

# Remove or Modify NetFlow Configuration Using Flexconfig

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Initial Configuration](#)

### [Remove NetFlow Configurations](#)

### [Modify the existing NetFlow Configurations](#)

### [Related Documents](#)

---

## Introduction

This document describes how to remove or modify the NetFlow configuration on Firepower Threat Defense (FTD) via Firepower Management Center (FMC).

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of FMC
- Knowledge of FTD
- Knowledge of the FlexConfig Policy

### Components Used

The information in this document is based on these software and hardware versions:

- FTD version less than 7.4
- FMC version less than 7.4

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.



**Note:** Important Note for Firepower Versions 7.2.x: When configuring NetFlow, there is a known Cisco bug ID [CSCwh29167](#) where the Flex object reorders, causing deployment to fail due to the class-map not being configured. To address this issue, implement the workaround documented under Cisco bug ID [CSCwf99848](#) (duplicate of Cisco bug ID [CSCwh29167](#) ).

---

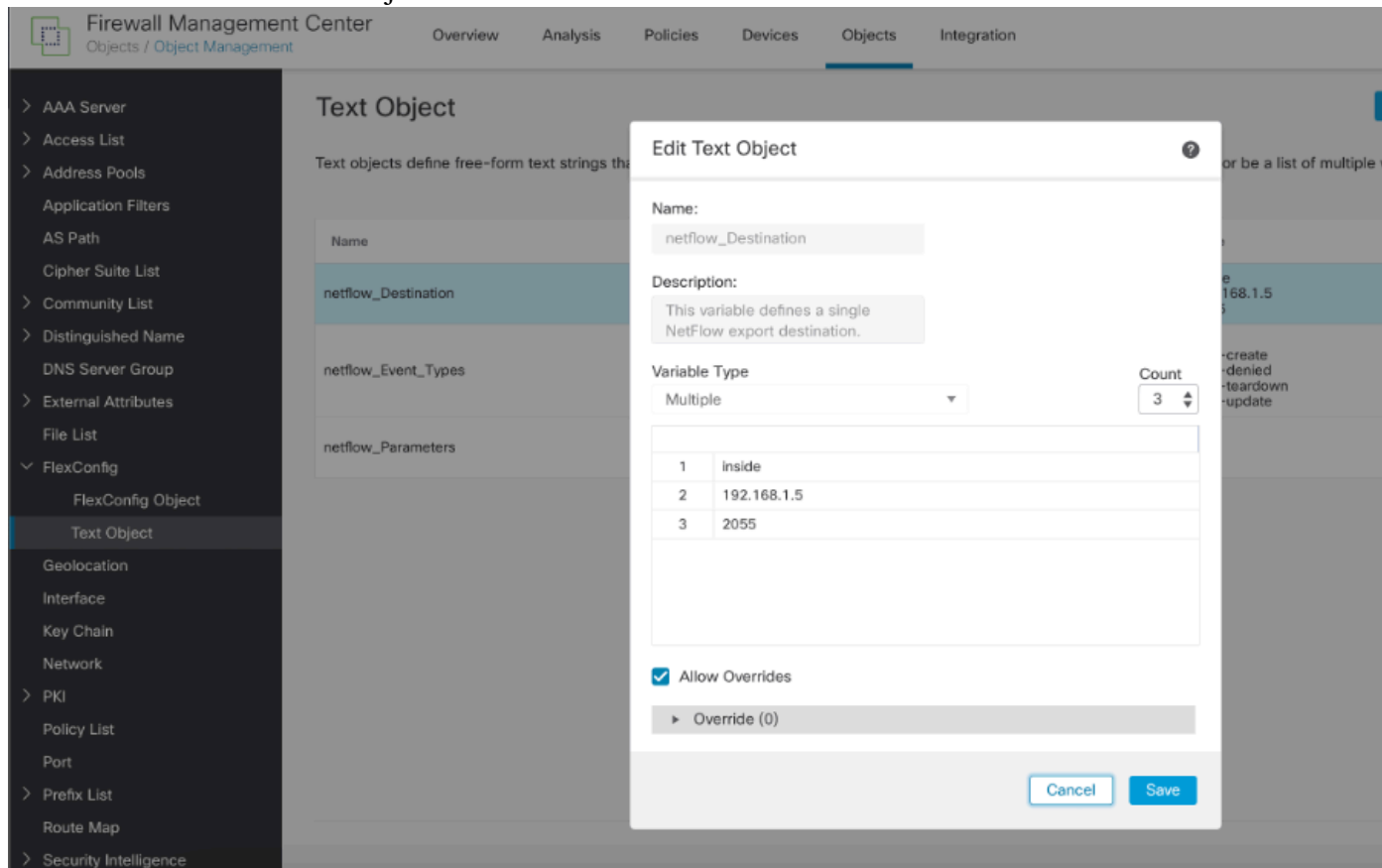
## Initial Configuration

```
access-list flow_export_acl extended permit ip any any
!
class-map flow_export_class
  match access-list flow_export_acl
!
policy-map global_policy
  class flow_export_class
    flow-export event-type flow-create destination 192.168.1.5
    flow-export event-type flow-denied destination 192.168.1.5
    flow-export event-type flow-teardown destination 192.168.1.5
    flow-export event-type flow-update destination 192.168.1.5
!
```

flow-export destination Inside 192.168.1.5 2055

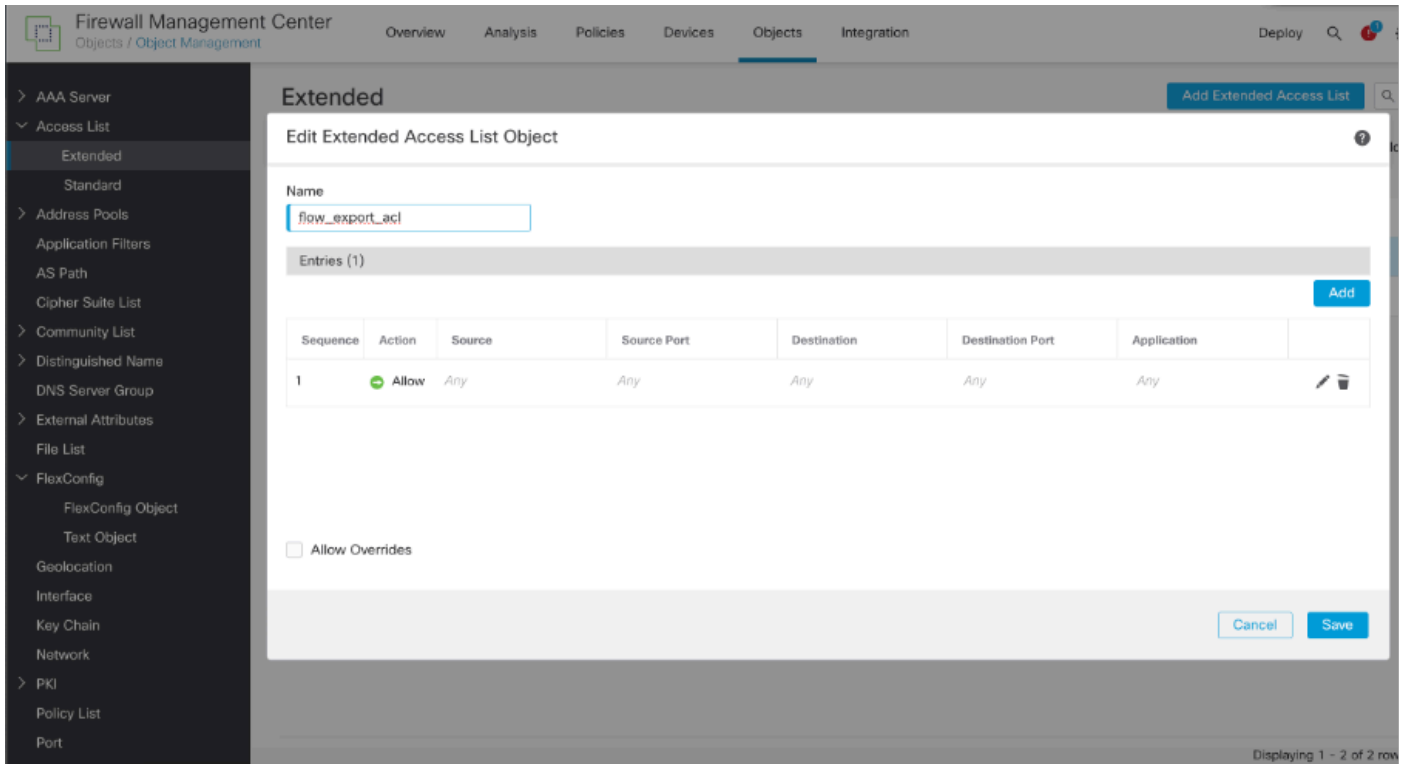
For configuring these initial configurations, flex config objects used are:

1. Netflow destination text object



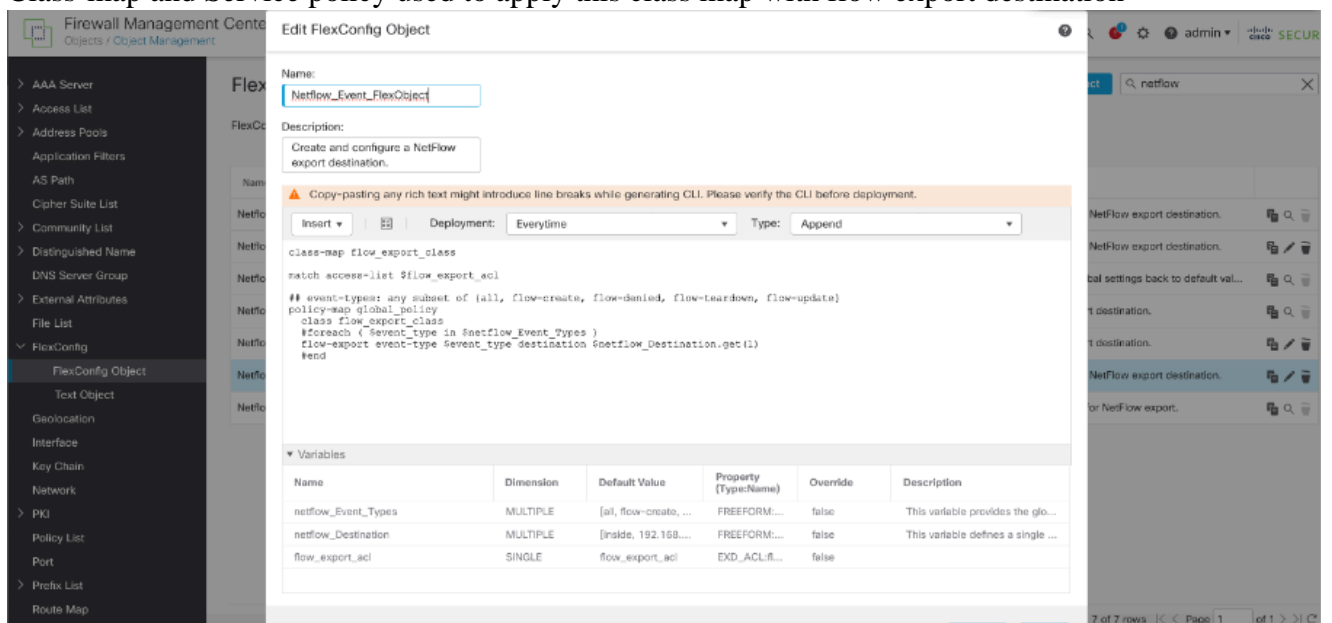
*Netflow Destination Text Object*

2. Extended ACL named: flow\_export\_acl



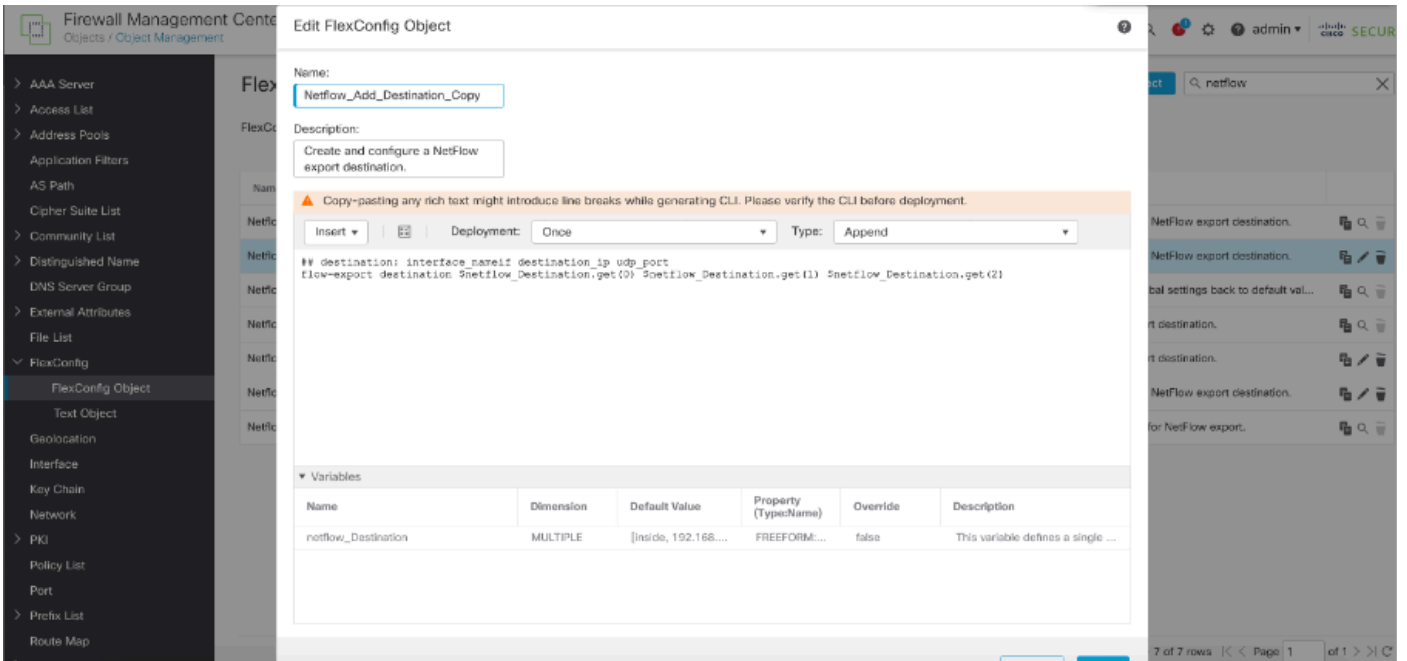
Flow Export ACL

### 3. Class-map and Service policy used to apply this class map with flow export destination



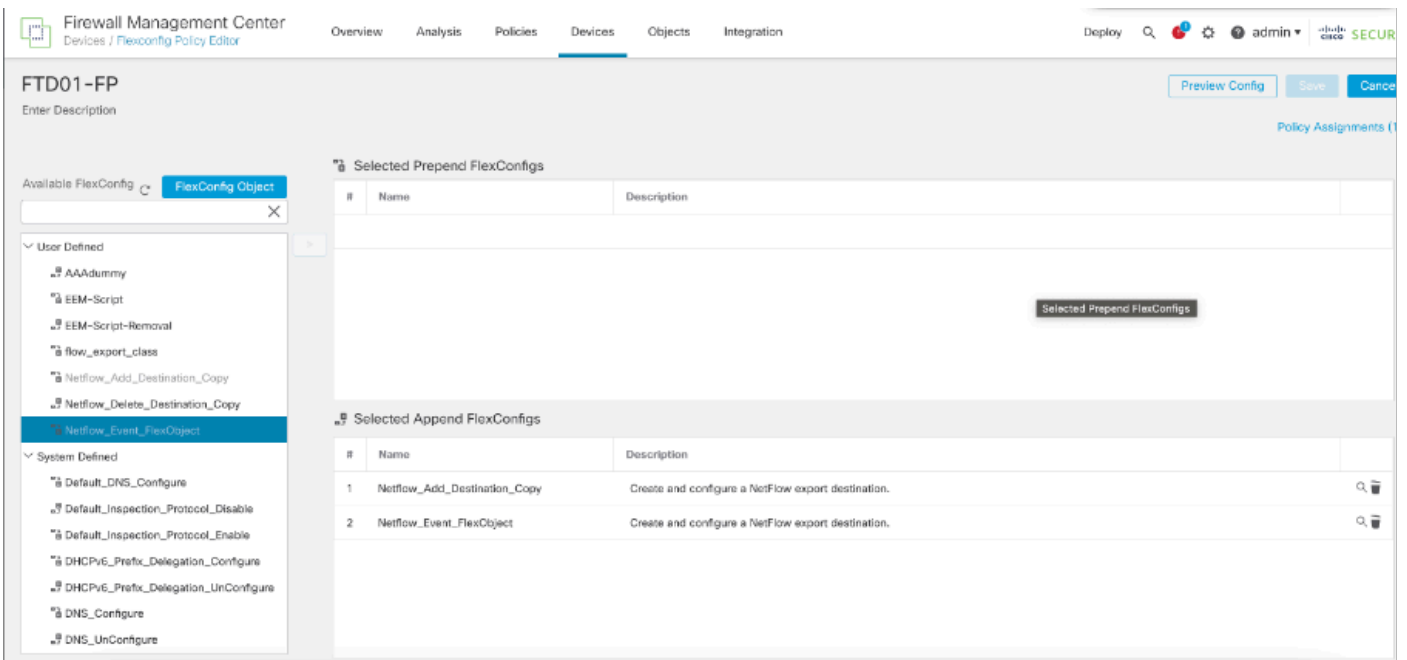
Class map and Service policy

### 4. Flow export destination



Flow export Destination

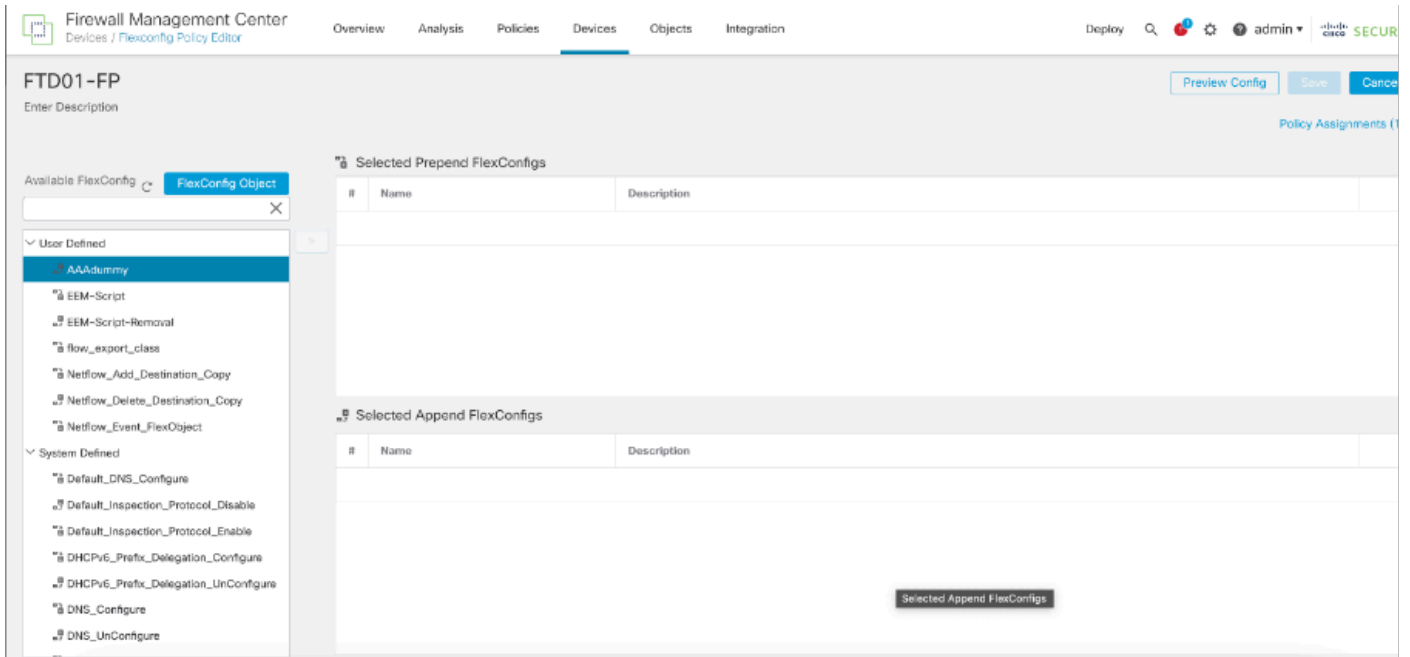
5. Then Added these two objects in flex config policy and deployed:



FlexConfig Policy

## Remove NetFlow Configurations

Step 1: Delete the flex objects from the flex policy.



*Delete existing flexconfig*

Step 2: Deploy the policy. From the command line, we would see that removed configurations are:

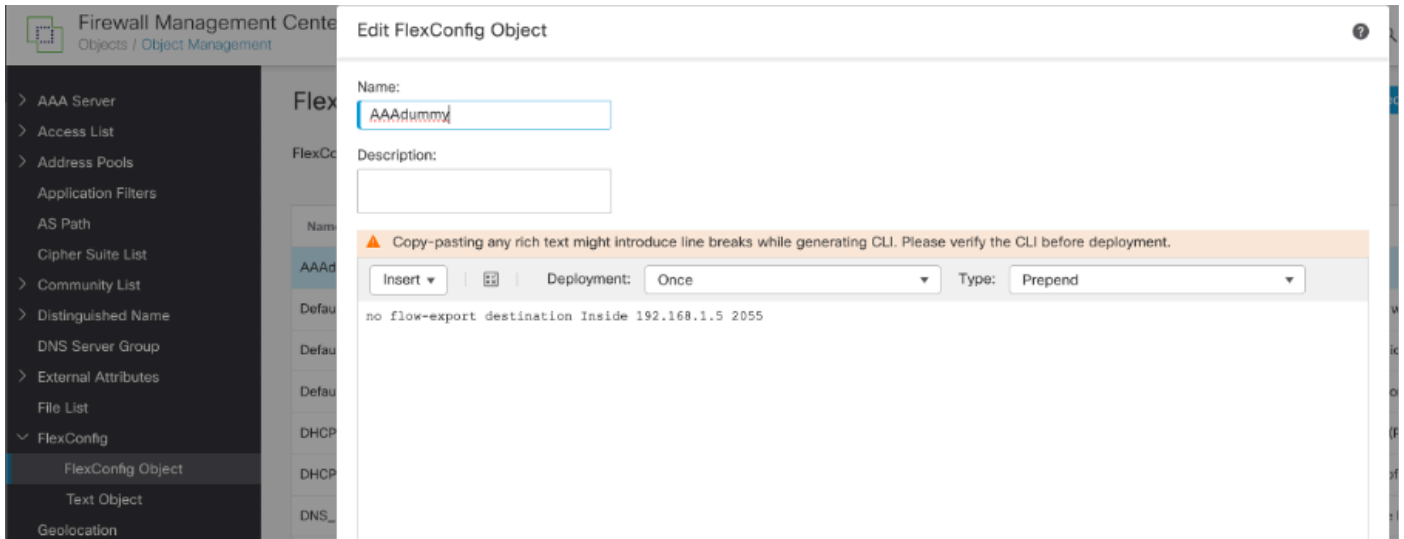
```
access-list flow_export_acl extended permit ip any any
!
class-map flow_export_class
 match access-list flow_export_acl
!
policy-map global_policy
 class flow_export_class
  flow-export event-type flow-create destination 192.168.1.5
  flow-export event-type flow-denied destination 192.168.1.5
  flow-export event-type flow-teardown destination 192.168.1.5
  flow-export event-type flow-update destination 192.168.1.5
```

Whereas, configuration which is not removed is:

```
flow-export destination Inside 192.168.1.5 2055
```

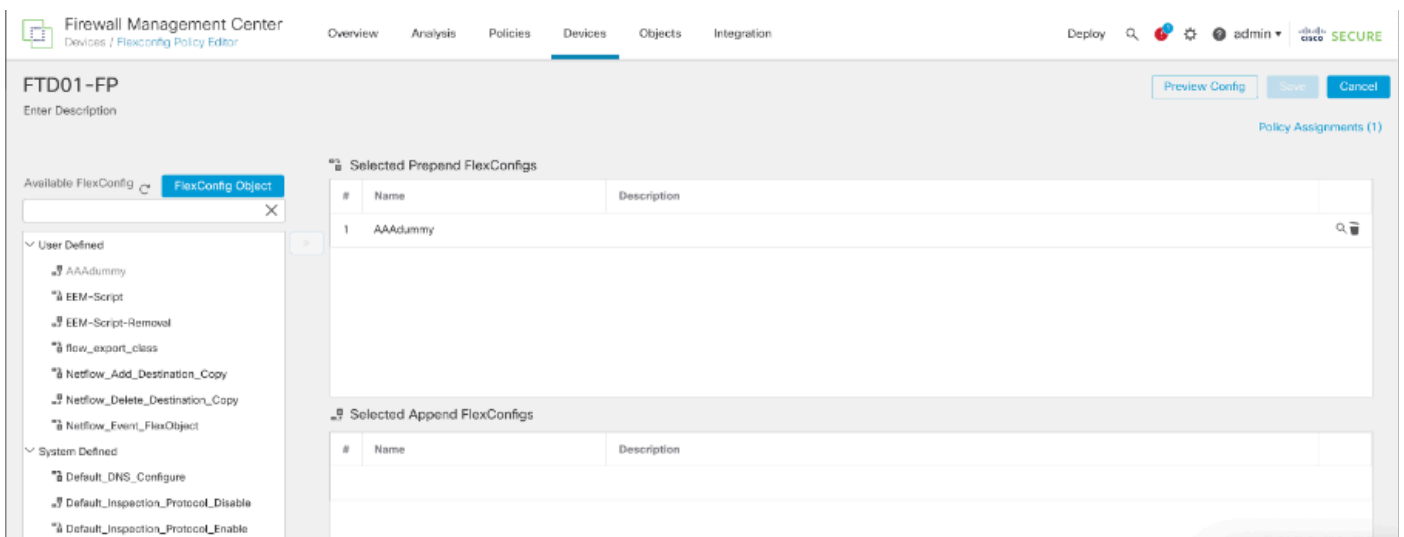
Step 3: To remove this, we need to create a flex object with Type 'prepend' and adding the configuration:

```
no flow-export destination Inside 192.168.1.5 2055
```



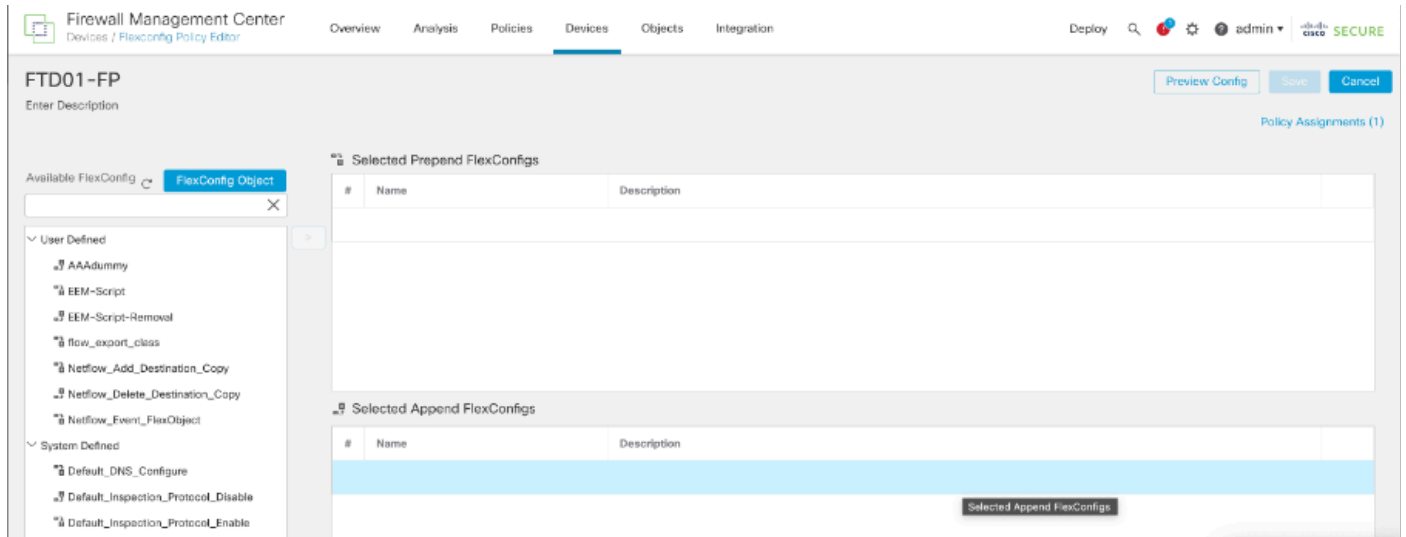
*Delete flex config destination*

Step 4: Under flex policy call the newly created prepend object in Step 3 and deploy the policy.



*Add this under flex config policy*

Step 5: Delete that prepend object from the flex policy and deploy again.



*Delete the prepend object*

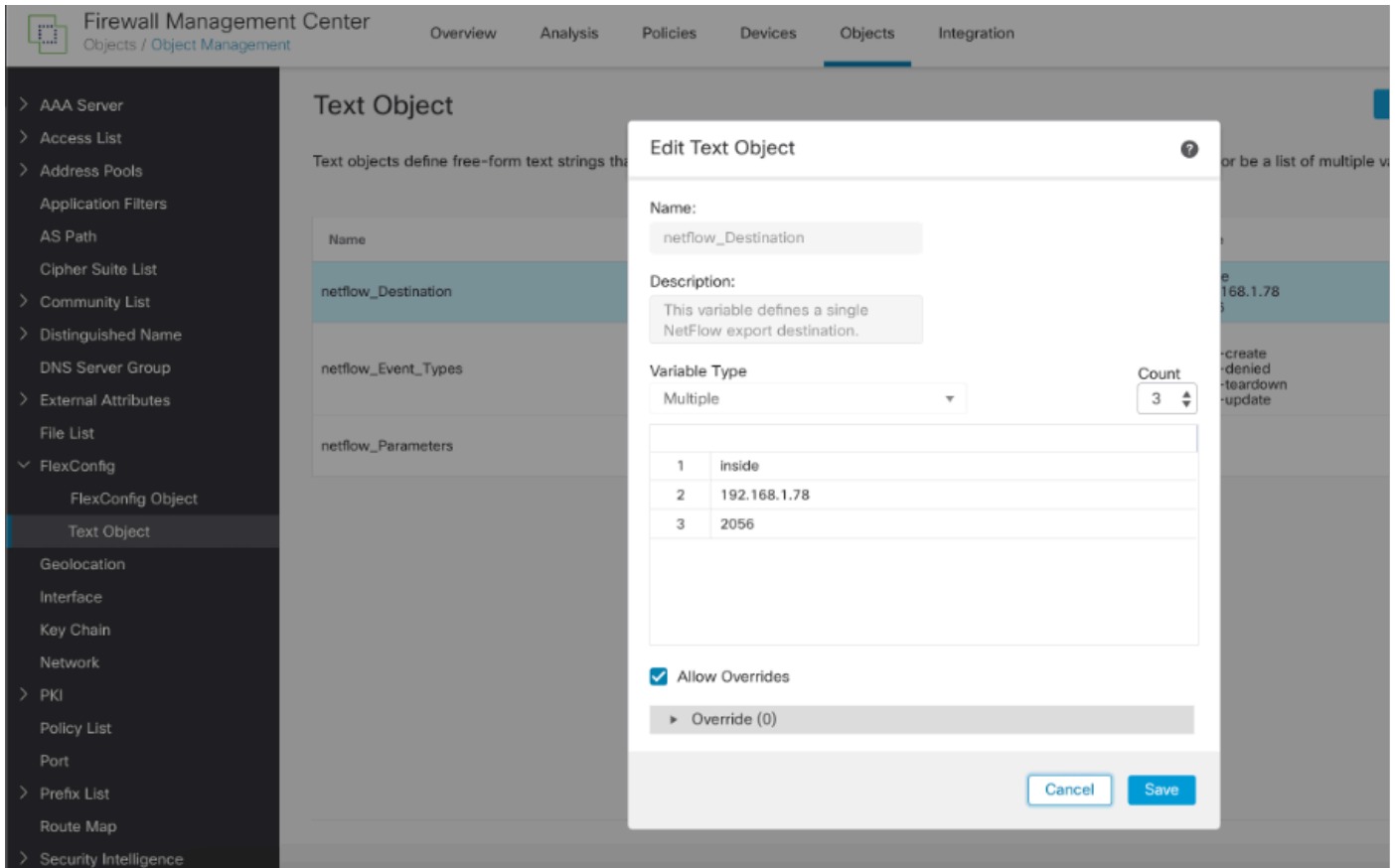
All the flow-export related configuration gets removed now.

## Modify the existing NetFlow Configurations

Step 1: Edit the Text object created for Netflow Destination. Change the required parameters IP, Interface name or Port.

Example: We changed the IP and port from (192.168.1.5, 2055) to (192.168.1.78, 2056)





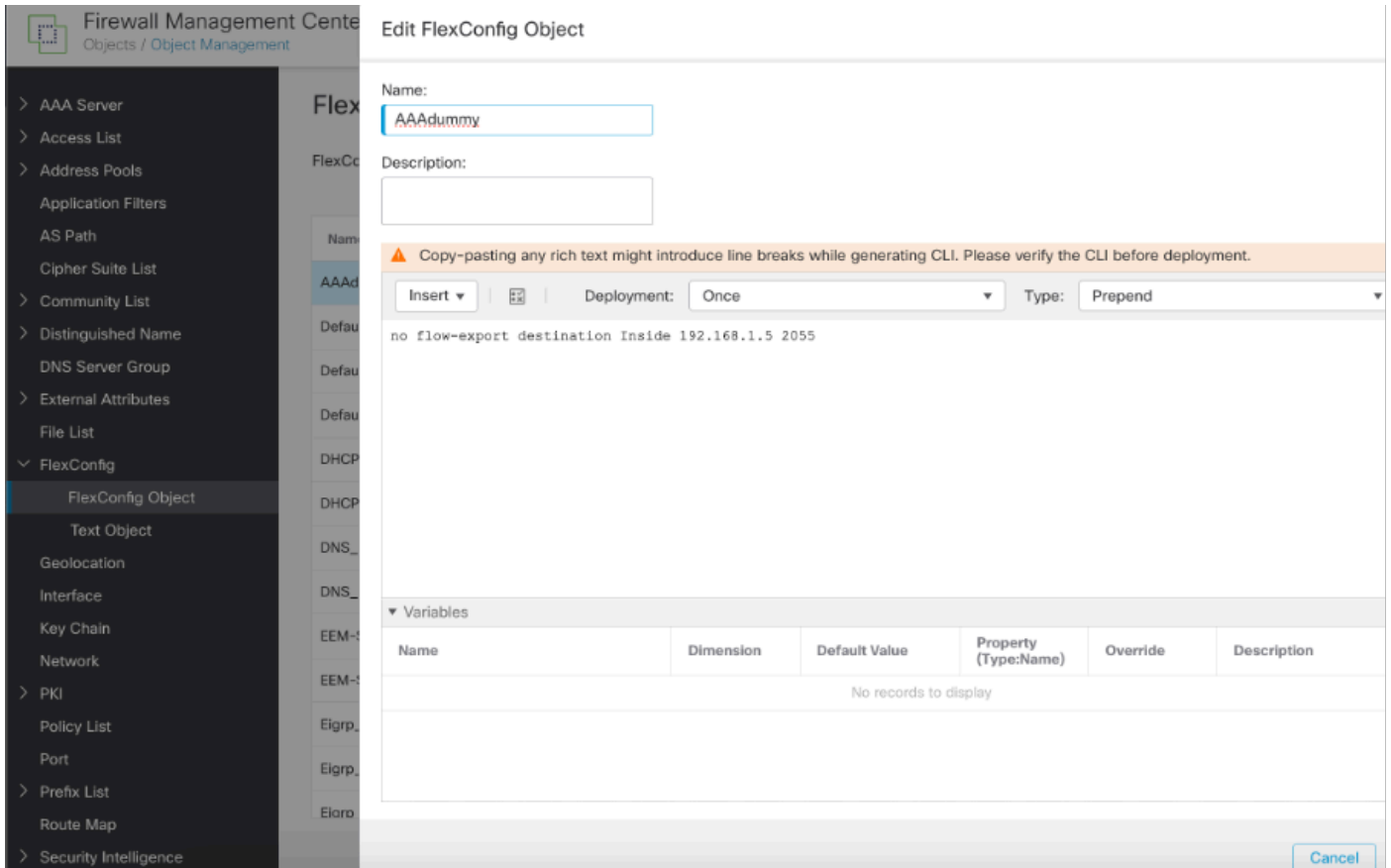
*Netflow destination text object*

Step 2: Deploy the policy. You would see the changes are reflected as expected but along with the old Netflow destination config:

```
access-list flow_export_acl extended permit ip any any
!
class-map flow_export_class
 match access-list flow_export_acl
!
policy-map global_policy
 class flow_export_class
  flow-export event-type flow-create destination 192.168.1.78
  flow-export event-type flow-denied destination 192.168.1.78
  flow-export event-type flow-teardown destination 192.168.1.78
  flow-export event-type flow-update destination 192.168.1.78
!
flow-export destination Inside 192.168.1.78 2056
flow-export destination Inside 192.168.1.5 2055
```

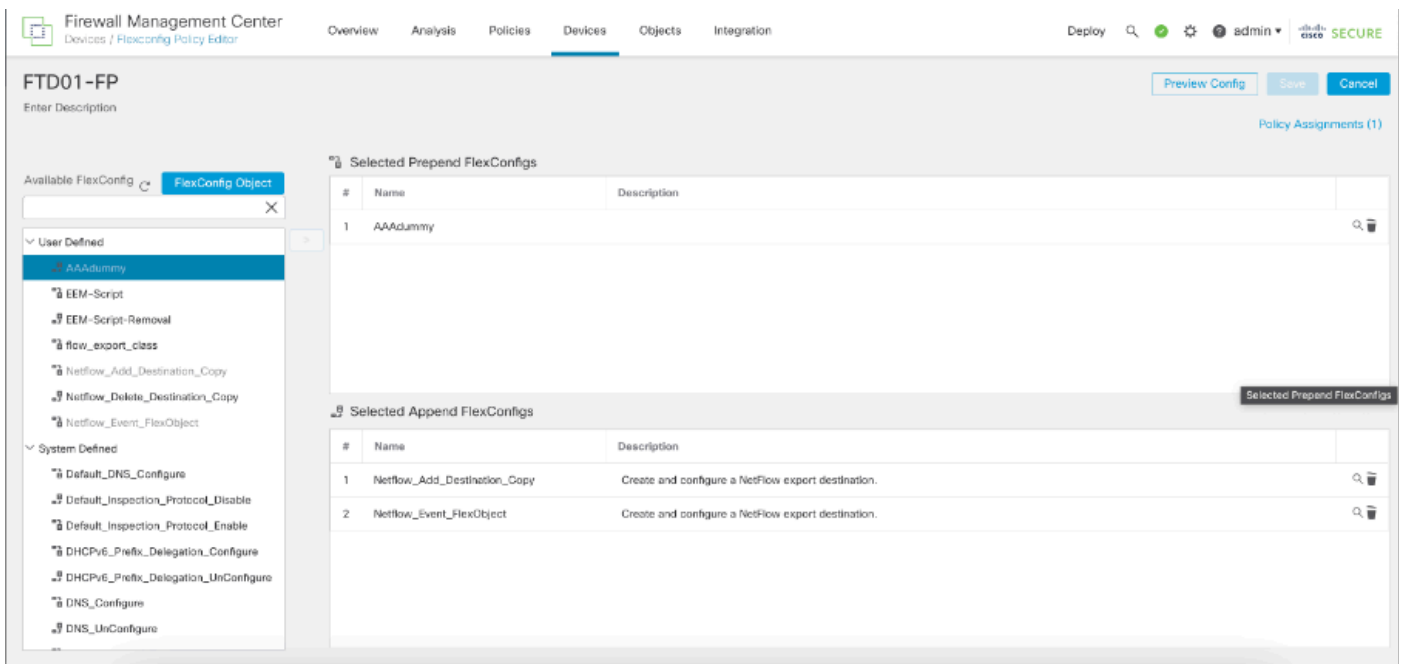
Step 3: To remove this, you need to create a flex object with Type 'prepend' and adding the configuration:

```
no flow-export destination Inside 192.168.1.5 2055
```



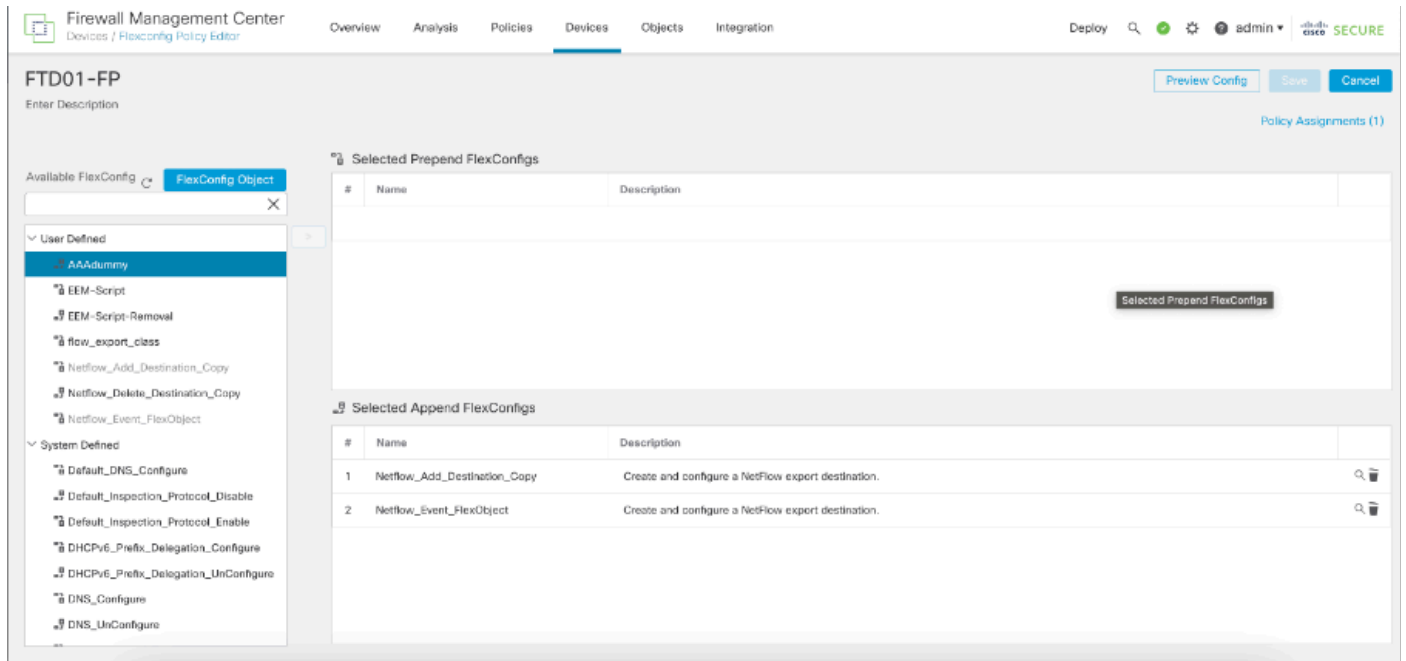
Delete netflow destination

Step 4: Under flex policy call the newly created prepend object in Step 3 and deploy the policy.



Add to Prepend Flex Config

Step 5: Delete that prepend object from the flex policy and deploy again.



*Delete the Prepend FlexConfig*

NetFlow related configuration got modified successfully.

```
access-list flow_export_acl extended permit ip any any
!
flow-export destination Inside 192.168.1.78 2056
!
class-map flow_export_class
 match access-list flow_export_acl
!
policy-map global_policy
 class flow_export_class
  flow-export event-type flow-create destination 192.168.1.78
  flow-export event-type flow-denied destination 192.168.1.78
  flow-export event-type flow-teardown destination 192.168.1.78
  flow-export event-type flow-update destination 192.168.1.78
```

## Related Documents

<https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/netflow/216126-configure-netflow-secure-event-logging-o.html>