Password Recovery for SFTD/ASA Instance through FXOS CLI

Contents

Introduction

This document describes how to recover the password for an SFTD or an ASA instance via the FXOS CLI.

Prerequisites

Requirements

SFTD or ASA instances over FP41XX or FP93XX Secure Firewall Series.

Cisco recommends that you have knowledge of this topic:

- Cisco Firepower eXtensible Operating System (FXOS) Command Line Interface (CLI)

Components Used

- Cisco Secure Firewall 4110
- Cisco Secure Firewall ASA software

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 password for a device is lost and needs to be recovered, and the use of the FXOS Firepower Chassis Manager is not an option. For SFTD or ASA instances over FP41XX or FP93XX Secure Firewall Series, password recovery can be accomplished via FXOS CLI.

Caution: This process requires a reboot of the instance, which can cause a traffic outage.

Configure

Procedure

Step 1**.** Log in to FXOS CLI with the Admin rights credentials.

Step 2**.** Get the **App Name**, **Identifier,** and **Slot ID** information.

scopessa

show app-instance

Example:

<#root>

```
FPR4110-K9-1# scope ssa
```

```
FPR4110-K9-1 /ssa # show app-instance

App Name Identifier Slot ID

Admin State Oper State   Running Version Startup Version Deploy Type Turbo Mode Profile Name Cluster St
-------- ---------- ------- ----------- -----------  --------------- --------------- ----------- ------

asa      ASA        1

Enabled     Online       9.16.3(14)       9.16.3(14)       Native      No                    Not Appl
```

Step 3. Specify the new admin and enable password, then save the changes.

scope logical-device identifier

scope mgmt-bootstrap app_name

scope bootstrap-key-secret PASSWORD

set value

Enter a value: password

Confirm the value: password

commit-buffer

exit

exit

Example:

```
FPR4110-K9-1 /ssa # scope logical-device ASA
FPR4110-K9-1 /ssa/logical-device # scope mgmt-bootstrap asa
FPR4110-K9-1 /ssa/logical-device/mgmt-bootstrap # scope bootstrap-key-secret PASSWORD
FPR4110-K9-1 /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret # set value

Enter value:

Confirm the value:
Warning: Bootstrap changes are not automatically applied to app-instances. To apply the changes, please
FPR4110-K9-1 /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* #commit-buffer
FPR4110-K9-1 /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret # exit
FPR4110-K9-1 /ssa/logical-device/mgmt-bootstrap # exit
```

Step 4**.** Clear the management bootstrap, then save the changes.

scope slot slot_id

scope app-instance app_name identifier

clear-mgmt-bootstrap

commit-buffer

Example:

```
FPR4110-K9-1 /ssa # scope slot 1
FPR4110-K9-1 /ssa/slot # scope app-instance asa ASA
FPR4110-K9-1 /ssa/slot/app-instance # clear-mgmt-bootstrap
Warning: Clears the application management bootstrap. Application needs to be restarted for this action
FPR4110-K9-1 /ssa/slot/app-instance* # commit-buffer
```

Step 5. Restart the instance.

restart

commit-buffer

Example:

```
FPR4110-K9-1 /ssa/slot/app-instance # restart
FPR4110-K9-1 /ssa/slot/app-instance* # commit-buffer
```

Note: The instance restarts once the changes are saved.

Step 6. Log in to the SFTD/ASA instance via SSH using the new credentials.