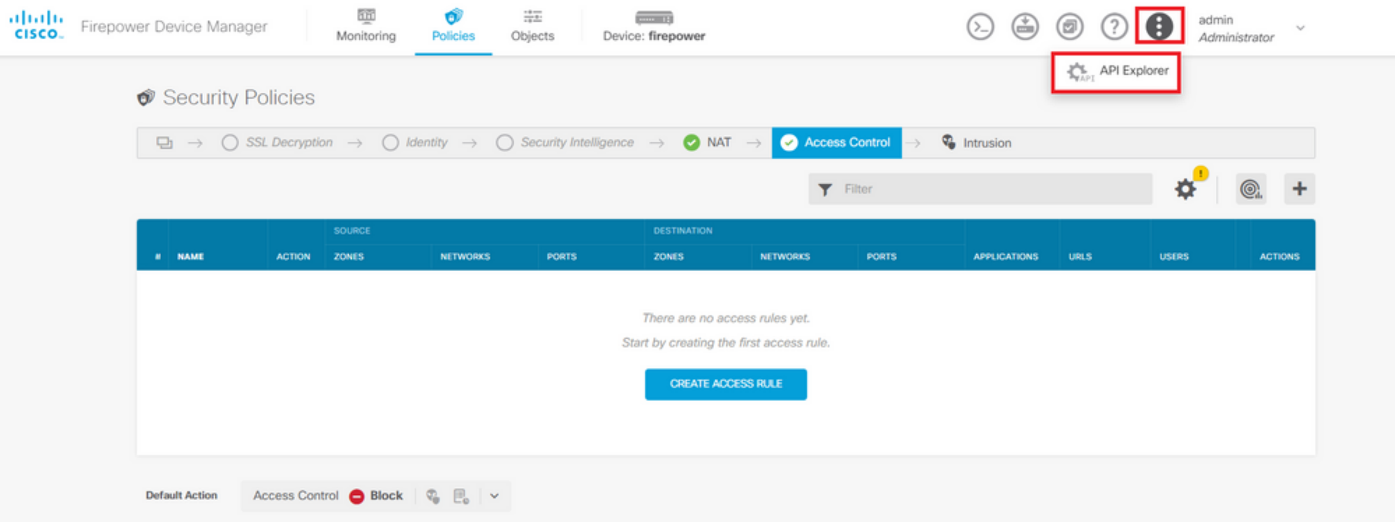
Background Information

FTD API version 6.6.0 and later support access control rules that are limited based on time.

Using the FTD API, you can create time range objects, which specify one-time or recurring time ranges, and apply these objects to access control rules. Using time ranges, you can apply an access control rule to traffic during certain times of day, or for certain periods of time, in order to provide flexibility to network usage. You cannot use FDM in order to create or apply time ranges, nor does FDM show you if an access control rule has a time range applied to it.

Configure

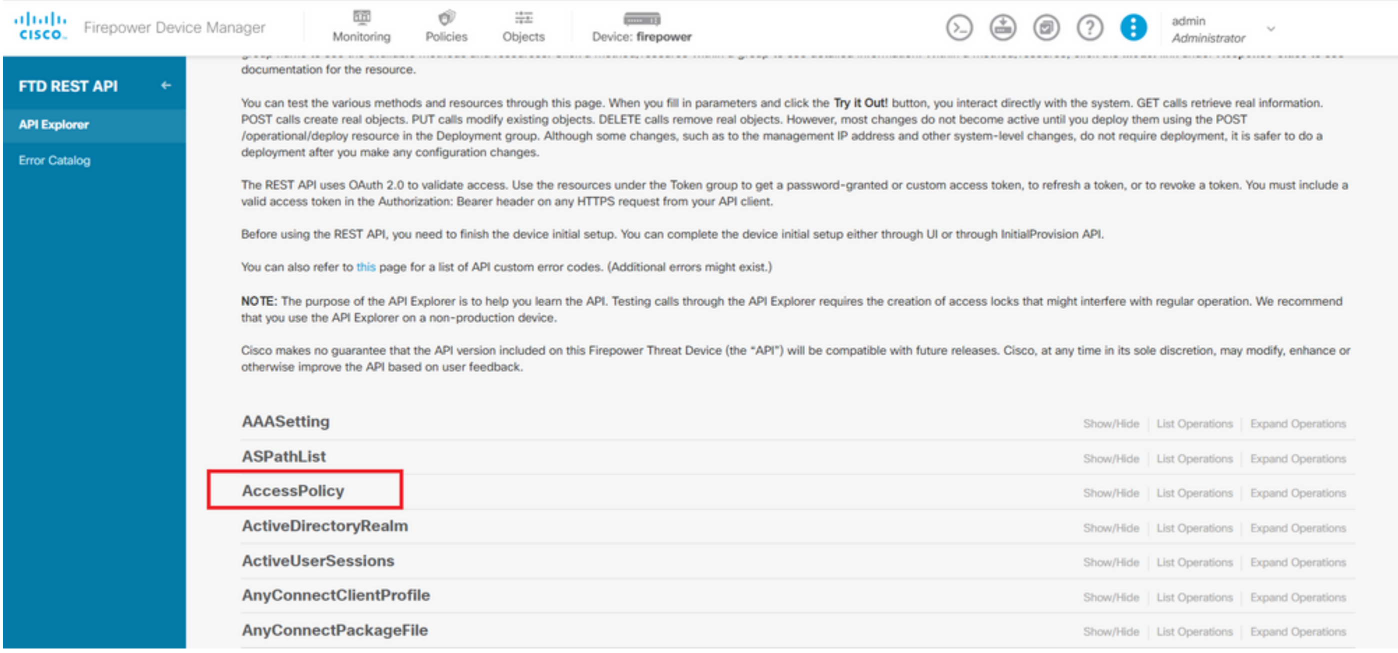
Step 1. Click the advanced options (Kebab menu) in order to open the FDM API explorer.



There are no access rules yet.
Start by creating the first access rule.

Image 1. FDM web user interface.

Step 2. Choose the category **AccessPolicy** in order to display the different API calls.



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.)

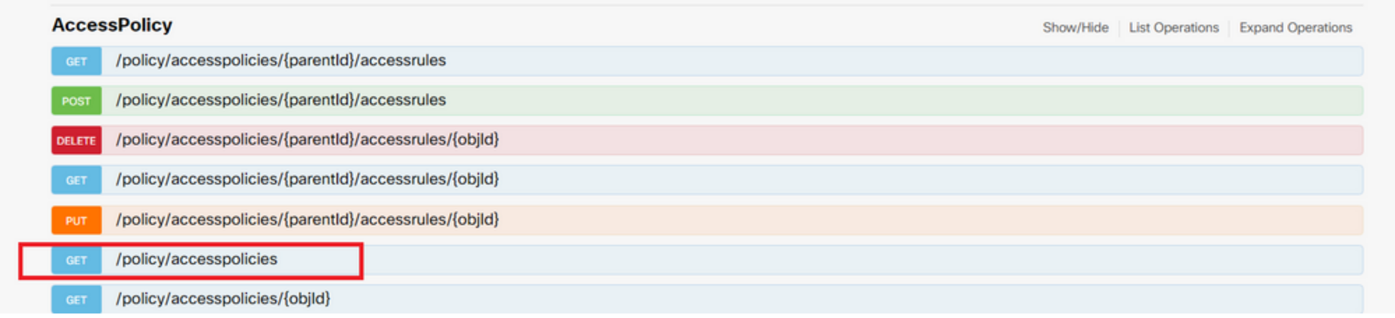
NOTE: The purpose of the API Explorer is to help you learn the API. Testing calls through the API Explorer requires the creation of access locks that might interfere with regular operation. We recommend that you use the API Explorer on a non-production device.

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
ActiveDirectoryRealm — Show/Hide | List Operations | Expand Operations
ActiveUserSessions — Show/Hide | List Operations | Expand Operations
AnyConnectClientProfile — Show/Hide | List Operations | Expand Operations
AnyConnectPackageFile — Show/Hide | List Operations | Expand Operations

Image 2. API Explorer web user interface.

Step 3. Run the **GET** call in order to obtain the Access Policy ID.

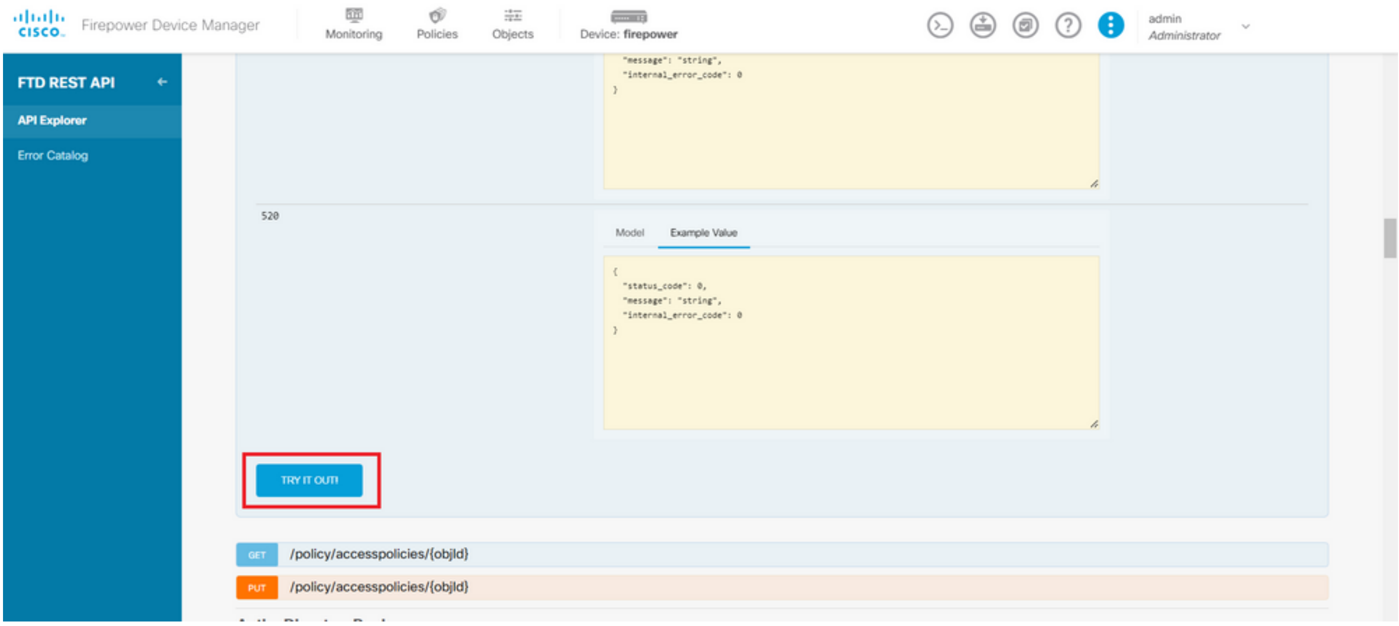


AccessPolicy — Show/Hide | List Operations | Expand Operations

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
GET /policy/accesspolicies/{objId}

Image 3. Access Policy category.

Step 4. You must hit on TRY IT OUT! in order to retrieve the API response.



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

520

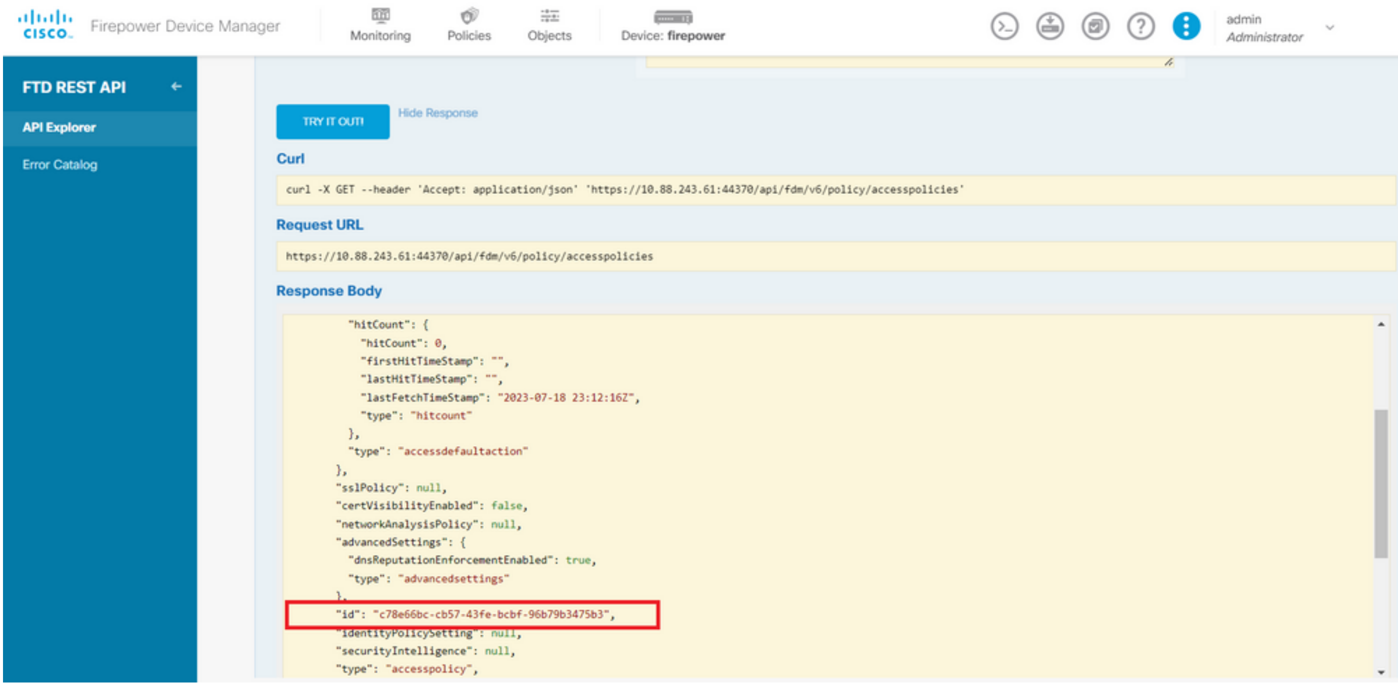
```
{
"status_code": 0,
"message": "string",
"internal_error_code": 0
}
```

GET /policy/accesspolicies/{objId}

PUT /policy/accesspolicies/{objId}

Image 4. TRY IT OUT! button which runs the API call.

Step 5. Copy the JSON data from the response body to a notepad. Later, you must use the Access Control Policy ID.



Curl

```
curl -X GET --header 'Accept: application/json' 'https://10.88.243.61:44370/api/fdm/v6/policy/accesspolicies'
```

Request URL

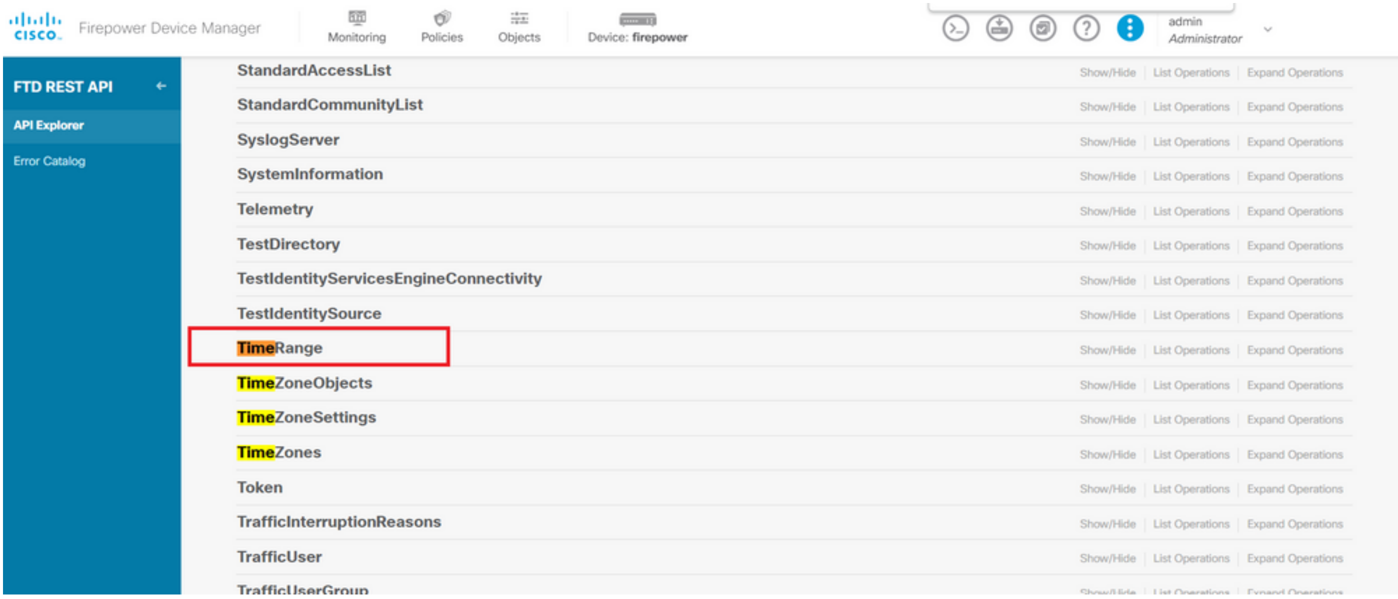
```
https://10.88.243.61:44370/api/fdm/v6/policy/accesspolicies
```

Response Body

```
      "hitCount": {
        "hitCount": 0,
        "firstHitTimeStamp": "",
        "lastHitTimeStamp": "",
        "lastFetchTimeStamp": "2023-07-18 23:12:16Z",
        "type": "hitcount"
      },
      "type": "accessdefaultaction"
    },
    "sslPolicy": null,
    "certVisibilityEnabled": false,
    "networkAnalysisPolicy": null,
    "advancedSettings": {
      "dnsReputationEnforcementEnabled": true,
      "type": "advancedsettings"
    },
    "id": "c78e66bc-cb57-43fe-bcbf-96b79b3475b3",
    "identityPolicySetting": null,
    "securityIntelligence": null,
    "type": "accesspolicy",
```

Image 5. GET response from Access Policy.

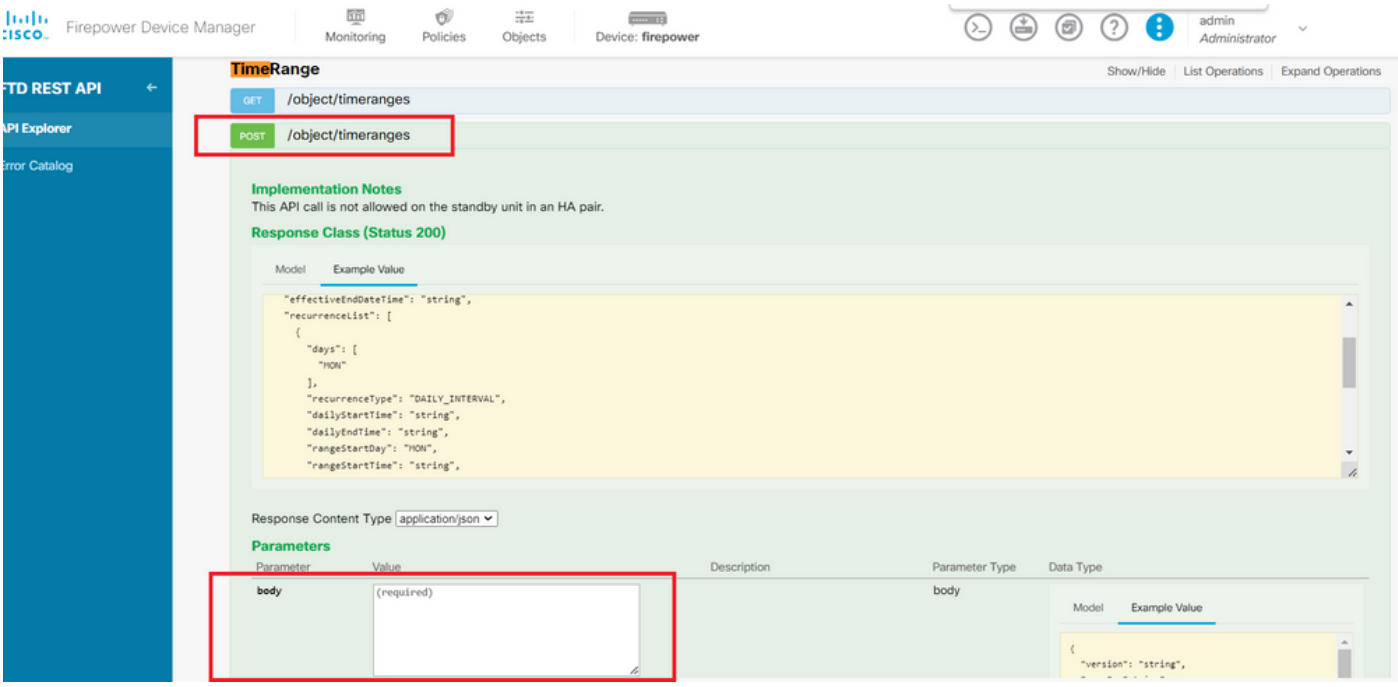
Step 6. Find and open the TimeRange category on the API Explorer in order to display the different API calls.



StandardAccessList
StandardCommunityList
SyslogServer
SystemInformation
Telemetry
TestDirectory
TestIdentityServicesEngineConnectivity
TestIdentitySource
TimeRange
TimeZoneObjects
TimeZoneSettings
TimeZones
Token
TrafficInterruptionReasons
TrafficUser
TrafficUserGroup

Image 6. Time Range category.

Step 7. Create as many TimeRange objects as you want by using the **POST** API call.



TimeRange

GET /object/timeranges

POST /object/timeranges

Implementation Notes

This API call is not allowed on the standby unit in an HA pair.

Response Class (Status 200)

```
  "effectiveEndDateTime": "string",
  "recurrenceList": [
    {
      "days": [
        "MON"
      ],
      "recurrenceType": "DAILY_INTERVAL",
      "dailyStartTime": "string",
      "dailyEndTime": "string",
      "rangeStartDay": "MON",
      "rangeStartTime": "string",
```

Response Content Type application/json

Parameters

body (required) body

```
{
  "version": "string",
```

Image 7. Time Range POST call.

Find here a couple of JSON format examples to create two different TimeRange objects.

Object 1:

```
<#root>
{
  "name": "
range-obj-1
",
  "recurrenceList": [
    {
      "days": [
        "MON",
        "TUE",
        "WED",
        "THU",
        "FRI"
      ],
      "recurrenceType": "DAILY_INTERVAL",
      "dailyStartTime": "

00:00

",
      "dailyEndTime": "

23:50

",
      "type": "recurrence"
    }
  ],
  "type": "timerangeobject"
}
```

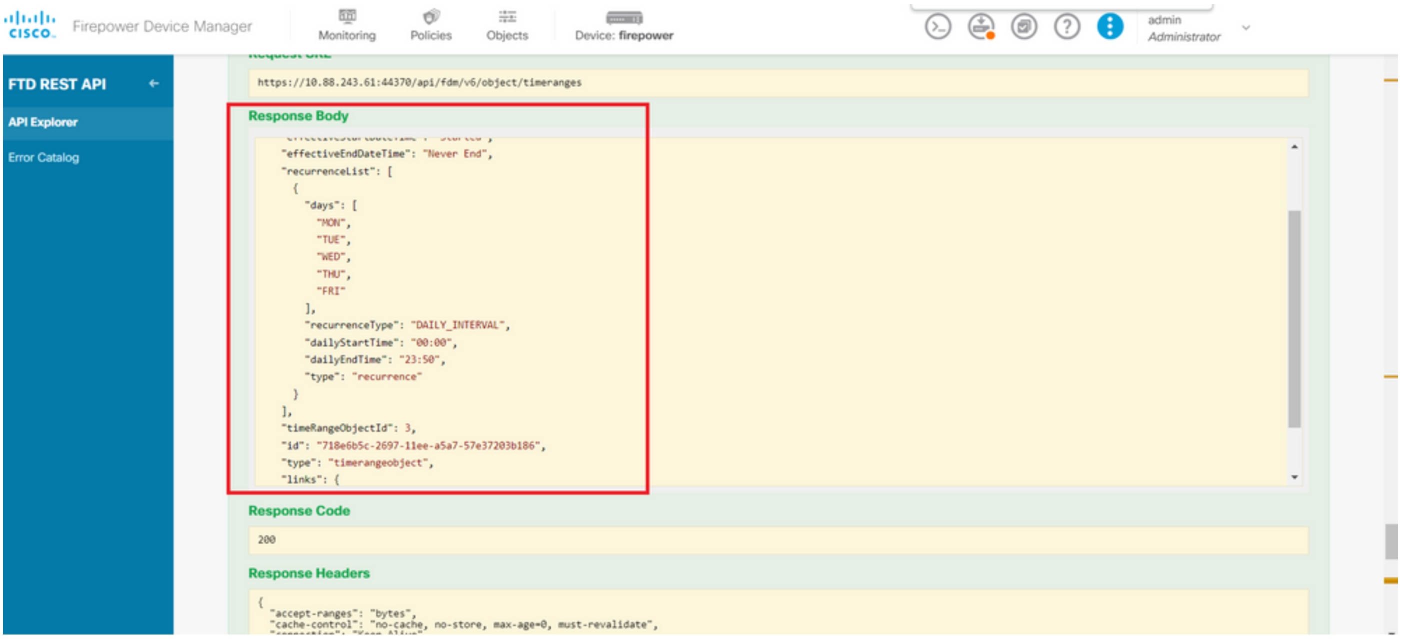
Object 2:

<#root>

```
{

  "name": "

range-obj-2

",
  "recurrenceList": [
    {
      "days": [
        "MON"
      ],
      "recurrenceType": "DAILY_INTERVAL",
      "dailyStartTime": "

12:00

",
      "dailyEndTime": "

13:00

",
      "type": "recurrence"
    }
  ],
  "type": "timerangeobject",
}
```

Note: Remember to hit on **TRY IT OUT!** in order to run the API calls.

Step 8. Run the GET call to obtain the TimeRange object IDs.



```
https://10.88.243.61:44370/api/fdm/v6/object/timeranges
```

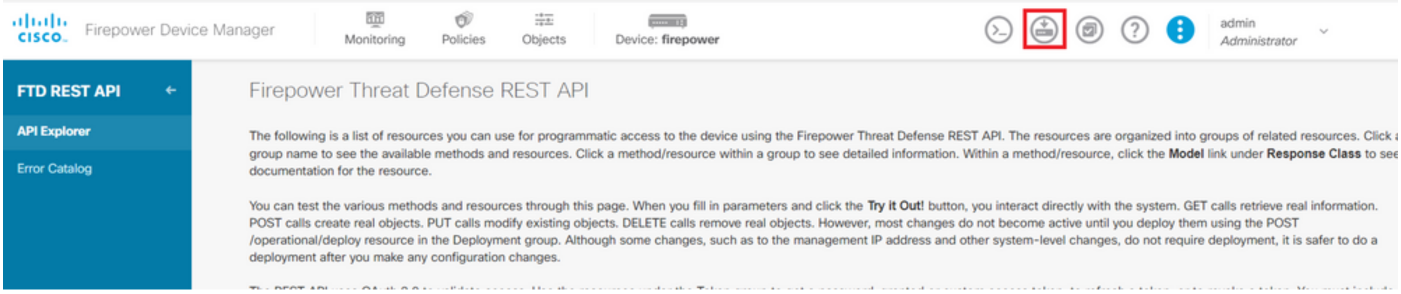
```
    "effectiveEndDateTime": "Never End",
    "recurrenceList": [
      {
        "days": [
          "MON",
          "TUE",
          "WED",
          "THU",
          "FRI"
        ],
        "recurrenceType": "DAILY_INTERVAL",
        "dailyStartTime": "00:00",
        "dailyEndTime": "23:50",
        "type": "recurrence"
      }
    ],
    "timeRangeObjectId": 3,
    "id": "718e6b5c-2697-11ee-a5a7-57e37203b186",
    "type": "timerangeobject",
    "links": {
```

```
200
```

```
{
  "accept-ranges": "bytes",
  "cache-control": "no-cache, no-store, max-age=0, must-revalidate",
```

Image 8. GET response from Time Range.

Step 9. Click the Deploy button in order to validate and apply your changes.



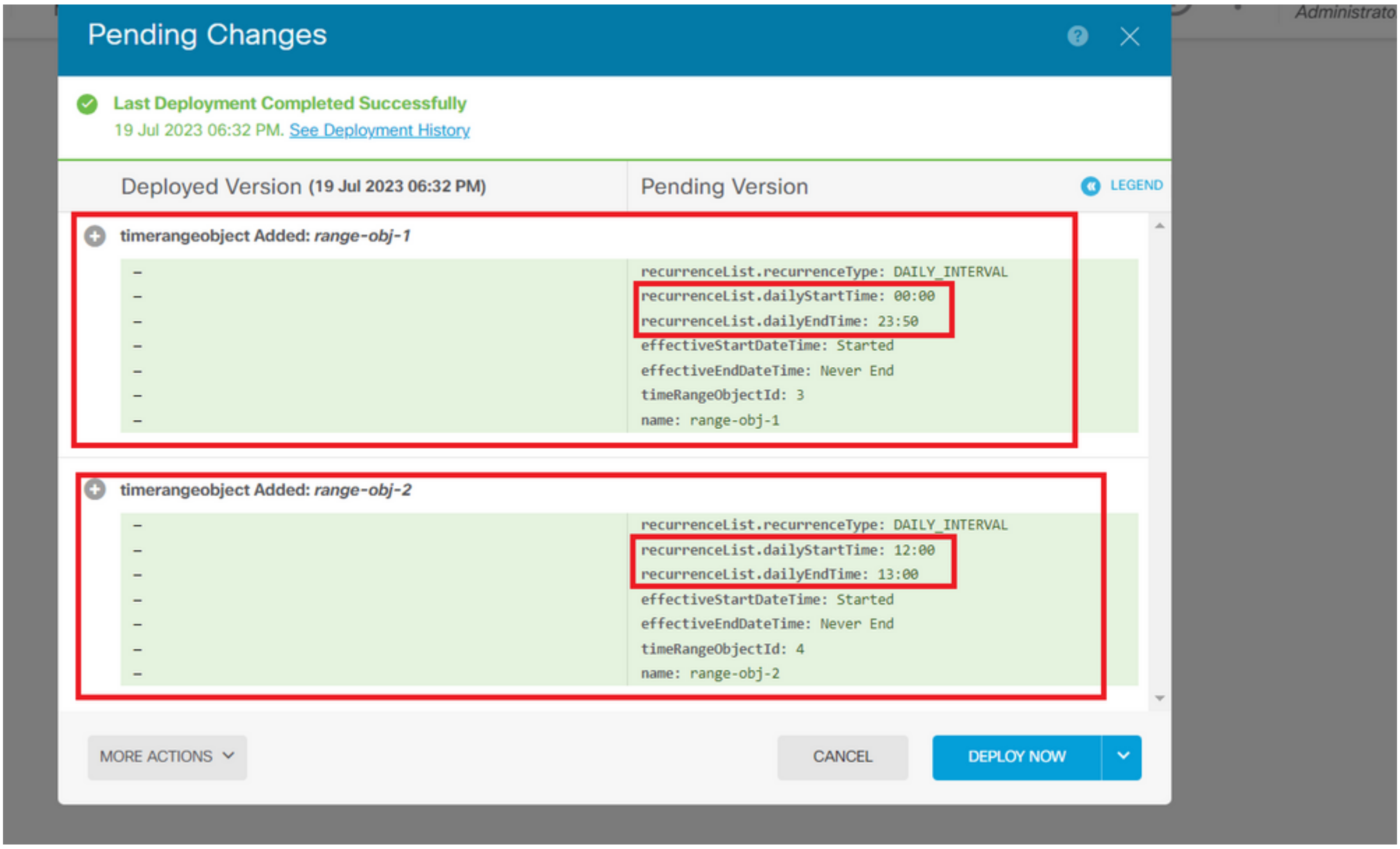
Firepower Threat Defense REST API

The following is a list of resources you can use for programmatic access to the device using the Firepower 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.

Image 9. Deploy button available from API explorer.

Step 10. Validate the configuration you just created and click **DEPLOY NOW**.



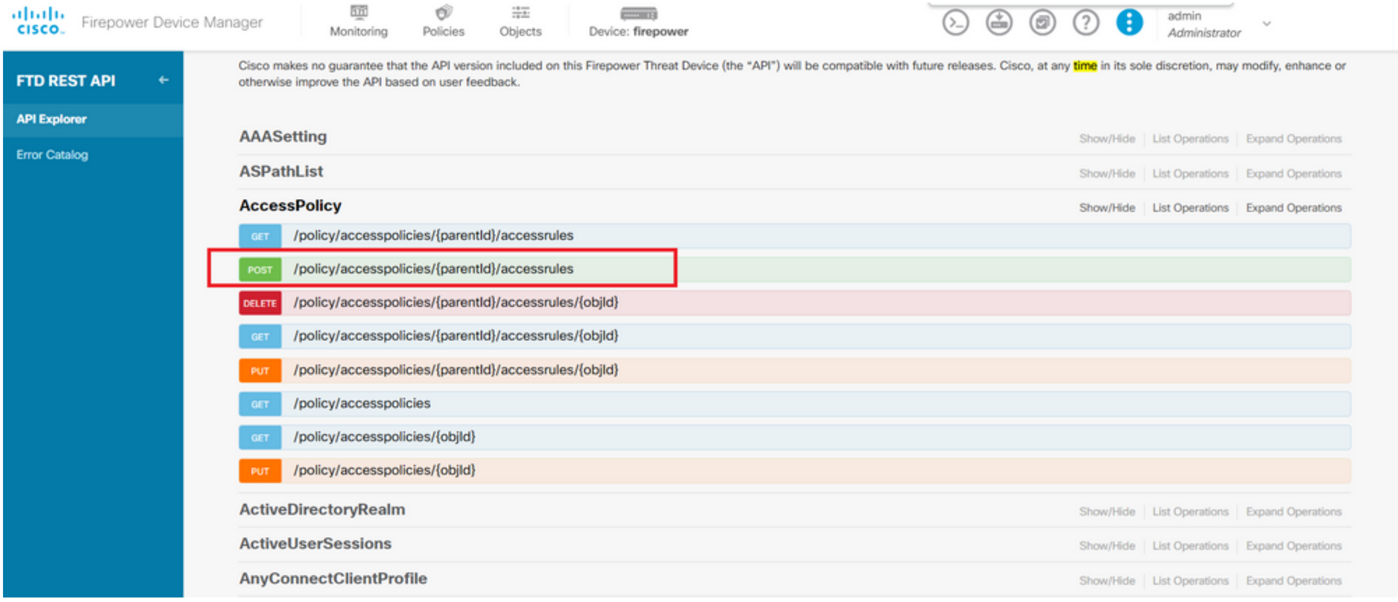
Pending Changes

✓ Last Deployment Completed Successfully
19 Jul 2023 06:32 PM. See Deployment History

Deployed Version (19 Jul 2023 06:32 PM)	Pending Version
timerangeobject Added: *range-obj-1*	
–	recurrenceList.recurrenceType: DAILY_INTERVAL
–	recurrenceList.dailyStartTime: 00:00
–	recurrenceList.dailyEndTime: 23:50
–	effectiveStartDateTime: Started
–	effectiveEndDateTime: Never End
–	timeRangeObjectId: 3
–	name: range-obj-1
timerangeobject Added: *range-obj-2*	
–	recurrenceList.recurrenceType: DAILY_INTERVAL
–	recurrenceList.dailyStartTime: 12:00
–	recurrenceList.dailyEndTime: 13:00
–	effectiveStartDateTime: Started
–	effectiveEndDateTime: Never End
–	timeRangeObjectId: 4
–	name: range-obj-2

Image 10. FDM Pending Changes window.

Step 11. Find the AccessPolicy category and open the **POST** call in order to create a time-based access control rule.



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

```
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
GET     /policy/accesspolicies/{objId}
PUT     /policy/accesspolicies/{objId}
```

ActiveDirectoryRealm — Show/Hide | List Operations | Expand Operations

ActiveUserSessions — Show/Hide | List Operations | Expand Operations

AnyConnectClientProfile — Show/Hide | List Operations | Expand Operations

Image 11. Access Policy POST call.

Find here a JSON format example to create the time-based ACL which allows traffic from the Inside to the Outside zone.

Ensure to use the correct Time Range object ID.

<#root>

```
{
  "name": "test_time_range_2",
  "sourceZones": [
    {
          "name": "inside_zone",
          "id": "90c377e0-b3e5-11e5-8db8-651556da7898",
          "type": "securityzone"
    }
  ],
  "destinationZones": [
    {
      "name": "outside_zone",
      "id": "b1af33e1-b3e5-11e5-8db8-afdc0be5453e",
      "type": "securityzone"
    }
  ],
  "ruleAction": "PERMIT",
  "eventLogAction": "
```

`LOG_FLOW_END`

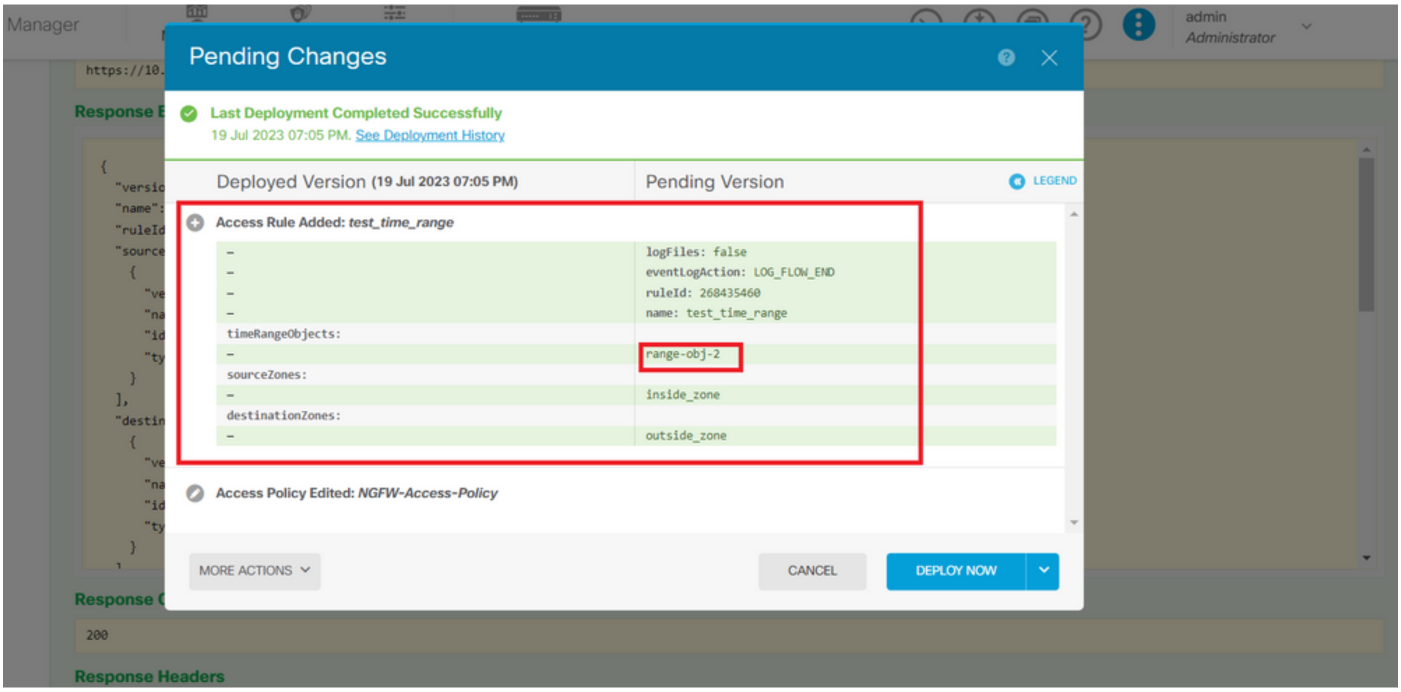
```
",
  "timeRangeObjects": [
    {
    "id": "
```

`718e6b5c-2697-11ee-a5a7-57e37203b186`

```
",
    "type": "timerangeobject",
    "name": "Time-test2"
    }
  ],
  "type": "accessrule"
}
```

Note: eventLogAction must be **LOG_FlOW_END** in order to log the event at the end of the flow, otherwise it gives an error.

Step 12. Deploy the changes in order to apply the new time-based ACL. The Pending Changes prompt must display the time range object used in Step 10.



Pending Changes

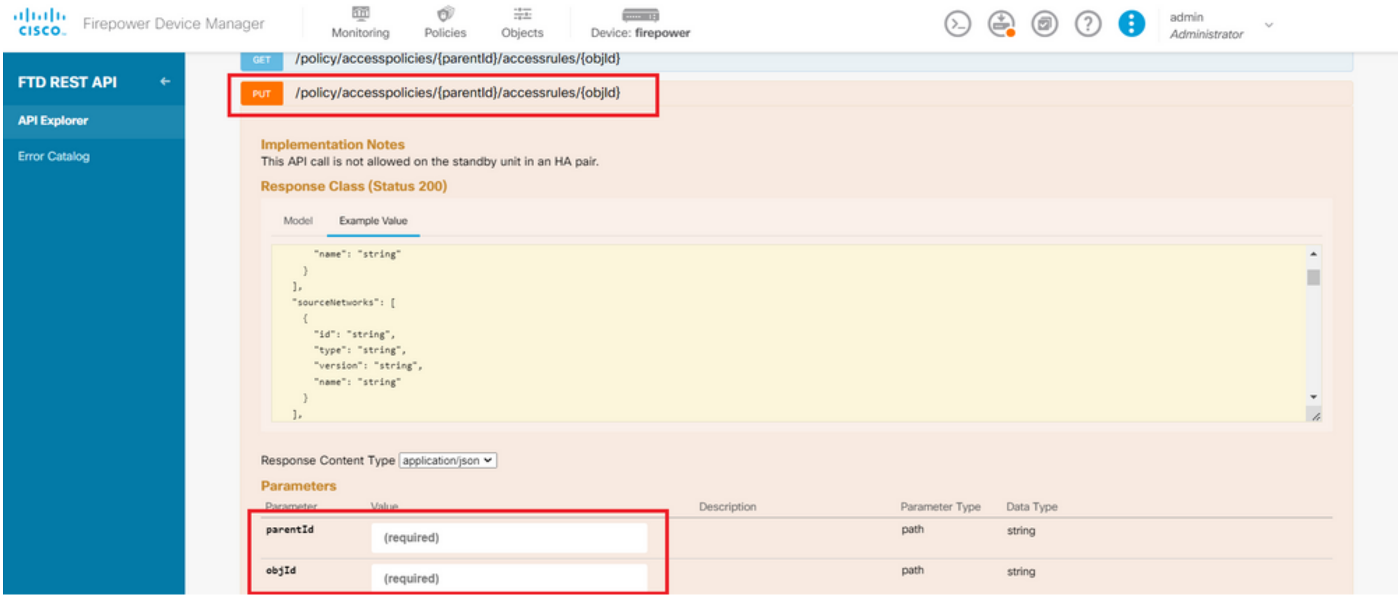
Last Deployment Completed Successfully
19 Jul 2023 07:05 PM. See Deployment History

Deployed Version (19 Jul 2023 07:05 PM)	Pending Version
Access Rule Added: *test_time_range*	
-	logFiles: false
-	eventLogAction: LOG_FLOW_END
-	ruleId: 268435460
-	name: test_time_range
timeRangeObjects:	
-	range-obj-2
sourceZones:	
-	inside_zone
destinationZones:	
-	outside_zone

Access Policy Edited: *NGFW-Access-Policy*

Image 12. FDM Pending Changes window displays the new rule.

Step 13 (Optional). If you want to edit the ACL, you can use the PUT call and edit the time range ID.



GET /policy/accesspolicies/{parentId}/accessrules/{objId}

PUT /policy/accesspolicies/{parentId}/accessrules/{objId}

Implementation Notes
This API call is not allowed on the standby unit in an HA pair.

Response Class (Status 200)

```
      "name": "string"
    }
  ],
  "sourceNetworks": [
    {
      "id": "string",
      "type": "string",
      "version": "string",
      "name": "string"
    }
  ],
```

Response Content Type application/json

Parameters

Parameter	Value	Description	Parameter Type	Data Type
parentId	(required)		path	string
objId	(required)		path	string

Image 13. Access Policy PUT call.

Find here the JSON format example in order to edit the time range, these time range IDs can be collected by using theGET call.

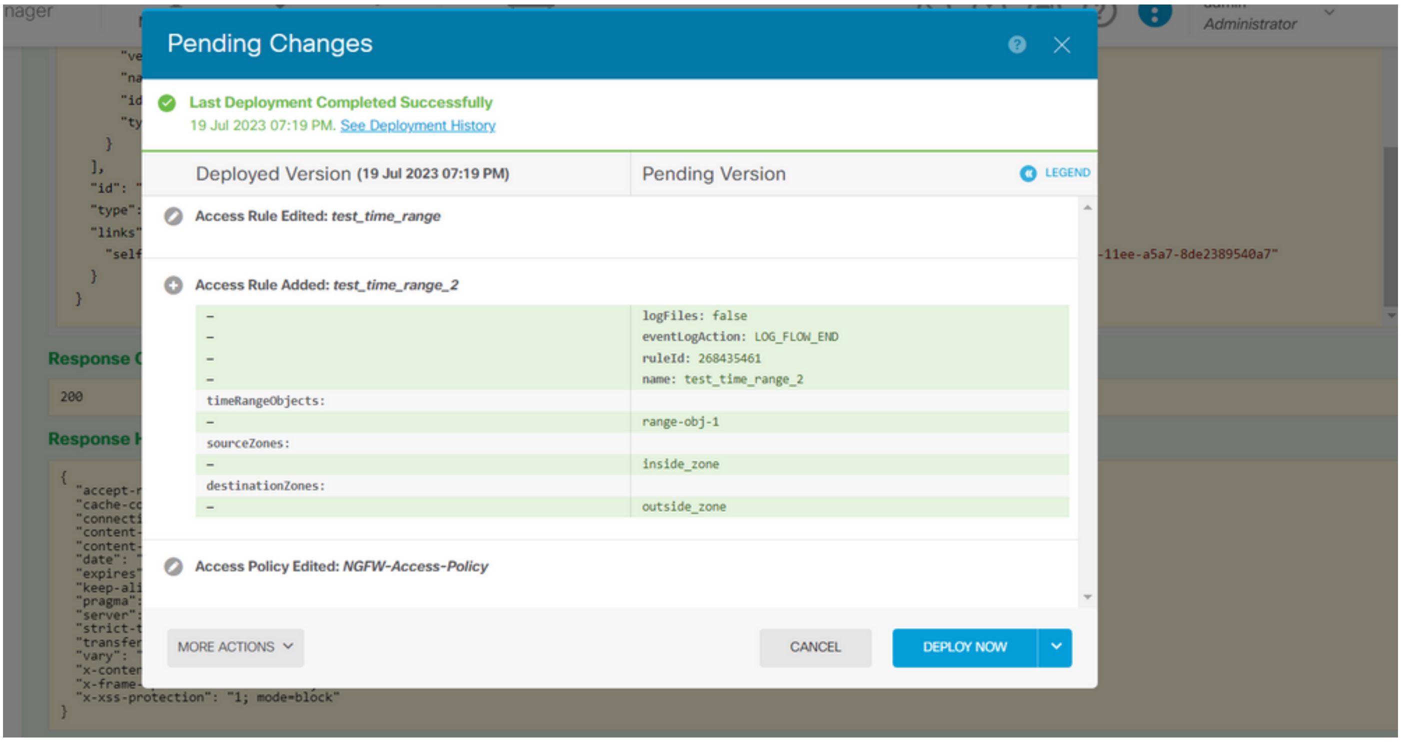
<#root>

```
{
"version": "flya3jw7wvqg7",
"name": "test_time_range",
"ruleId": 268435460,
"sourceZones": [
{
"version": "lypkhscmwq4bq",
"name": "inside_zone",
"id": "90c377e0-b3e5-11e5-8db8-651556da7898",
"type": "securityzone"
}
],
"destinationZones": [
{
"version": "pytctz6vvfb3i",
"name": "outside_zone",
"id": "b1af33e1-b3e5-11e5-8db8-afdc0be5453e",
"type": "securityzone"
}
],
"sourceNetworks": [],
"destinationNetworks": [],
"sourcePorts": [],
"destinationPorts": [],
"ruleAction": "PERMIT",
"eventLogAction": "LOG_FLOW_END",
"identitySources": [],
"users": [],
"embeddedAppFilter": null,
"urlFilter": null,
"intrusionPolicy": null,
"filePolicy": null,
"logFiles": false,
"syslogServer": null,
"destinationDynamicObjects": [],
"sourceDynamicObjects": [],
"timeRangeObjects": [
{
"version": "i3iohbd5iufol",
"name": "range-obj-1",
"id": "
```

718e6b5c-2697-11ee-a5a7-57e37203b186

```
",
"type": "timerangeobject"
}
],
"id": "0f2e8f56-269b-11ee-a5a7-6f90451d6efd",
"type": "accessrule"
}
```

Step 14. Deploy and validate your changes.



Pending Changes

Last Deployment Completed Successfully

19 Jul 2023 07:19 PM. See Deployment History

Access Rule Edited: *test_time_range*

Access Rule Added: *test_time_range_2*

Deployed Version (19 Jul 2023 07:19 PM)	Pending Version
–	logFiles: false
–	eventLogAction: LOG_FLOW_END
–	ruleId: 268435461
–	name: test_time_range_2
timeRangeObjects:	
–	range-obj-1
sourceZones:	
–	inside_zone
destinationZones:	
–	outside_zone

Access Policy Edited: *NGFW-Access-Policy*

Image 14. FDM Pending Changes window displays the change of the object.

Verify

1. Run the show time-range command in order to validate the status of your time range objects.

```
<#root>

>

show time-range


time-range entry:

range-obj-1

 (

active

)
   periodic weekdays 0:00 to 23:50
time-range entry:

range-obj-2

 (

inactive

)
   periodic Monday 12:00 to 13:00
```

2. Use the show access-control-config command in order to validate the access control rule configuration.

<#root>

```
>

show access-control-config


===============[ NGFW-Access-Policy ]===============
Description :
=================[ Default Action ]=================
Default Action : Block
Logging Configuration
DC : Enabled
Beginning : Disabled
End : Disabled
Rule Hits : 0
Variable Set : Object missing: 76fa83ea-c972-11e2-8be8-8e45bb1343c0

===[ Security Intelligence - Network Whitelist ]====
===[ Security Intelligence - Network Blacklist ]====
Logging Configuration : Disabled
DC : Disabled

=====[ Security Intelligence - URL Whitelist ]======
=====[ Security Intelligence - URL Blacklist ]======
Logging Configuration : Disabled
DC : Disabled


======[ Rule Set: admin_category (Built-in) ]=======

=====[ Rule Set: standard_category (Built-in) ]=====

-------------[ Rule: test_time_range ]--------------
Action :

Allow

Source ISE Metadata :


Source Zones : inside_zone
Destination Zones : outside_zone
Users
URLs
Logging Configuration
DC : Enabled
Beginning : Disabled
End : Enabled
Files : Disabled
Safe Search : No
Rule Hits : 0
Variable Set : Object missing: 76fa83ea-c972-11e2-8be8-8e45bb1343c0
Time Range :

 range-obj-1

Daily Interval
StartTime : 00:00
EndTime : 23:50
Days : Monday,Tuesday,Wednesday,Thursday,Friday
```

3. Run a System Support Trace debug in order to confirm the traffic is hitting the correct rule.

<#root>

```
> system support trace

Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:
Please specify a server port: 443
Monitoring packet tracer and firewall debug messages



10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 New firewall session
10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 app event with app id no change, url no chang
10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 Starting with minimum 1, 'test_time_range', a
10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1
```

match rule order 1, 'test_time_range', action Allow

```
10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 MidRecovery data sent for rule id: 268435460,
10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1
```

allow action

```
10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 Packet 1930048: TCP ******S*, 07/20-18:05:06.
10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 Session: new snort session
10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 AppID: service: (0), client: (0), payload: (0
10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 Firewall: starting rule matching, zone 2 -> 1
10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1
```

Firewall: allow rule, 'test_time_range', allow

```
10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 Policies: Network 0, Inspection 0, Detection
10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 Verdict:
```

pass