Recover Logical Device Password from Chassis Manager

Contents

Introduction

This document describes how to recover the password of a logical device from Secure Firewall Chassis Manager (FCM).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Secure Firewall eXtensible Operating System (FXOS)
- Cisco Adaptive Secure Appliance (ASA)
- Secure Firewall Threat Defense (FTD)

Components Used

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

- Secure Firewall 4100/9300 devices.
- Logical device, either ASA or FTD, already created and in online state.

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

The password of a logical device is configured when created, and this can also be changed after the bootstrap configuration has been deployed from CLI.

Procedure

This procedure describes how to change the password from the Chassis Manager GUI after a logical device is already created. This applies to ASA and FTD logical devices.

Warning: The procedure to recover the password overwrites the bootstrap configuration from FCM. This means that any changes to the management IP performed from logical device CLI after device creation are restored as well.

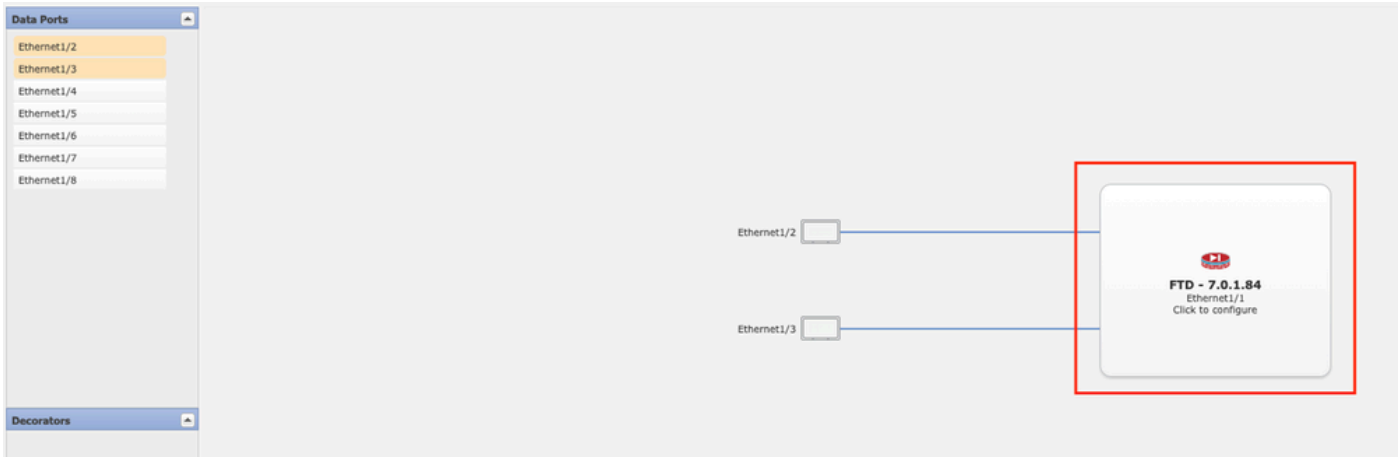
Configurations

1. Log into Secure Firewall Chassis Manager.

2. In order to change the password of the logical device, navigate to **Logical Device > Edit.**

Logical Device Menu

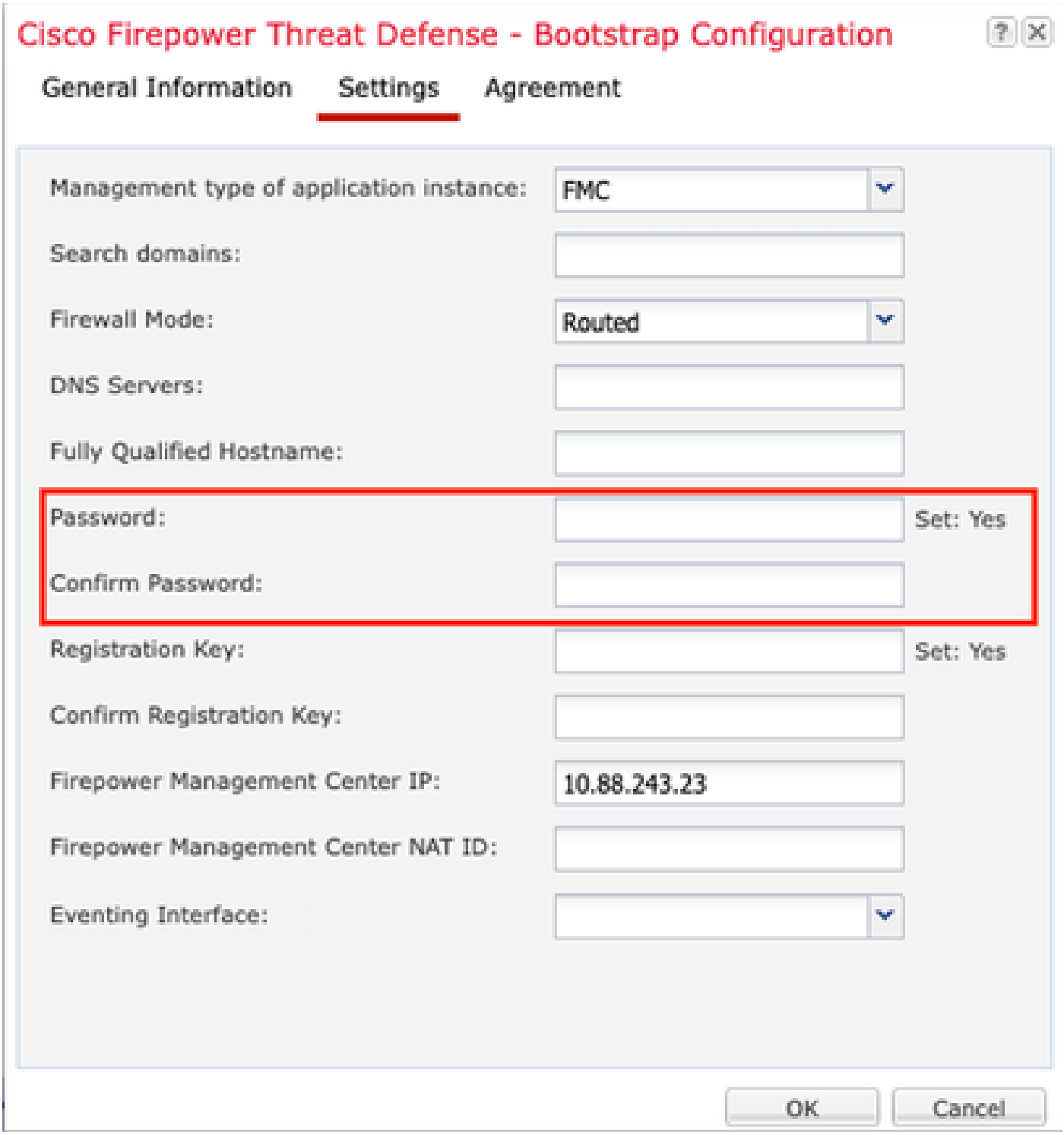
3. Enter the Bootstrap configuration by clicking on the device button.



Bootstrap Configuration

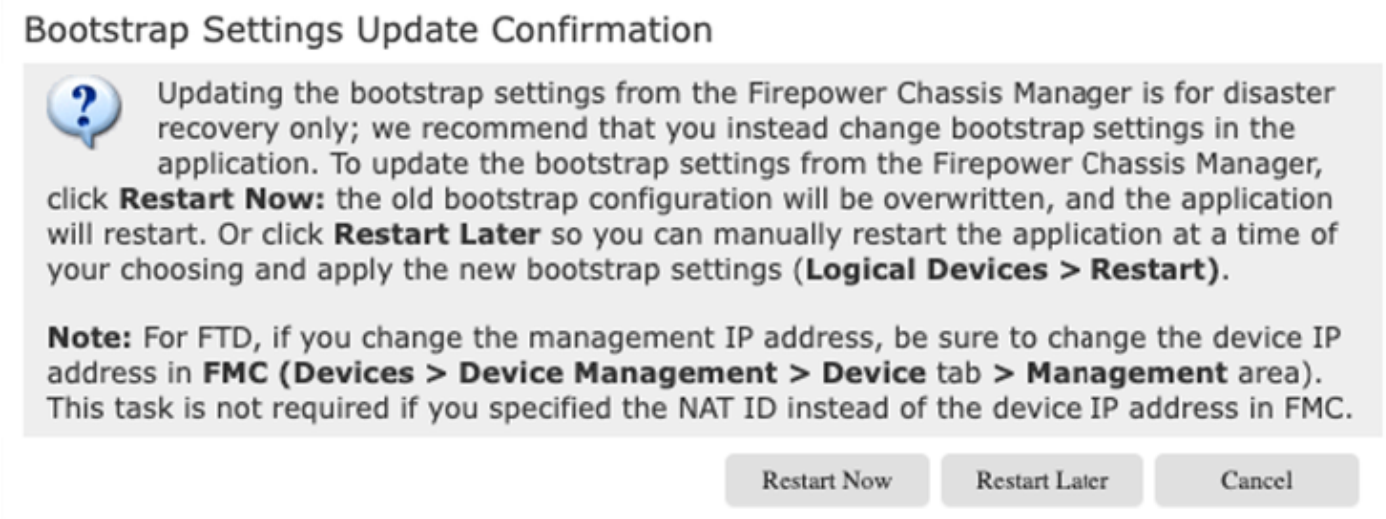
4. Click on **Settings**. Observe that **Password** is already set. Enter your new password and confirm it.

This action changes the password, but a reboot is needed to perform the changes.



Password Field

5. When you save the changes, a confirmation message appears. You can choose to restart the device now or later in **Logical Devices > Restart.**



Save Changes Warning

6. Once the logical device comes back, you can SSH to the device and access expert mode with the new credentials.

Related Information

- Cisco Technical Support & Downloads