Recover Password for Firepower 2100 Series

Contents

Introduction

Support Status

Prerequisites

- Requirements
- Components Used

Before Reset

Procedure

If you can still log in

Introduction

This document describes how to recover a Firepower 2100 when the admin password is lost.

Support Status

The Firepower 2100 series (2110, 2120, 2130, and 2140) is end of sale. These are important dates to make note of:

- End-of-sale date: May 27, 2025
- Software maintenance ended on: May 27, 2026
- Last date of support: May 31, 2030

For more information, refer to the EOL15548 document.

Recovery is a ROMMON factory reset. It erases the configuration and returns Firewall Threat Defense to factory defaults (it is not a password-only change). Use this procedure only when you cannot log in. If you still know your password, or you can still reach FXOS; use the non-destructive options in If you can still log in.

Prerequisites

Requirements

- Serial console access to the Firepower 2100.
- The ability to power-cycle the appliance.
- A maintenance window; this reset takes approximately 20-40 minutes, depending on the model, and the device is unusable until setup is completed.
- A record of the management IP address, manager registration, and high-availability role, if you have one. Otherwise, you must build that configuration again.

Components Used

Firepower 2110, 2120, 2130, and 2140 running Firewall Threat Defense. Command behavior follows the FXOS Troubleshooting Guide for Firewall Threat Defense, updated February 24, 2026: Perform a Factory Reset from ROMMON (Password Reset).

Before Reset

- Try the factory default admin account once. If the password was never changed, you can log in and skip this procedure. The first successful login still requires you to set a new password.
- This reset deletes the Firewall Threat Defense configuration and restores the factory default. Smart Licensing association, cloud registration, management connectivity, and high availability are not preserved.
- Register the firewall to its Firewall Management Center again after the reset, and rebuild high availability if the device was in a pair.
- On an ASA-mode Firepower 2100, the same ROMMON reset applies. Finish the setup with the ASA chapter of the **Firepower 2100 Getting Started Guide** instead of the threat defense chapter.

Procedure

1. Power-cycle the appliance. When ROMMON prints the interrupt prompt, press **ESC**.

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

---

2. Confirm the ROMMON version before you choose a command.

```
rommon 1 > show info
```

Example:

```
Cisco System ROMMON, Version 1.0.06, RELEASE SOFTWARE
```

---

3. Factory-reset the device, for ROMMON 1.0.06 or later:

```
rommon 2 > factory-reset
```

For ROMMON 1.0.04 only:

```
rommon 2 > password_reset
```

---

4. Do not use the **password_reset** on 1.0.06 or later. That command is not the current reset. On 1.0.06 or later, the **factory-reset** asks for two confirmations. Answer **yes**, then type **ERASE**. Any other value cancels the reset:

```
Warning: All configuration will be permanently lost with this operation
         and application will be initialized to default configuration.
         This operation cannot be undone after booting the application image.

         Are you sure you would like to continue ? yes/no [no]: yes
         Please type 'ERASE' to confirm the operation or any other value to cancel: ERASE
```

ROMMON then offers to boot the image already on the disk and asks again. Answer **yes**, and the image name differs by device. This example is only the prompt:

```
Rommon will continue to boot disk0: <installed-image>
Are you sure you would like to continue ? yes/no [no]: yes
```

---

5. If the device does not continue on its own, boot it.

```
rommon 3 > boot
```

---

6. When the login prompt is available, sign-in with the factory default admin account. The password is **Admin123**. The same account applies when Secure Firewall Device Manager is ready. Change the password when prompted. Do not leave the factory default in place. Finish the setup from the Firepower 2100 Getting Started Guide. Re-enter the management address and register the device again.

- Threat Defense with Firewall Management Center: Firewall Management Center Deployment.
- Threat Defense with Firewall Device Manager: Firewall Device Manager Deployment - The factory admin account is the CLI and Device Manager.
- ASA Appliance Mode: ASA Appliance Mode with ASDM. Chassis Manager is not used in this mode.
- ASA Platform Mode: ASA Platform Mode with ASDM and Firewall Chassis Manager.

If you can still log in

Do not factory-reset the appliance when a password change is enough.

- When the Firewall Threat Defense is reachable, from the threat defense CLI, run the **configure user password admin**. You must enter the current password.
- If the Threat Defense is offline and you can still log into FXOS, from FXOS, run **scope security**, then **set password**, then **commit-buffer**. On version 6.4 and later, FXOS asks for the current password.
- If you know the password and you want a factory default configuration without using ROMMON, from FXOS local-mgmt, run the base-install erase procedure in the same guide. That path also wipes the configuration and it is not the lost-password procedure.
- For additional details: FXOS Troubleshooting Guide, Image Management.