

# Configure BFD in Secure Firewall Threat Defense with Flex-Config

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Verify](#)

[Troubleshoot](#)

## Introduction

This document describes how to configure the BFD Protocol in Secure Firewall Management Center running 7.2 and earlier with Flex-Config.

## Prerequisites

Border Gateway Protocol (BGP) configured in Cisco Secure Firewall Threat Defense (FTD) with Cisco Secure Firewall Management Center (FMC).

## Requirements

Cisco recommends that you have knowledge of these topics:

- BGP protocol
- BFD concepts

## Components Used

- Cisco Secure Firewall Management Center running 7.2 or earlier versions.

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

Bidirectional Forwarding Detection (BFD) is a detection protocol designed to provide fast-forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols.

## Configure

BFD configurations in FMC running versions 7.2 and earlier must be configured with Flex-Config policies and objects.

## Step 1.

Create the BFD template through Flexconfig Object.

The BFD template specifies a set of BFD interval values. BFD interval values configured in the BFD template are not specific to a single interface. You can also configure authentication for single-hop and multi-hop sessions.

To Create the Flex-Config object, select the **Objects Tab** at the top, click the **FlexConfig** option on the left column, then click the **FlexConfig Object** option and then click on **Add FlexConfig Object**.

The screenshot shows the Cisco Firepower Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects' (highlighted with a red box and a '1'), 'AMP', and 'Intelligence'. The left sidebar contains a list of object types, with 'FlexConfig' (highlighted with a red box and a '2') and 'FlexConfig Object' (highlighted with a red box and a '3') selected. The main content area is titled 'FlexConfig Object' and contains a table of objects. The 'DNS\_Configure' object is highlighted in blue. The table has columns for 'Name' and 'Description'.

Name	Description
BFD-MULTIHOP	
BFD-SINGLEHOP	
BFD_Negate	
Default_DNS_Configure	Configu
Default_Inspection_Protocol_Disable	Disable
Default_Inspection_Protocol_Enable	Enable
DHCPv6_Prefix_Delegation_Configure	Configu
DHCPv6_Prefix_Delegation_UnConfigure	Remove
DNS_Configure	Configu
DNS_UnConfigure	Remove
Eigrp_Configure	Configu
Eigrp_Interface_Configure	Configu
Eigrp_UnConfigure	Clears
Eigrp_Unconfigure_All	Clears

## Step 2.

Add the parameters needed for the BFD Protocol:

The BFD template specifies a set of BFD interval values. BFD interval values configured in the BFD template are not specific to a single interface. You can also configure authentication for single-hop and multi-hop sessions.

```
bfd-template [single-hop | multi-hop] template_name
```

- single-hop - Specifies a single-hop BFD template.

- multi-hopâ€” Specifies a multi-hop BFD template.
- template\_name â€” Specifies the template name. The template name cannot contain spaces.
- (Optional) Configure Echo on a single-hop BFD template.

---

**Note:** You can only enable Echo mode on a single-hop template.

---

Configure the intervals in the BFD template:

```
interval both milliseconds | microseconds {both | min-tx} microseconds | min-tx milliseconds echo
```

- bothâ€”Minimum transmit and receive interval capability.
- The interval in milliseconds. The range is 50 to 999.
- microsecondsâ€”Specifies the BFD interval in microseconds for both and min-tx.
- microseconds â€”The range is 50,000 to 999,000.
- min-txâ€”The minimum transmit interval capability.

Configure authentication in the BFD template:

```
authentication {md5 | meticulous-md5 | meticulous-sha-1 | sha-1}[0|8] wordkey-id id
```

- authenticationâ€” Specifies the authentication type.
- md5â€” Message Digest 5 (MD5) authentication.
- meticulous-md5â€” Meticulous keyed MD5 authentication.
- meticulous-sha-1â€” Meticulous keyed SHA-1 authentication.
- sha-1â€” Keyed SHA-1 authentication.
- 0|8â€”0 specifies that an UNENCRYPTED password follows. 8 specifies that an ENCRYPTED password follows.
- wordâ€”The BFD password (key), which is a single-digit password/key of up to 29 characters. Passwords starting with a digit followed by a whitespace are not supported, for example, 0 pass and 1 are not valid.
- key-idâ€”The authentication Key ID.
- idâ€”The shared key ID that matches the key string. The range is 0 to 255 characters.

## Edit FlexConfig Object

Name:

BFD-SINGLEHOP

Description:



Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert ▾



Deployment:

Once ▾

Type:

Append

```
bfd-template single-hop TEMPLATE1
echo
interval both 50
authentication sha-1 0 cisco key-id 10
```

▾ Variables

Name	Dimension	Default Value	Property (Type:Name)	Override
No records to display				

Step 3.

Associate the BFD Template with the interface.

## Edit FlexConfig Object

Name:

BFD-SINGLEHOP

Description:



Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert ▾



Deployment:

Once ▾

Type:

Append

```
bfd-template single-hop TEMPLATE1
echo
interval both 50
authentication sha-1 0 cisco key-id 10

interface Ethernet1/7
bfd template TEMPLATE1
```

▾ Variables

Name	Dimension	Default Value	Property (Type:Name)	Override
No records to display				

---

**Note:** Associate the BFD multi-hop template with a map of destinations.

---

Step 4 (Optional).

Create a BFD map containing destinations that you can associate with a multi-hop template. You must have a multi-hop BFD template already configured.

Associate the BFD multi-hop template with a map of destinations:

```
bfd map {ipv4 | ipv6} destination/cdir source/cdire template-name
```

- `ipv4` Configures an IPv4 address.
- `ipv6` Configures an IPv6 address.
- `destination/cdir` Specifies the destination prefix/length. The format is A.B.C.D/<0-32>.
- `source/cdir` Specifies the destination prefix/length. The format is X:X:X;X::X/<0-128>.
- `template-name` Specifies the name of the multi-hop template associated with this BFD map.

Click the **Save** button to save the object.

## Edit FlexConfig Object

Name:

BFD-MULTIHOP

Description:



Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert ▾



Deployment:

Once ▾

Type:

Append

```
bfd-template multi-hop MULTI-TEMPLATE1
  interval both 50

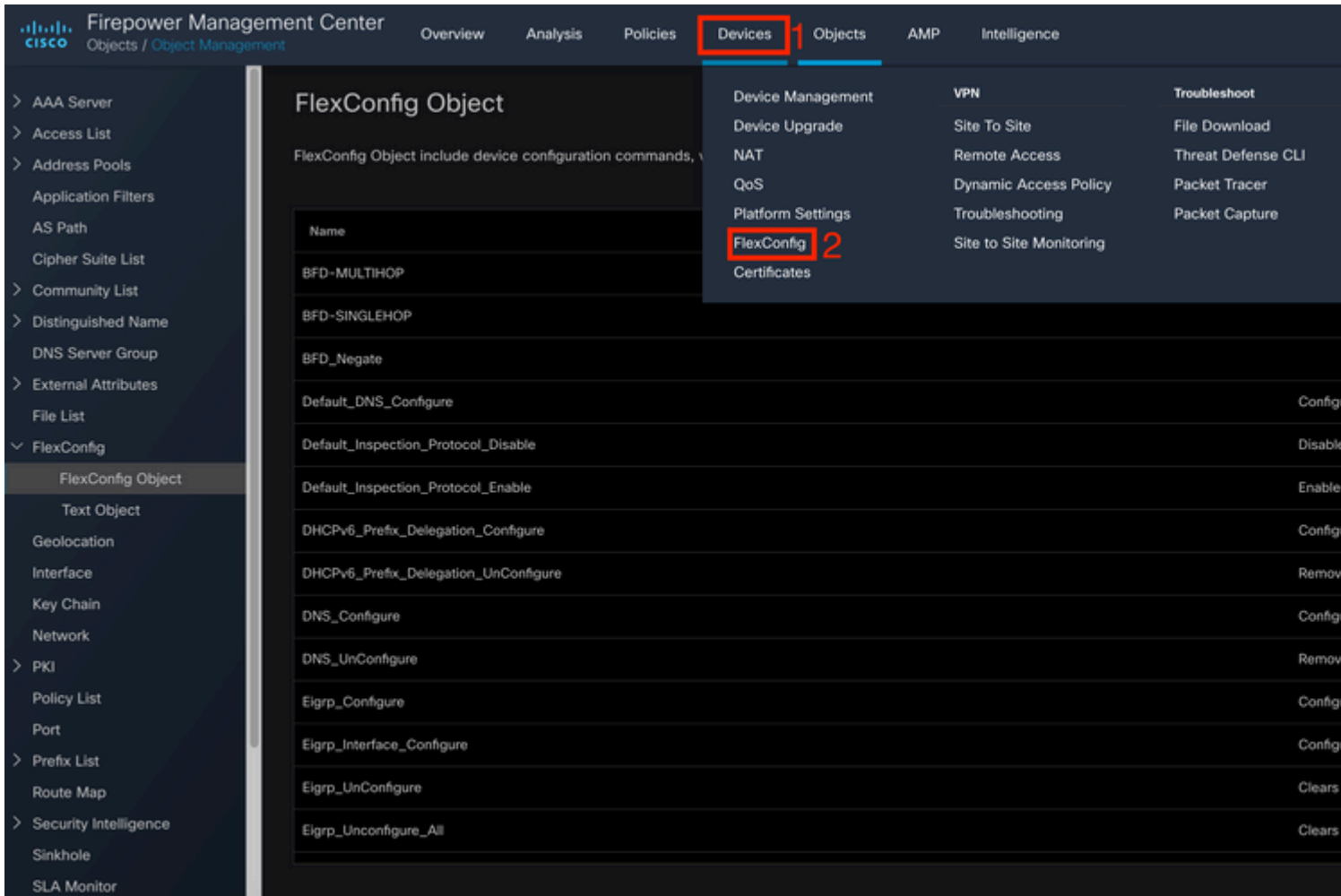
bfd map ipv4 10.11.11.0/24 10.36.42.5/32 MULTI-TEMPLATE1
```

▾ Variables

Name	Dimension	Default Value	Property (Type:Name)	Override
No records to display				

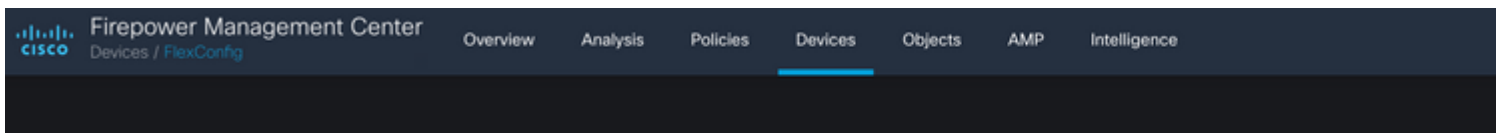
Step 5.

Click the **Devices** tab at the top, and select the **FlexConfig** option.



Step 6.

To create a new FlexConfig Policy, click the **New Policy** button.



Step 7.

Name the policy and select the devices assigned to the policy. Click the **Add to Policy** then click the **Save** button.



## New Policy

Name:

BFD

1

Description:

### Targeted Devices

Select devices to which you want to apply this policy.

#### Available Devices

🔍 Search by name or value

SF3130-A

SF3130-B

2

Add to Policy

#### Selected Devices

SF3130-A

SF3130-B

3

Step 8.

Select the FlexConfig Object on the left column and click the > button to add the object to the FlexConfig Policy, and click the Save button.

Firepower Management Center  
Devices / Flexconfig Policy Editor

Overview Analysis Policies **Devices** Objects AMP Intelligence

### BFD

Enter Description

Available FlexConfig  FlexConfig Object

- User Defined
  - BFD-MULTIHOP** 1
  - BFD-SINGLEHOP
  - BFD\_Negate
- System Defined
  - Default\_DNS\_Configure
  - Default\_Inspection\_Protocol\_Disable
  - Default\_Inspection\_Protocol\_Enable
  - DHCPv6\_Prefix\_Delegation\_Configure
  - DHCPv6\_Prefix\_Delegation\_UnConfigure
  - DNS\_Configure
  - DNS\_UnConfigure
  - Eigrp\_Configure
  - Eigrp\_Interface\_Configure
  - Eigrp\_UnConfigure
  - Eigrp\_Unconfigure\_All
  - Inspect\_IPv6\_Configure
  - Inspect\_IPv6\_UnConfigure

Selected Prepend FlexConfigs

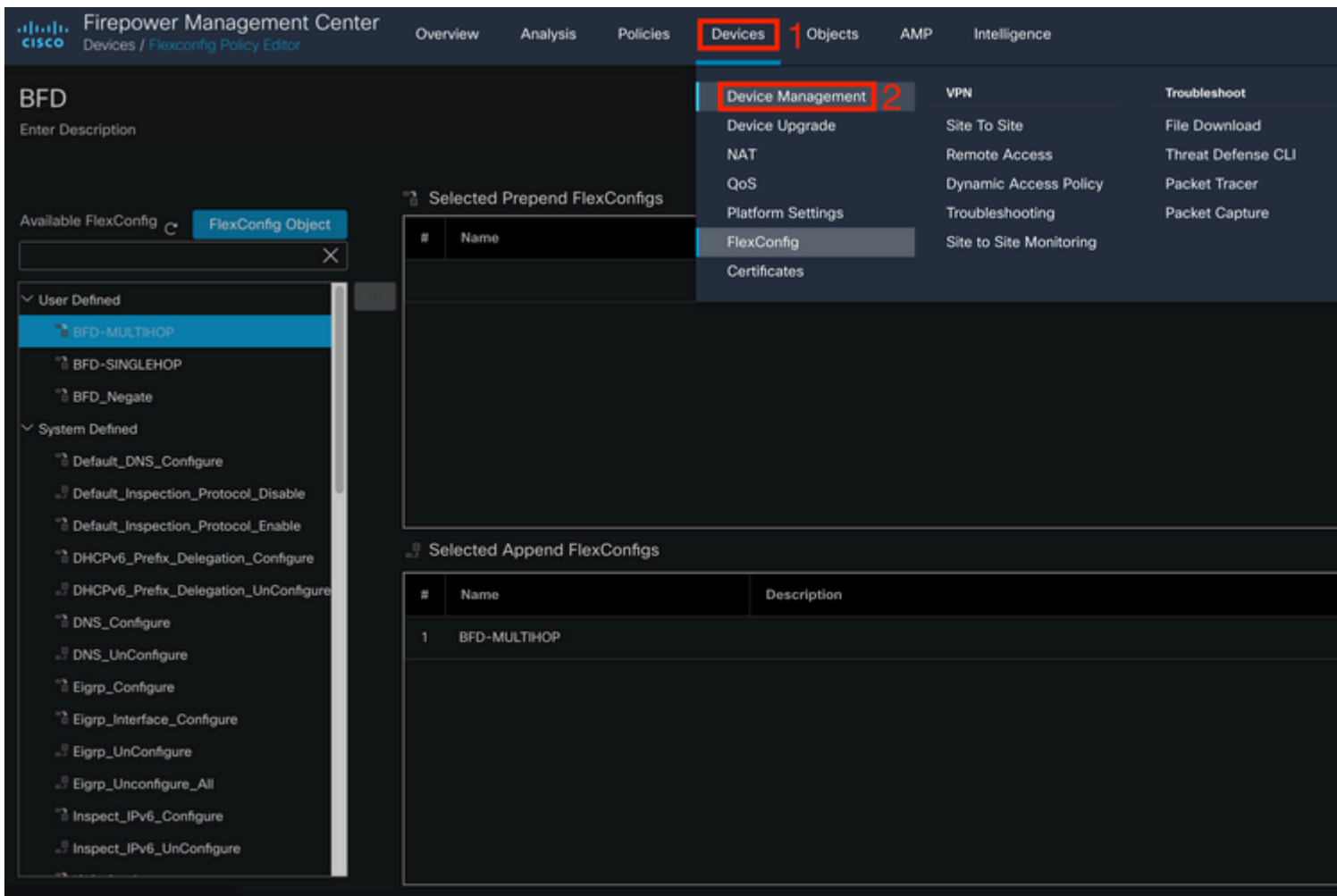
#	Name	Description
---	------	-------------

Selected Append FlexConfigs

#	Name	Description
1	BFD-MULTIHOP	

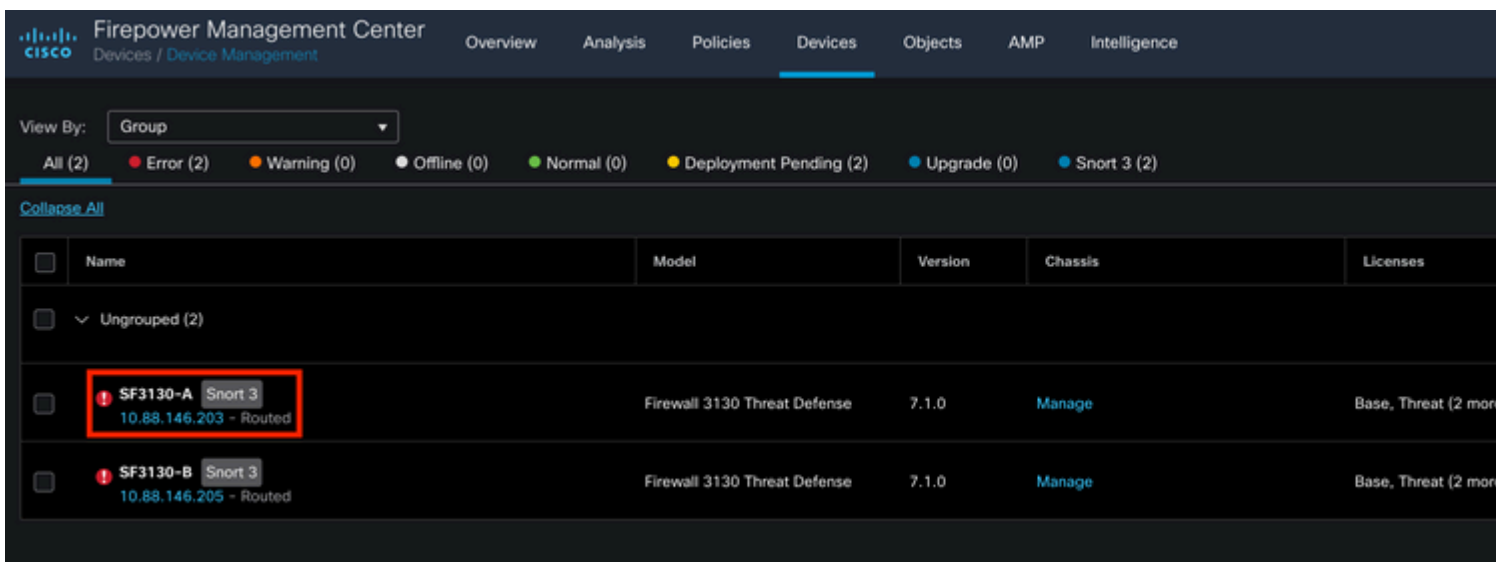
Step 9.

Click the **Devices** tab at the top and click the **Device Management** option.



Step 10.

Select the device where the BFD configuration is going to be assigned.



Step 11.

Click the Routing tab, then click the IPv4 or IPv6, depending on your configuration in the BGP section on the left column, then click the Neighbor tab, and click the edit pencil button to edit it.

Firepower Management Center  
Devices / NGFW Routing

Overview Analysis Policies **Devices** Objects AMP Intelligence

### SF3130-A

Cisco Secure Firewall 3130 Threat Defense

Device **Routing** 1 Interfaces Inline Sets DHCP

#### Manage Virtual Routers

Global

- Virtual Router Properties
- ECMP
- OSPF
- OSPFv3
- RIP
- Policy Based Routing
- BGP
  - IPv4** 2
  - IPv6
  - Static Route
- Multicast Routing
  - IGMP
  - PIM
  - Multicast Routes
  - Multicast Boundary Filter

Enable IPv4:

AS Number 65000

General **Neighbor** 3 Add Aggregate Address Filtering Networks Redistribution Route Injection

Address	Remote AS Number	Address Family	Remote Private AS Number
172.16.10.2	65001	Enabled	

Step 12.

Select the **checkbox** for BFD fallover and click the **OK** button.

## Edit Neighbor

IP Address\*

172.16.10.2

Enabled address

Shutdown administratively

Remote AS\*

65001

(1-4294967295 or 1.0-65535.65535)

Configure graceful restart

Graceful restart(failover/spanned mode)

Description

BFD Fallover ⓘ

Configuring BFD support for BGP for multi-hop, ensure that the BFD map is already created for the source destination pair through flex-config.

Filtering Routes

Routes

Timers

Advanced

Migration

Incoming

Outgoing

Access List

Access List

+

+

Route Map

Route Map

+

+

Prefix List

Prefix List

+

+

AS path filter

AS path filter

+

+

Limit the number of prefixes allowed from the neighbor

Maximum Prefixes\*

(1-2147483647)

Step 13.

Click the **Deploy** button, then click the **Deployment** button.

Firepower Management Center  
Devices / Device Management

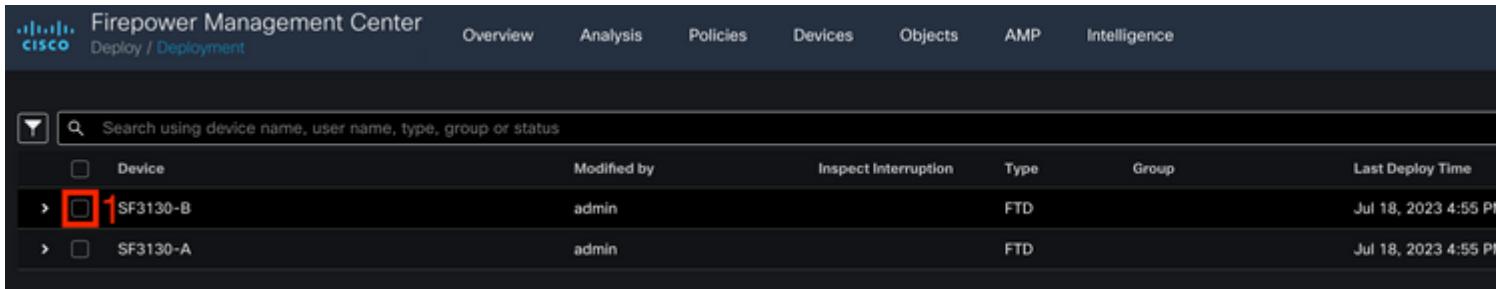
Overview Analysis Policies **Devices** Objects AMP Intelligence

View By: Group

All (2) Error (2) Warning (0) Offline (0) Normal (0) Deployment Pending (2) Upgrade (0) Snort 3 (2)

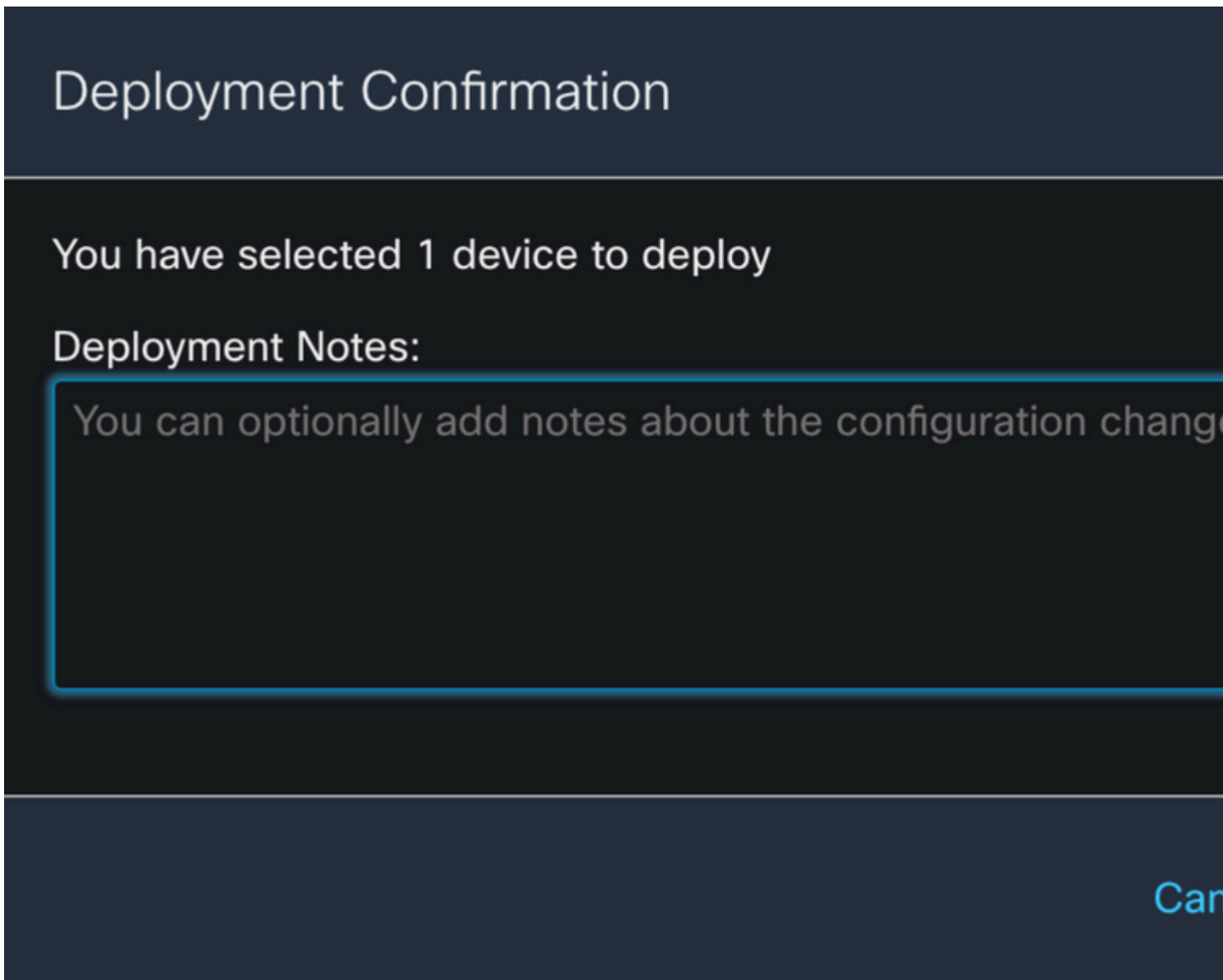
Step 14.

Select the device where the changes are going to be assigned by clicking the **checkbox**, and then click the **Deploy** button.



Step 15.

Click the **Deploy** button.



Step 16.

Click the **Deploy** button.

## Validation Messages: SF3130-B

1 total

0 errors

1 warning

0 info

### PG.TEMPLATE.TemplatePolicy: BFD

- > **Warning:** FlexConfig policies intentionally do not contain extensive input validation. Please ensure that the configurations

---

**Note:** The warning is expected and it is just informational.

---

## Verify

Verify the BFD configuration and the status directly on the CLI session with the next commands.

```
<#root>
```

```
>
```

```
system support diagnostic-cli
```

Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.  
Type help or '?' for a list of available commands.

SF3130-A>

enable

Password:

SF3130-A#

show running-config | inc bfd

bfd-template single-hop Template

  bfd template Template

  neighbor 172.16.10.2 fall-over bfd single-hop

SF3130-A#

show bfd summary

	Session	Up	Down
Total	1	1	0

SF3130-A#

show bfd neighbors

IPv4 Sessions

NeighAddr	LD/RD	RH/RS	State	Int
172.16.10.2	1/1	Up		

## Troubleshoot

There is currently no specific troubleshooting information available for this configuration.