Firepower 2100系列的恢复密码

目录

简介

支持状态

先决条件

- 要求
- 使用的组件

重置前

步骤

如果仍然可以登录

简介

本文档介绍在管理员密码丢失时如何恢复Firepower 2100。

支持状态

Firepower 2100系列（2110、2120、2130和2140）已停止销售。以下是需要注意的重要日期：

- 终止销售日期：2025年5月27日
- 软件维护结束于：2026年5月27日
- 最后支持日期:2030年5月31

有关详细信息，请参阅EOL1548文档。

恢复是ROMMON出厂重置。它会清除配置并将防火墙威胁防御恢复为出厂默认设置（并非仅更改密码）。 仅在无法登录时使用此过程。如果您仍然知道密码，或者仍然可以访问FXOS;使用If you can still log in中的非破坏性选项。

先决条件

要求

- 串行控制台访问Firepower 2100。
- 能够重新启动设备。
- 维护窗口；此重置大约需要20-40分钟（具体取决于型号），并且设备在设置完成之前不可用。
- 管理IP地址、经理注册和高可用性角色的记录（如果有）。否则，必须重新构建该配置。

使用的组件

运行防火墙威胁防御的Firepower 2110、2120、2130和2140。命令行为遵循2026年2月24日更新的《防火墙威胁防御FXOS故障排除指南》：从ROMMON执行出厂重置（密码重置）。

重置前

- 尝试一次出厂默认管理员帐户。如果密码从未更改，您可以登录并跳过此过程。首次成功登录仍需要您设置新密码。
- 此重置将删除防火墙威胁防御配置并恢复出厂默认设置。智能许可关联、云注册、管理连接和高可用性不会得到保留。
- 重置后，再次将防火墙注册到其防火墙管理中心，如果设备成对，则重建高可用性。
- 在ASA模式Firepower 2100上，应用相同的ROMMON重置。使用Firepower 2100入门指南的ASA一章（而不是威胁防御一章）完成设置。

步骤

1.重新通电设备。当ROMMON打印中断提示时，按ESC。

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

2.在选择命令之前，请确认ROMMON版本。

```
rommon 1 > show info
```

示例：

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

3.对ROMMON 1.0.06或更高版本，出厂重置设备：

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

仅适用于ROMMON 1.0.04:

```
rommon 2 > password_reset
```

4.请勿在1.0.06或更高版本上使用password_reset。该命令不是当前重置。在1.0.06或更高版本上，factory-reset会请求两个确认。回答yes，然后键入ERASE。任何其他值都会取消重置：

```
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
```

然后，ROMMON提供引导磁盘上已经存在的映像，并再次询问。回答yes，并且映像名称因设备而异。此示例仅提示符：

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

5.如果设备无法自行继续，请启动它。

```
rommon 3 > boot
```

6.当登录提示可用时，使用出厂默认管理员帐户登录。密码是Admin123。当Secure Firewall Device Manager准备就绪时，应用相同的帐户。出现提示时更改密码。不要保留原厂默认值。从Firepower 2100入门指南中完成设置。重新输入管理地址并再次注册设备。

- 通过防火墙管理中心进行威胁防御：防火墙管理中心部署。
- 使用防火墙设备管理器进行威胁防御：防火墙设备管理器部署 — 工厂管理员帐户是CLI和设备管理器。
- ASA设备模式：带ASDM的ASA设备模式。此模式下不使用机箱管理器。
- ASA平台模式：带ASDM和防火墙机箱管理器的ASA平台模式。

如果仍然可以登录

当密码更改足够时，请勿出厂重置设备。

- 当防火墙威胁防御可访问时，从威胁防御CLI运行configure user password admin。您必须输入当前密码。
- 如果威胁防御处于脱机状态，并且您仍然可以登录FXOS，请从FXOS运行scope security，然后设置password，然后执行commit-buffer。在6.4版及更高版本中，FXOS会要求输入当前密码。
- 如果您知道密码，并且希望在不使用ROMMON的情况下使用出厂默认配置，请从FXOS本地管理运行同一指南中的基本安装擦除过程。该路径还擦除配置，而不是丢失密码过程。
- 有关其他详细信息：FXOS故障排除指南，映像管理。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。