

# Migrate EIGRP Configuration from Flexconfig to MC UI

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Notice for 7.3+:](#)

[Configurations](#)

[Troubleshoot](#)

[Related Information](#)

## Introduction

This document describes what the behavior is after the upgrade to version 7.2, when EIGRP configuration is used in the MC/TD devices.

## Prerequisites

### Requirements

Cisco recommends that you have basic knowledge of these topics:

- EIGRP Protocol
- FlexConfig feature
- Upgrade process

### Components Used

This feature was introduced in version 7.1 per the release note of that version. This document uses these software and hardware versions:

- SecureFirewall Management Center (MC) version 7.1.0 and 7.2.0
- SecureFirewall Threat Defense (TD) version 7.1.0 and 7.2.0

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

Prior to version 7.2, EIGRP configuration was supported in Secure Firewall Threat Defense devices via Flexconfig. In version 7.2, you can now use the management center web interface to configure EIGRP.

## Notice for 7.3+:

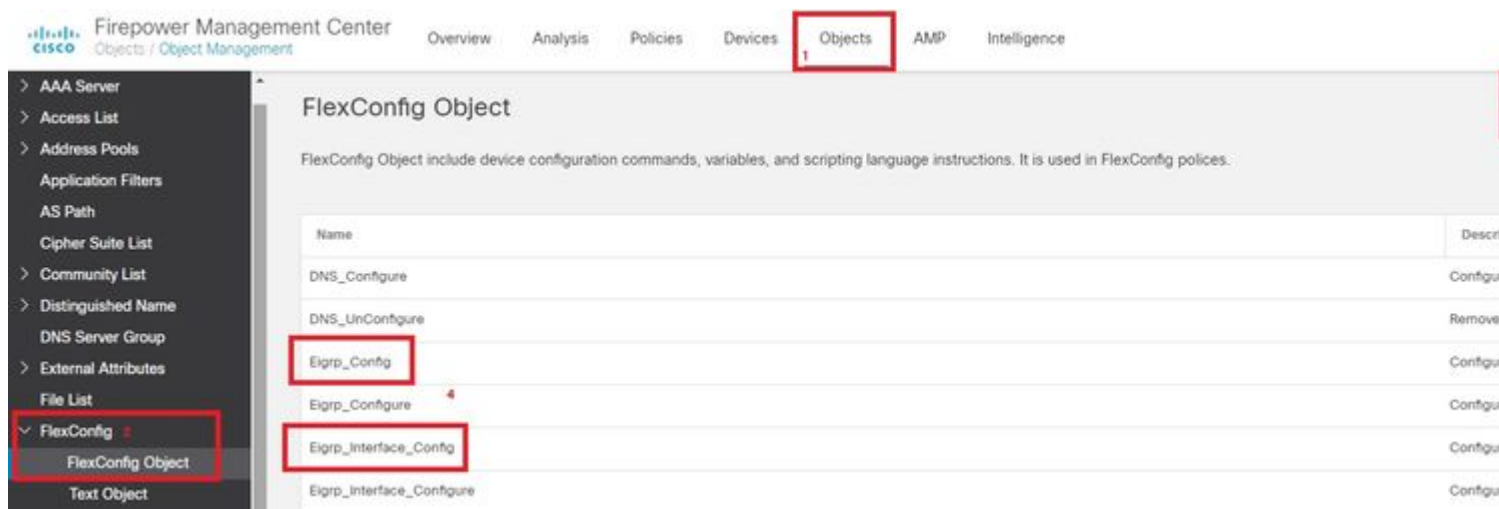
After version 7.3, this migration script is deprecated. Refer to this guide on how to use FlexConfig Migration to configure EIGRP:

[https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/730/management-center-device-config-73/flex-config.html#Cisco\\_Task.dita\\_380221ea-8356-4343-b852-609e61a69193](https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/730/management-center-device-config-73/flex-config.html#Cisco_Task.dita_380221ea-8356-4343-b852-609e61a69193)

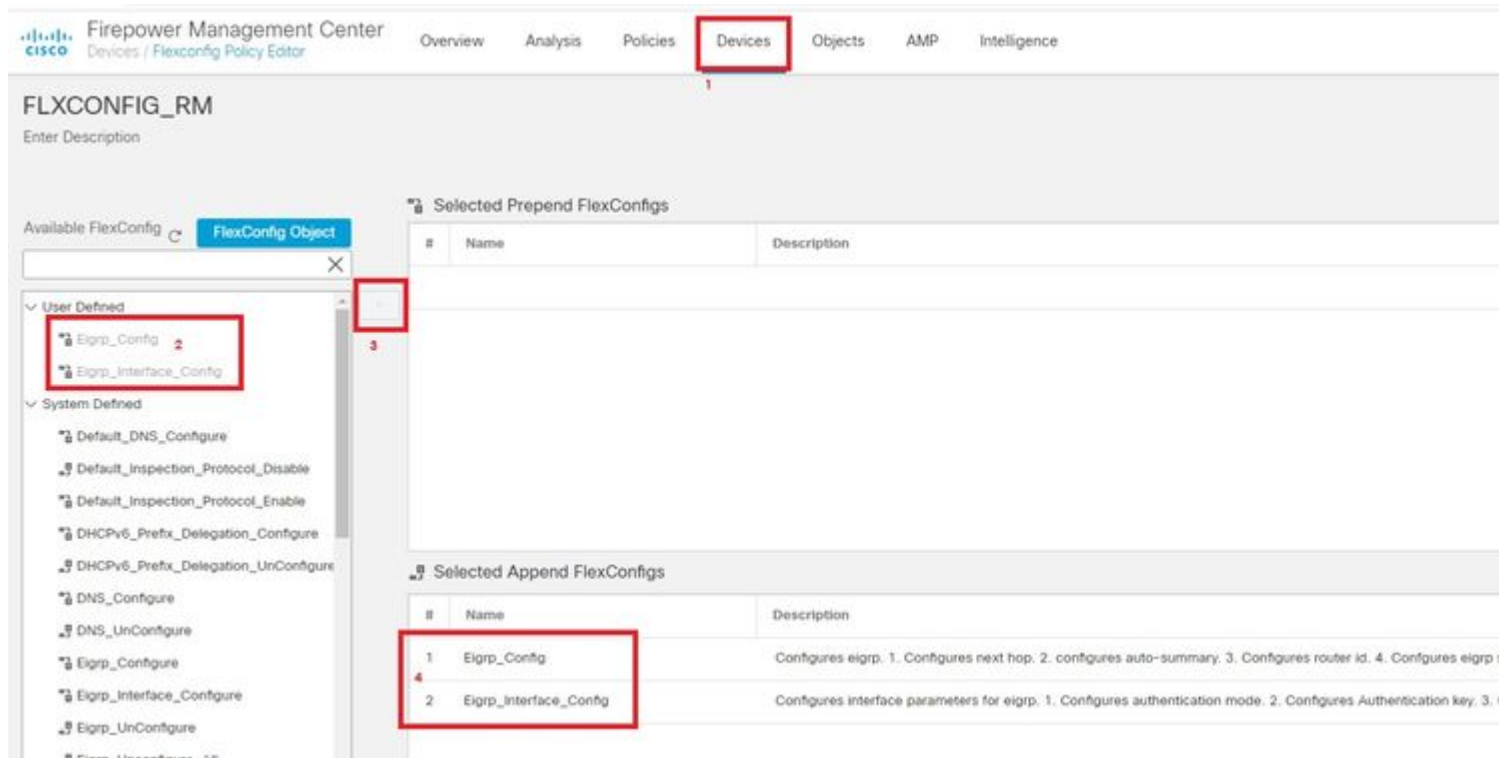
## Configurations

Prior to version 7.2, the EIGRP configuration is done as follows:

1. Create FlexConfig objects for EIGRP.



2. Assign the FlexConfig objects to the FlexConfig Policy.



3. Finally, deploy this configuration to managed devices.

The EIGRP configuration via TD CLI is visualized with show commands:

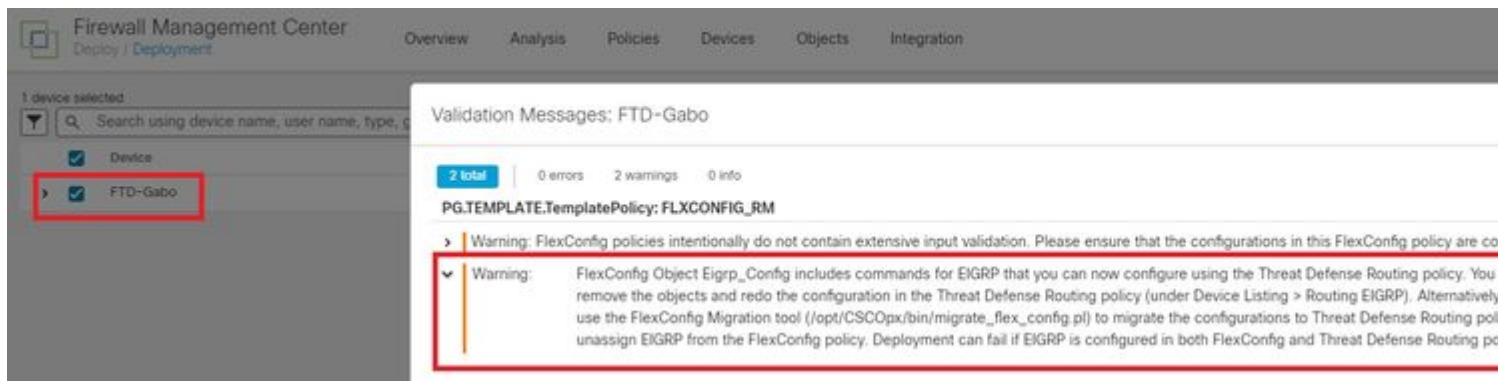
```
firepower# show run router router eigrp 3 neighbor 10.40.2.2 interface OUTSIDE network 10.40.2.0 255.255.255.0
```

```
firepower# show run | inc eigrp
authentication key eigrp 3 ***** key-id 120
authentication mode eigrp 3 md5
hello-interval eigrp 3 60
hold-time eigrp 3 60
```

For this demonstration: Prior to the upgrade of the MC to version 7.2, the TD device has the previously shown EIGRP configuration. It was configured via FlexConfig.

Once the MC is upgraded to version 7.2, an automatic deployment gets available post-upgrade process. (This is normal behavior.)

After the deployment of this pending deployment post-upgrade, this warning appears:



**Warning:** FlexConfig Object includes commands for EIGRP that you can now configure and use the Threat Defense Routing policy. You must remove the objects and redo the configuration in the Threat Defense Routing policy (under Device Listing > Routing EIGRP).

This first deployment post-upgrade of the MC to version 7.2 is successful and does not remove the EIGRP configuration from TD.

## Troubleshoot

Navigate to **System > Monitoring > Audit**. An audit log was created for the migration of the EIGRP Flexconfig configuration.



No Search Constraints ([Edit Search](#))

Table View of the Audit Log

<input type="checkbox"/>	↓ Time ×	User ×	Subsystem ×	Message ×
▼ <input type="checkbox"/>	2022-09-13 19:45:45	admin	Audit Log Events	Delete
▼ <input type="checkbox"/>	2022-09-13 19:45:16	admin	System > Monitoring > Audit	Page View
▼ <input type="checkbox"/>	2022-09-13 18:50:13	admin	Objects > Object Management > >NetworkObject	Page View
▼ <input type="checkbox"/>	2022-09-13 18:50:06	admin	/ui/ddd/	Page View
▼ <input type="checkbox"/>	2022-09-13 18:40:55	admin	Devices > Device Management > Secure Firewall Interfaces	Page View
▼ <input type="checkbox"/>	2022-09-13 18:40:51	admin	Devices > Device Management	Page View
▼ <input type="checkbox"/>	2022-09-13 18:39:54	csm_processes	Devices > Device Management > Secure Firewall Routing	Flex Config Migration FTD-Gabo:273
▼ <input type="checkbox"/>	2022-09-13 18:33:46	admin	Devices > Troubleshoot > Threat Defense CLI	Page View
▼ <input type="checkbox"/>	2022-09-13 18:31:39	admin	Devices > FlexConfig	Page View

Open the report to confirm which EIGRP configuration was migrated to the MC UI.



Legend: | Added | Edited | Removed

Changed Policies

Routing

Virtual Router (Global)

EIGRP

Previous Version

Latest Version

**EIGRP:**

Modified: 2022-09-13 20:40:20

2022-09-13 22:39:53

Name: .PG.PLATFORM.PixAsaEigrpPage-1663101620000

.2b8412b0-338e-11ed-9779-c560fac634

Description: Device ID: 4294967406

ModifiedBy: admin

csm\_processes

**Neighbors:**

Interface:

OUTSIDE

Address:

gw\_10.40.2.2

**Setup:**

Enable EIGRP:

true

AS Number:

3

Selected Networks/Hosts:

bb\_1663108778125\_0

Passive Interface:

None

Log Neighbor Changes:

true

Log Neighbor Warnings:

true

**Interfaces:**

Eigrp Hello Interval:

60

Eigrp Hold Time:

60

Eigrp Split Horizon:

true

Eigrp MD5Auth:

true

Eigrp MD5 Auth Key Format:

None

Eigrp MD5 Auth Key:

0HA8bt8OFuekfTFwyvYzcQ==

Eigrp MD5 Auth Id:

120

Eigrp Interface:

OUTSIDE

## Related Information

[Secure Firewall Management Center Device Configuration Guide, 7.2 | Migrating FlexConfig Policies](#)