

Password Recovery Procedure For Firepower 9300/4100 Series Appliances

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Step By Step Password Recovery Procedure](#)

[Related Information](#)

Introduction

This document describes how to recover the Supervisor Management Input Output (MIO) password for FirePOWER 9300/4100 series appliances.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- Cisco Firepower 4100 Series and 9300 appliances.

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, make sure that you understand the potential impact of any command.

Background Information

Password recovery procedure is performed when a user forgets the Supervisor MIO password. To achieve this, all the database files and configurations are reset to factory default setting while you perform the password recovery procedure.

Note: This procedure should not be used to reset the password which is already known.

Step By Step Password Recovery Procedure

In order to recover passwords for the Supervisor MIO, perform these steps:

Step 1. Connect a PC to the console port using the provided console cable, and connect to the console using a terminal emulator set for 9600 baud, 8 data bits, no parity, 1 stop bit, no flow control. Check [Cisco Firepower 9300 Hardware Installation Guide](#) for more information about the console cable.

Note: Password recovery needs console access to the FXOS Supervisor.

Step 2. Power off the system, and then power it on.

Step 3. While booting, press the **ESC** or **CTRL + L** key when you are prompted to enter ROMMON mode.

```
!! Rommon image verified successfully !!
```

```
Cisco System ROMMON, Version 1.0.09, RELEASE SOFTWARE  
Copyright (c) 1994-2015 by Cisco Systems, Inc.  
Compiled Thu 05/28/2015 17:21:39.46 by gilchen
```

```
Current image running: Boot ROM0  
Last reset cause: ResetRequest  
DIMM Slot 0 : Present  
DIMM Slot 1 : Present  
No USB drive !!  
BIOS has been locked !!
```

```
Platform FPR9K-SUP with 16384 Mbytes of main memory  
MAC Address: b0:aa:77:2f:93:74
```

```
find the string ! boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.3.14.69.SPA  
bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA
```

```
Use BREAK, ESC or CTRL+L to interrupt boot.  
Use SPACE to begin boot immediately.  
Boot interrupted.  
rommon 1 >
```

Step 4. Make a note of kickstart image and system image highlighted above.

!! Rommon image verified successfully !!

Cisco System ROMMON, Version 1.0.09, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.
Compiled Thu 05/28/2015 17:21:39.46 by gilchen

Current image running: Boot ROM0
Last reset cause: ResetRequest
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
BIOS has been locked !!

Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address: b0:aa:77:2f:93:74

**find the string ! boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.3.14.69.SPA
bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA**

Use BREAK, ESC or CTRL+L to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.
rommon 1 >

Step 5. Load kickstart image as you enter **boot (kickstart image name)** command at rommon prompt.

```
rommon 1 > boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.3.14.69.SPA
!! Kickstart Image verified successfully !!
```

```
Linux version: 2.6.27.47 (security@cisco.com) #1 SMP Tue Nov 24 12:10:28 PST 2015
[ 0.000000] Fastboot Memory at 0c100000 of size 201326592
Usage: init 0123456SsQqAaBbCcUu
INIT: POST INIT Starts at Wed Jun 1 13:46:33 UTC 2016
can't create lock file /var/lock/mtab-302: No such file or directory (use -n flag to override)
S10mount-ramfs.supnuovaca Mounting /isan 3000m
Mounted /isan
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2015, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch(boot)#
```

Step 6. At the **switch(boot)#** prompt, enter the **config terminal** command in order to navigate to configure mode and thereafter, enter the **admin-password erase** command to reset the password. Later the user is prompted for the confirmation.

Warning: If you select **Y** at this prompt, it erases all the configuration and brings the system back to the factory default configuration.

```
switch(boot)#
switch(boot)# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(boot)(config)# admin-password erase
Your password and configuration will be erased!
Do you want to continue? (y/n) [n] y
```

Step 7. Exit to switch(boot)# prompt and load system image saved earlier to complete the procedure.

```
switch(boot)(config)# exit
switch(boot)# load bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA

Uncompressing system image: bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA
```

<lines ommitted>

---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of the system. Only minimal configuration including IP connectivity to the Fabric interconnect and its clustering mode is performed through these steps.

Type Ctrl-C at any time to abort configuration and reboot system. To back track or make modifications to already entered values, complete input till end of section and answer no when prompted to apply configuration.

You have chosen to setup a new Security Appliance. Continue? (y/n): **y**

Enforce strong password? (y/n) [**y**]: **n**

Enter the password for "admin":
Confirm the password for "admin":

Enter the system name: **FF09-FPR9300-1**

Physical Switch Mgmt0 IP address : **192.168.10.10**

Physical Switch Mgmt0 IPv4 netmask : **255.255.255.0**

IPv4 address of the default gateway : **192.168.10.1**

Configure the DNS Server IP address? (yes/no) [**n**]: **n**

Configure the default domain name? (yes/no) [**n**]: **n**

Following configurations will be applied:

```
Switch Fabric=A
System Name=FF09-FPR9300-1
Enforced Strong Password=no
Physical Switch Mgmt0 IP Address=192.168.10.1
Physical Switch Mgmt0 IP Netmask=255.255.255.0
Default Gateway=192.168.10.1
Ipv6 value=0
```

Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): **yes**
Applying configuration. Please wait.
Configuration file - **Ok**

Cisco FPR Series Security Appliance
FF09-FPR9300-1 login:

Related Information

- [Navigating the Cisco FXOS Documentation](#)
- [Cisco ASA for Firepower 9300 Quick Start Guide](#)
- [Technical Support & Documentation - Cisco Systems](#)