

# Configure Rollback on SFTD When SFMC Not Reachable

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Background Information](#)

### [Configure](#)

[Network Diagram](#)

[Scenario](#)

[Procedure](#)

### [Troubleshooting](#)

---

## Introduction

This document describes how to rollback a deployment change from the Secure SFMC that affects the connectivity to SFTD.

## Prerequisites

### Requirements

The use of this feature is supported on Secure FirePOWER Threat Detection® version 6.7 onwards.

Cisco recommends that you have knowledge of these topics:

- Secure Firewall Management Center (SFMC®) configuration
- Cisco Secure FirePOWER Threat Defense (SFTD) configuration

### Components Used

- Secure Firewall Management Center for VMware version 7.2.1
- Secure Firepower Threat Defense for VMware version 7.2

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

There are scenarios where the communication to SFMC, SFTD, or between SFMC and SFTD is lost when a deployment change affects the network connectivity. You can roll back the configuration on the SFTD to the last-deployed configuration to restore the management connectivity.

Use the **configure policy rollback** command to roll back the configuration on the threat defense to the last-deployed configuration.

---

 **Note:** The **configure policy rollback** command was introduced in version 6.7

---

See the guidelines:

- Only the previous deployment is available locally on the threat defense; you cannot roll back to any earlier deployments.
- Rollback is supported for high availability from management center 7.2 onwards.
- Rollback is not supported for clustering deployments.
- The rollback only affects configurations that you can set in the management center. For example, the rollback does not affect any local configuration related to the dedicated Management interface, which you can only configure at the threat defense CLI. Note that if you changed data interface settings after the last management center deployment using the **configure network management-data-interface** command, and then you use the rollback command, those settings are not be preserved; they roll back to the last deployed management center settings.
- UCAPL/CC mode cannot be rolled back.
- Out-of-band SCEP certificate data that was updated during the previous deployment cannot be rolled back.
- During the rollback, connections can drop because the current configuration is cleared.

## Configure

### Network Diagram

This document uses this network setup:

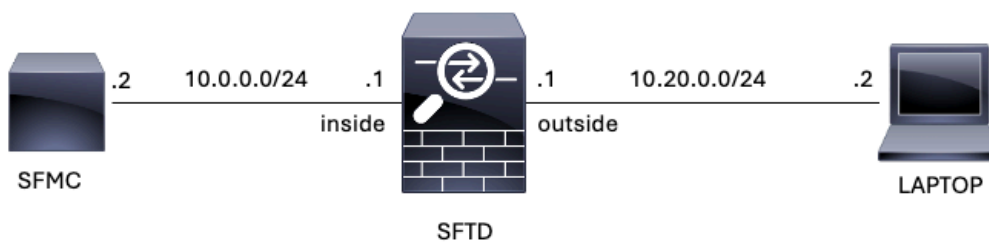


Image 1. Diagram

### Scenario

In this configuration, SFTD is managed by the SFMC using the Firewall inside interface, there is a rule that allows the reachability from the Laptop to the SFMC.

### Procedure

Step 1. The rule named **FMC-Access** was disabled on the SFMC, after deployment, the communication

from the Laptop to the SFMC is blocked.

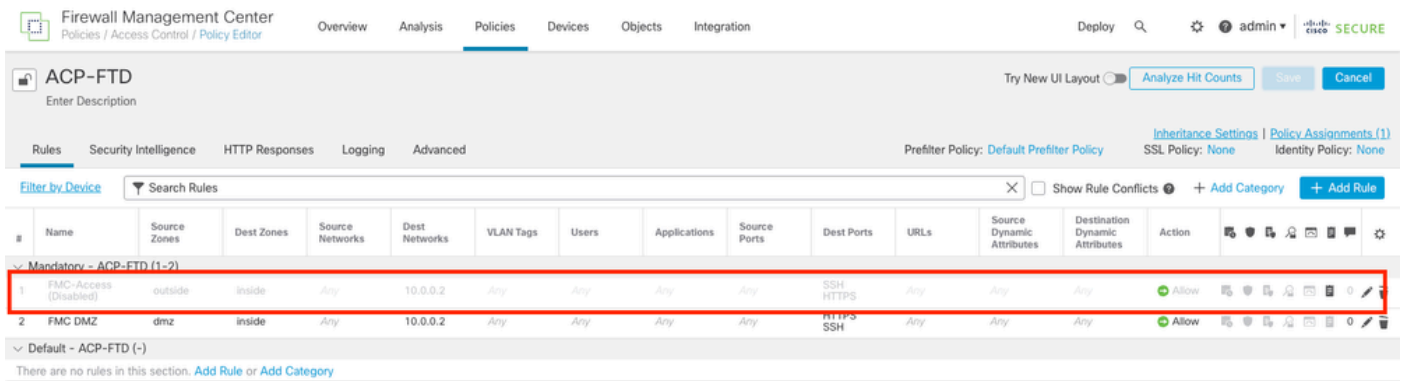


Image 2. The Rule that Allows SFMC Reachability Disabled

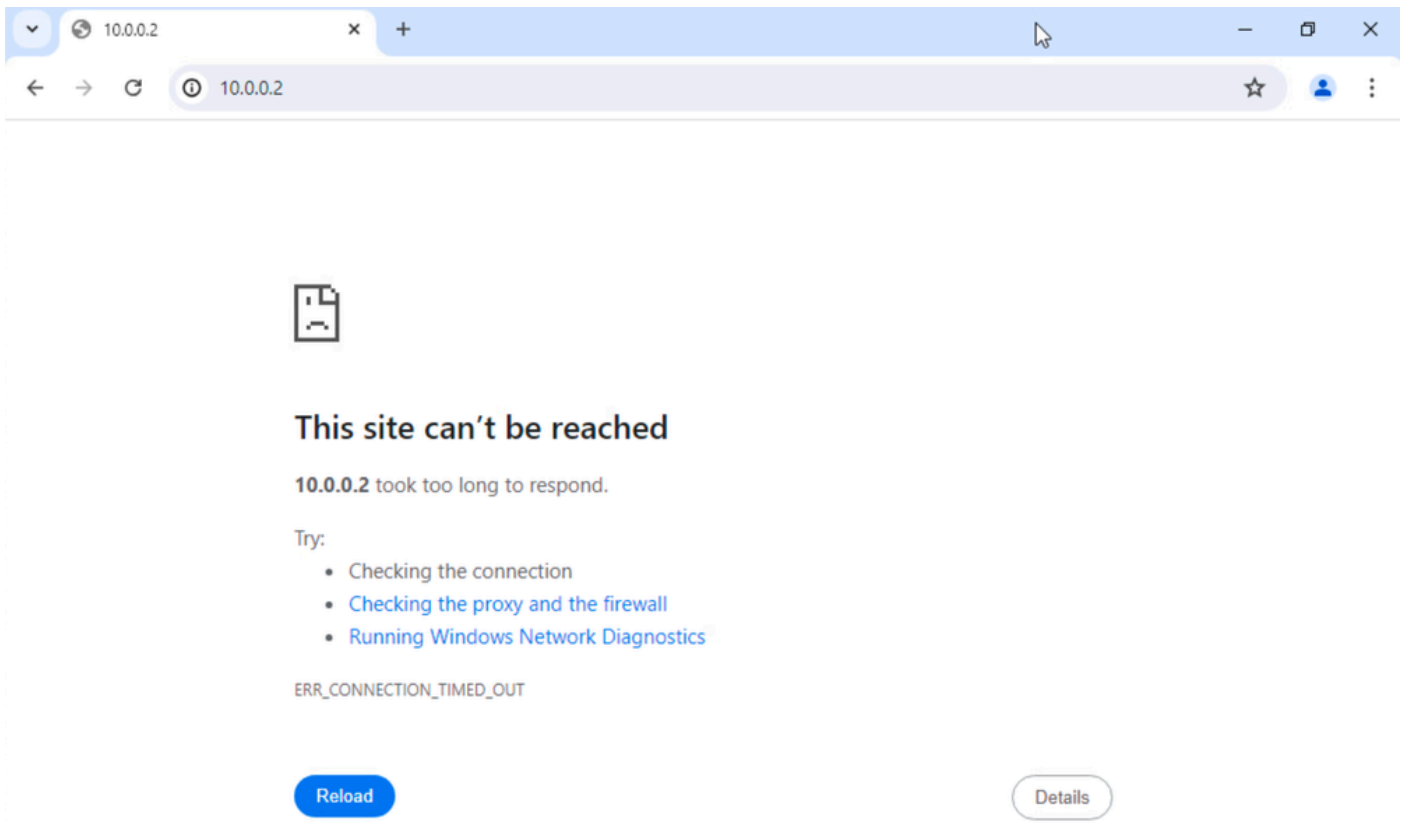



Image 3. SFMC Reachability from Laptop not Working

Step 2. Log in to the SFTD via SSH or console, then use the **configure policy rollback** command.

 **Note:** If access via SSH is not possible, connect via telnet.

```
<#root>
```

```
>
```

```
configure policy rollback
```

-----  
[Warning] Perform a policy rollback if the FTD communicates with the FMC on a data interface, and it ha  
and you want to perform a policy rollback for other purposes, then you should do the rollback on the FM

Checking Eligibility ....

===== DEVICE DETAILS =====

Device Version: 7.2.0

Device Type: FTD

Device Mode: Offbox

Device in HA: false

Device in Cluster: false

Device Upgrade InProgress: false

=====

Device is eligible for policy rollback

This command will rollback the policy to the last deployment done on Jul 15 20:38.

[Warning] The rollback operation will revert the convergence mode.

Do you want to continue (YES/NO)?

Step 3. Write the word **YES** to confirm the rollback of the last deployment, then wait until the rollback process ends.

<#root>

Do you want to continue (YES/NO)?

**YES**

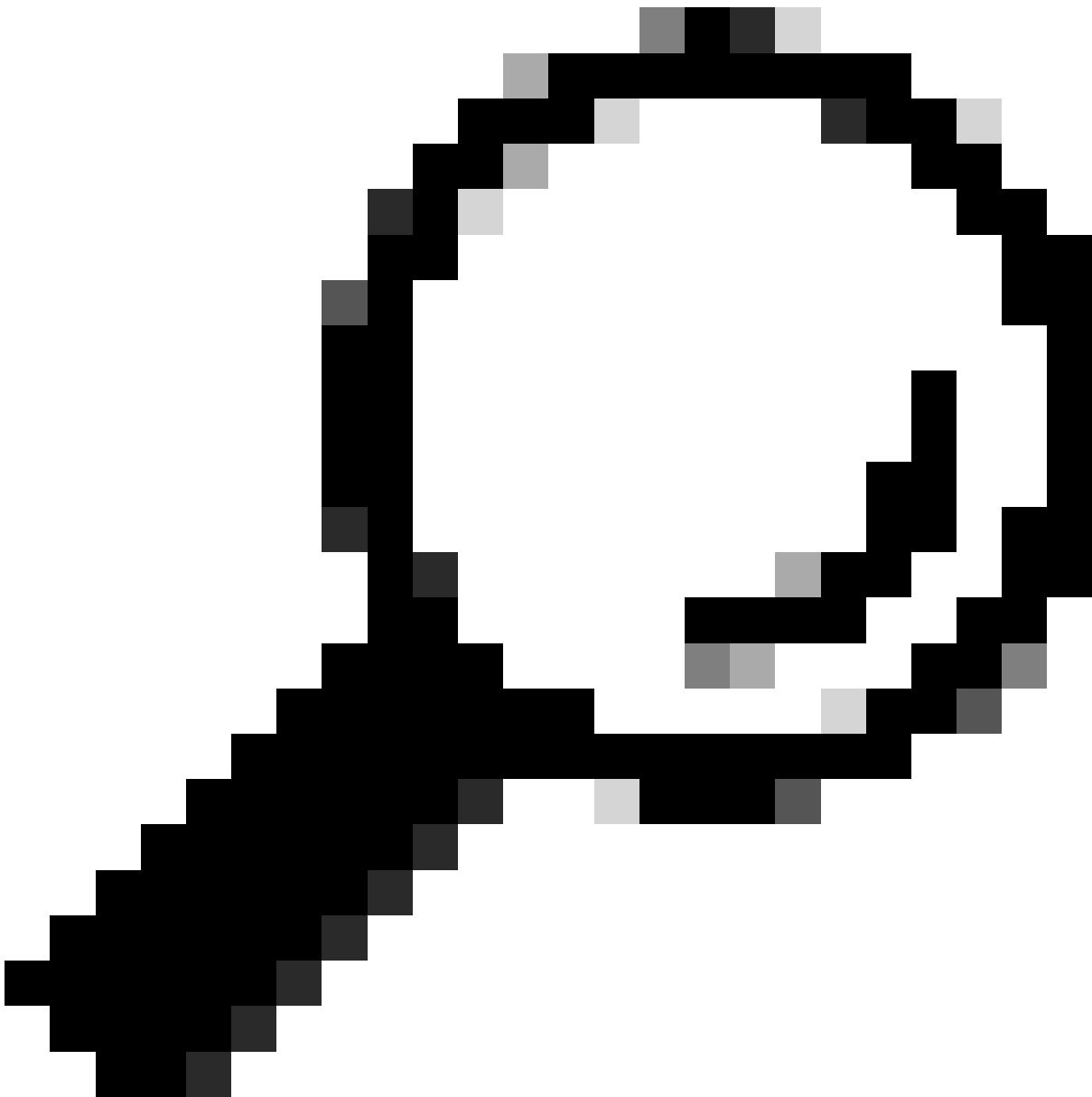
Starting rollback...

Deployment of Platform Settings to device.	Status: success
Preparing policy configuration on the device.	Status: success
Applying updated policy configuration on the device.	Status: success
Applying Lina File Configuration on the device.	Status: success
INFO: Security level for "diagnostic"set to 0 by default.	
Applying Lina Configuration on the device.	Status: success
Commit Lina Configuration.	Status: success
Commit Lina File Configuration.	Status: success
Finalizing policy configuration on the device.	Status: success

=====

**POLICY ROLLBACK STATUS: SUCCESS**

=====



**Tip:** In case rollback fails, contact Cisco TAC

---

Step 4. After the rollback, confirm the SFMC reachability. The SFTD notifies the SFMC that the rollback was completed successfully. In the SFMC, the deployment screen shows a banner stating that the configuration was rolled back.

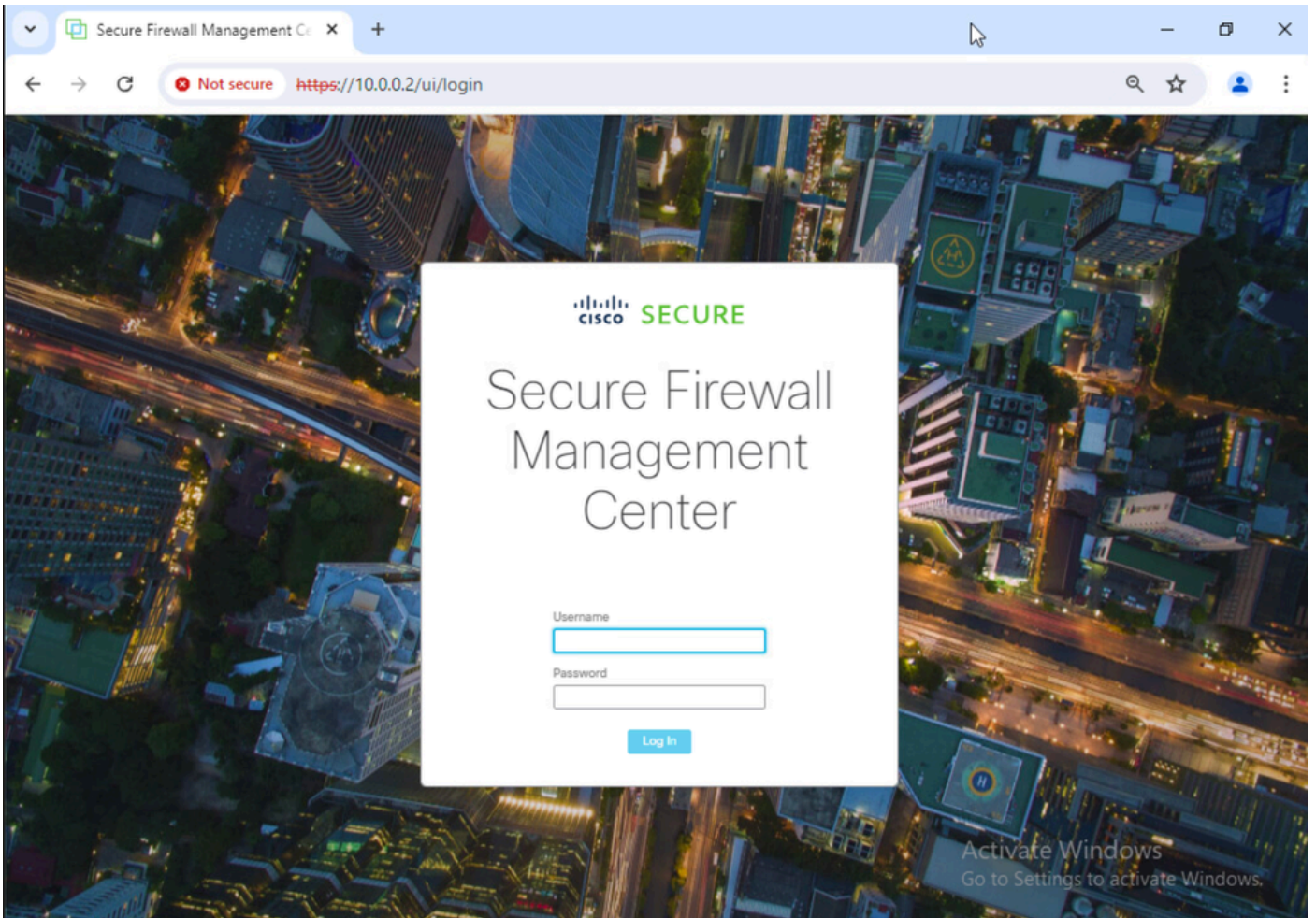


Image 4. SFMC Reachability from Laptop Restored

✔ FTD Rollback triggered from device is successful.

[Show deployment history](#)

Image 5. SFMC Message Confirming Rollback from SFTD

Step 5. When SFMC access is restored, resolve the SFMC configuration issue and redeploy.

Firewall Management Center Policies / Access Control / Policy Editor Overview Analysis Policies Devices Objects Integration Deploy  admin SECURE

ACP-FTD Enter Description Try New UI Layout  Analyze Hit Counts Save Cancel

Rules Security Intelligence HTTP Responses Logging Advanced Prefilter Policy: Default Prefilter Policy [Inheritance Settings](#) | [Policy Assignments \(1\)](#) SSL Policy: None Identity Policy: None

Filter by Device Search Rules  Show Rule Conflicts  + Add Category + Add Rule

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destination Dynamic Attributes	Action	Tools
Mandatory - ACP-FTD (1-2)															
1	FMC-Access	outside	inside	Any	10.0.0.2	Any	Any	Any	Any	SSH HTTPS	Any	Any	Any	Allow	Tools
2	FMC DMZ	dmz	inside	Any	10.0.0.2	Any	Any	Any	Any	HTTPS SSH	Any	Any	Any	Allow	Tools
Default - ACP-FTD (-) There are no rules in this section. <a href="#">Add Rule</a> or <a href="#">Add Category</a>															

Image 6. Revert the Changes

## Troubleshooting

In case rollback fails, contact Cisco TAC, for additional issues during the process please review the next article:

- [Deployment Rollback](#)