

# Project Summary

## Project Overview

Create a Python script to read the security zone on and FTD in standalone mode. Create a second Python script to create a security zone.

## Project Summary

- 1) Create Python Scripts based on the scenarios detailed below.
- 2) Ansible Scripts for only one appliance architecture will be required (Cisco Firepower Threat Defense (FTD) version 6.4).

## Resources

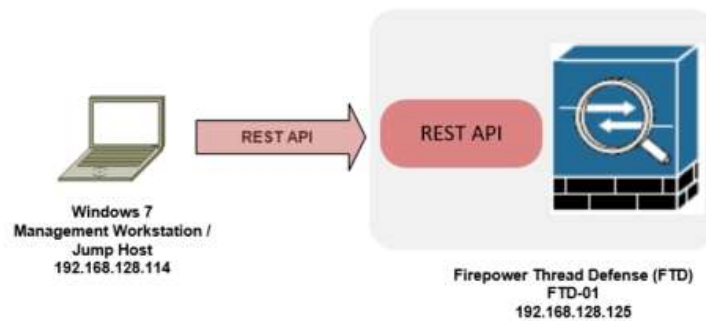
- Cisco Firepower Threat Defense REST API Guide:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/ftd-api/guide/ftd-rest-api/api-explorer.html>

## Test Environment Details

A test environment will be provided for testing.

- Cisco FTD version 6.4 installed and configured.
- The topology shown below will be configured with TFTP/IP and all necessary initialization.



## Project Details

Cisco FTD version 6.4 installed and configured. Create a Python script to read the security zone on and FTD in standalone mode. Create a second Python script to create a security zone.

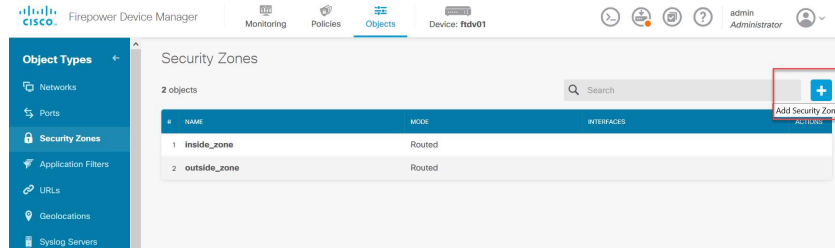
## Manual Process

This is the manual process for creating a security zone using the FDM interface on the FTD.

From the main screen click on Objects.



Click on Security Zones on the left side and Click Add.



Enter the zone information, leave everything else default. Click OK.

Add Security Zone

Name

dmz\_zone

Description

Mode

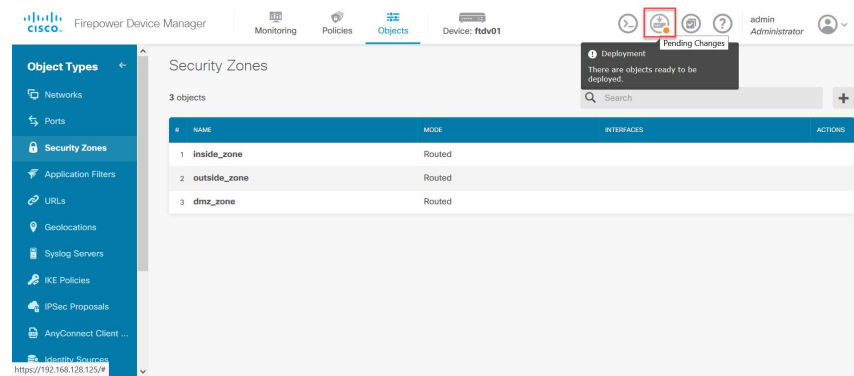
☒ Routed ☐ Passive

Interfaces

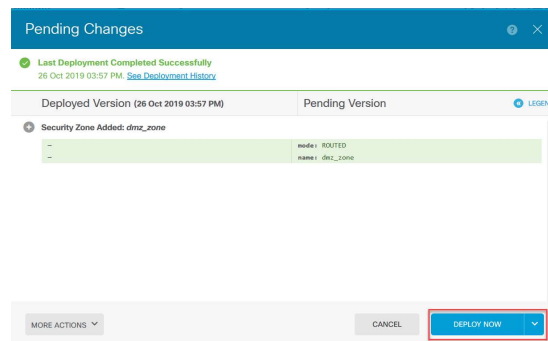
CANCEL

OK

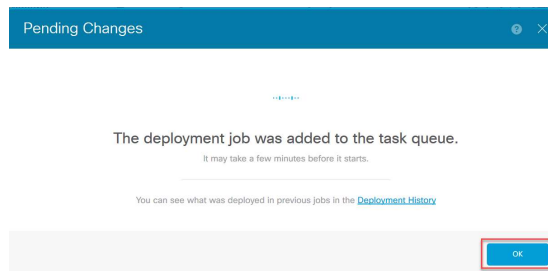
Once created click on the pending changes to apply the changes to the FTD.



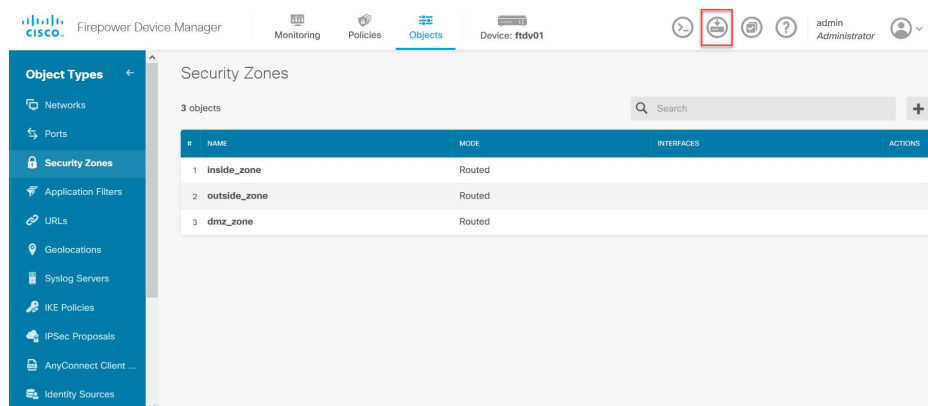
A list of pending changes will display.



Click Deploy Now.



The deployment is complete.

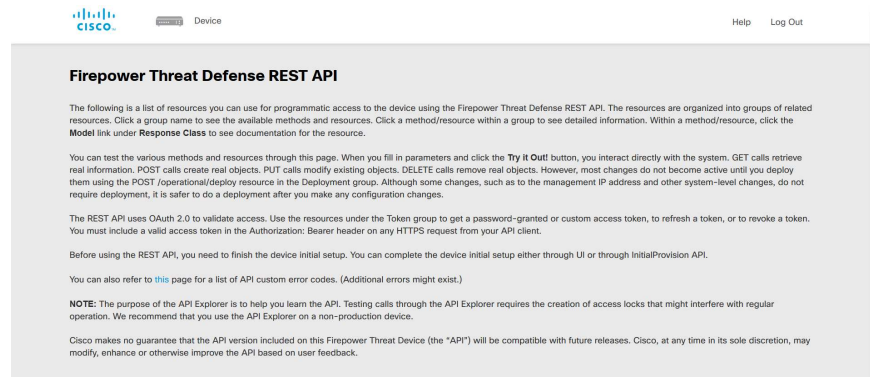


## API Explorer

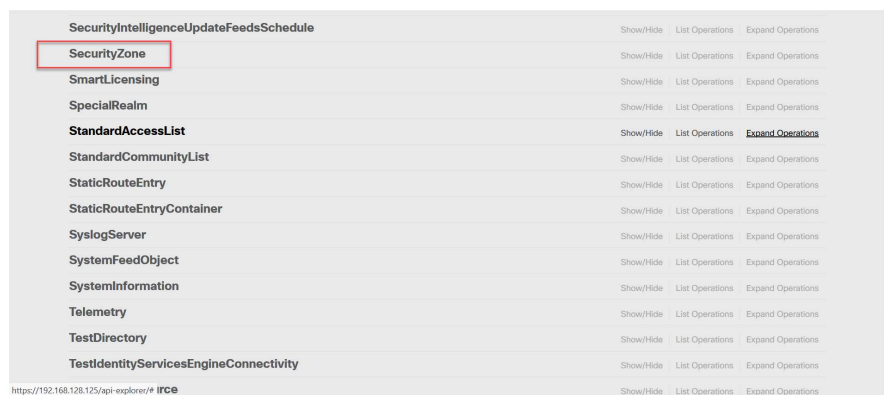
This section will demonstrate the API Explorer steps to create a Security Zone on the FTD.

<https://192.168.128.125/api-explorer>

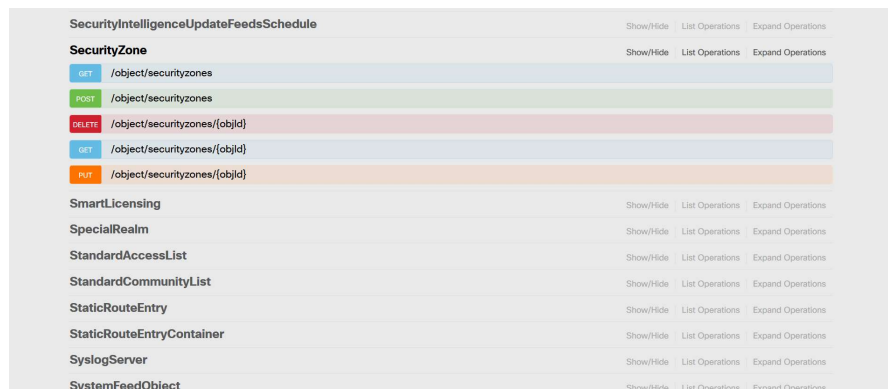
At the main screen, scroll down until you see the security zone on the left side.



Click on Security Zone.



Click on Get



Scroll down and click on Try Now.



The API call is shown in addition to the Security Zones that are configured on the FTD.



Got an error....

## **POSTMAN Process**

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.

## **Python Script**