Understand Rebranding Device Outputs to Cisco Secure Firewall

Contents

Introduction

This document describes insight into Rebranding Device Outputs to Cisco Secure Firewall.

Prerequisites

Background Information

- Displayed device names now match other branding materials
- This creates a stronger brand and a more straightforward user experience
- No functional impact to any platforms; only the text has changed.
- Older FTD hardware platforms (FPR1010/11XX, FPR41XX, FPR93XX) still use Firepower branding
- Some system defaults and component names can still use firepower

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Next Gen Firewall(NGFW) portfolio

Components Used

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

- Firepower Management Center(FMC) version 7.6.0
- Firepower Device Manager(FDM) version 7.6.0
- All Virtual Firepower Threat Defense(FTD) version 7.6.0
- Cisco Secure Firewall 31XX,42XX

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.

Feature Description

How it works:

- Full model names and short model names for CSF31XX, CSF42XX, Firewall Threat Defense (FTD) Virtual, and all Firewall Management Center (FMC) platforms contain Cisco Secure Firewall branding.
- The CSF31XX FDM software is now SFDM, Secure Firewall Device Manager.
- There are no functional components to this feature.
- There are no configuration options for this feature.

Upgrading:

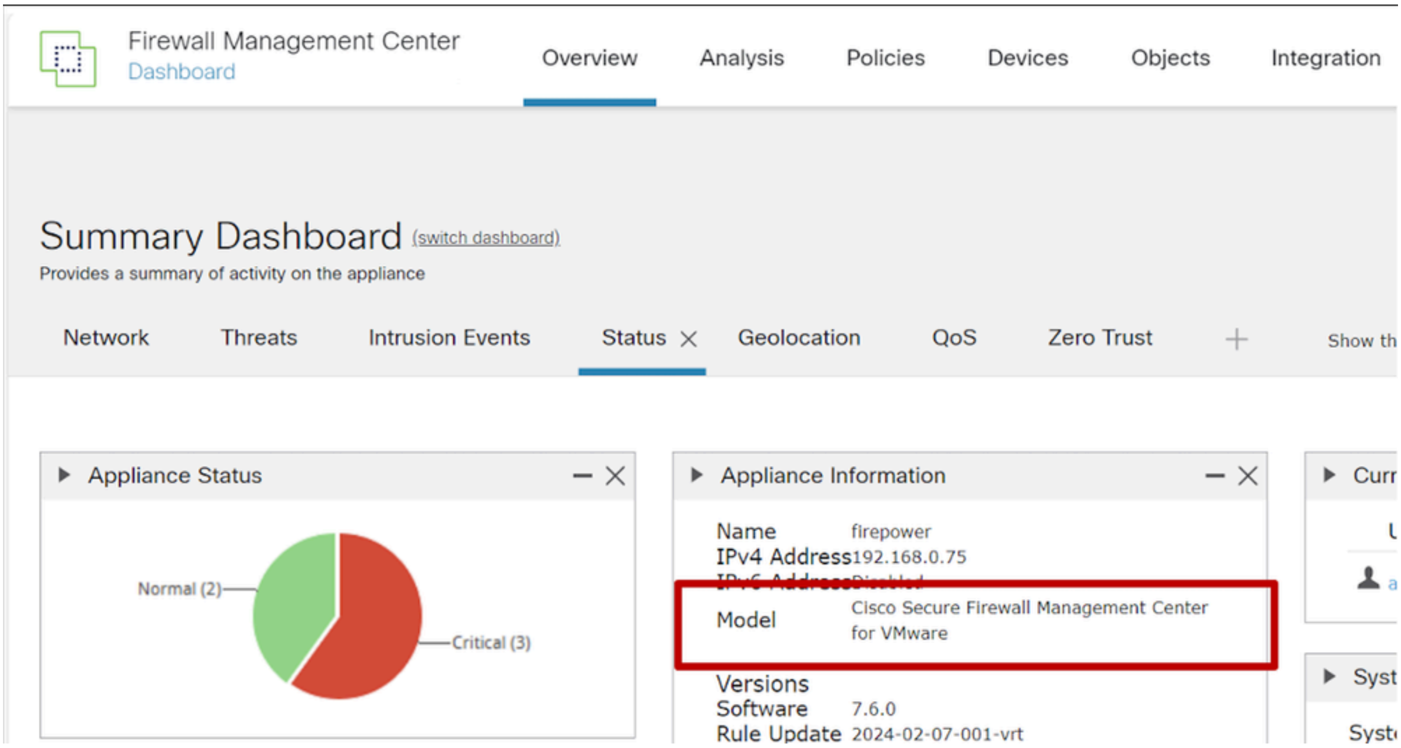
- When upgrading to Secure Firewall 7.6, all relevant CLIs and GUIs updated to reflect current branding.
- No issues during upgrade for registered devices
  - If Firewall Threat Defense (FTD) is upgraded, Firewall Management Center (FMC) update its GUI with current branding.
  - If Firewall Management Center (FMC) is upgraded, all registered devices restore connectivity after upgrade as expected.

Configure

Firewall Management Center Examples

Summary Status:

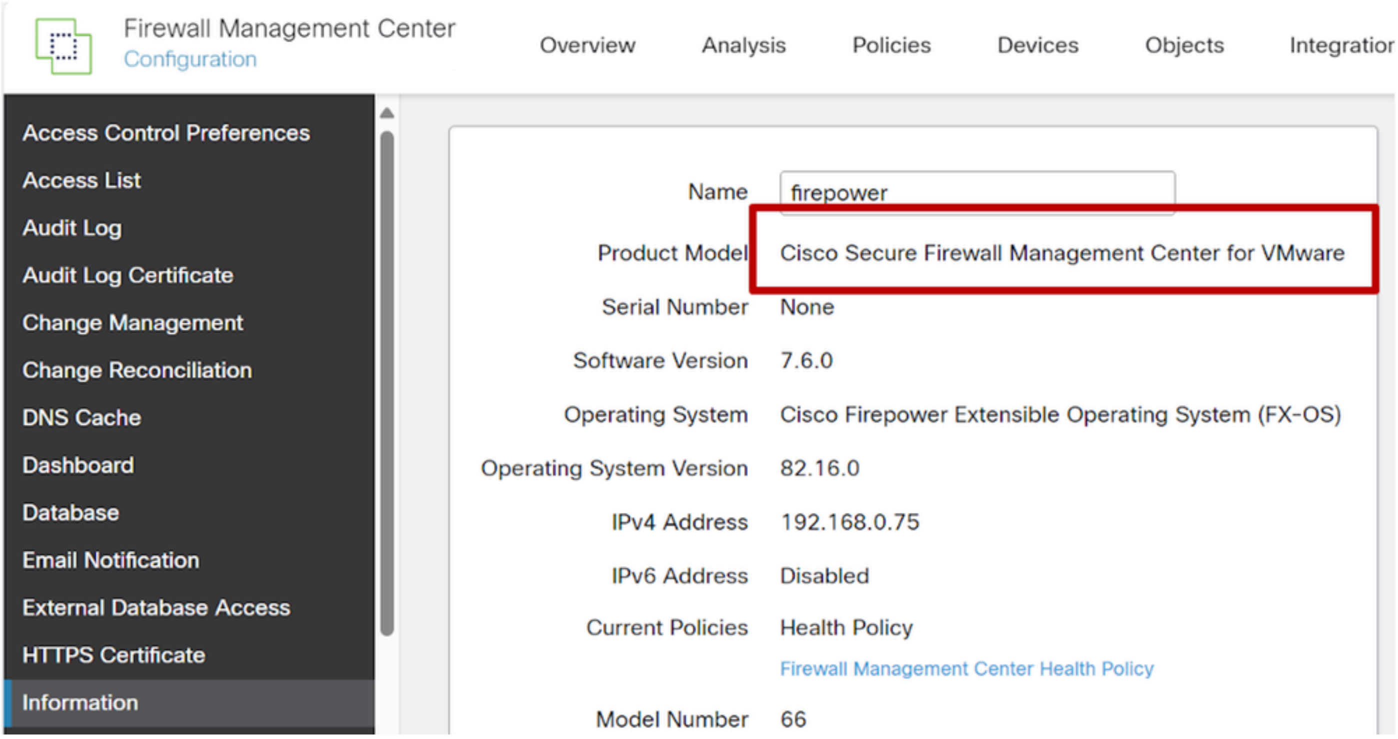
- Management Center model name has Cisco branding prepended.



Name firepower
IPv4 Address 192.168.0.75
IPv6 Address Disabled
Model Cisco Secure Firewall Management Center for VMware
Versions
Software 7.6.0
Rule Update 2024-02-07-001-vrt

Configuration Information:

- Management Center model name has Cisco branding prepended.



Name: firepower

Product Model: Cisco Secure Firewall Management Center for VMware

Serial Number: None

Software Version: 7.6.0

Operating System: Cisco Firepower Extensible Operating System (FX-OS)

Operating System Version: 82.16.0

IPv4 Address: 192.168.0.75

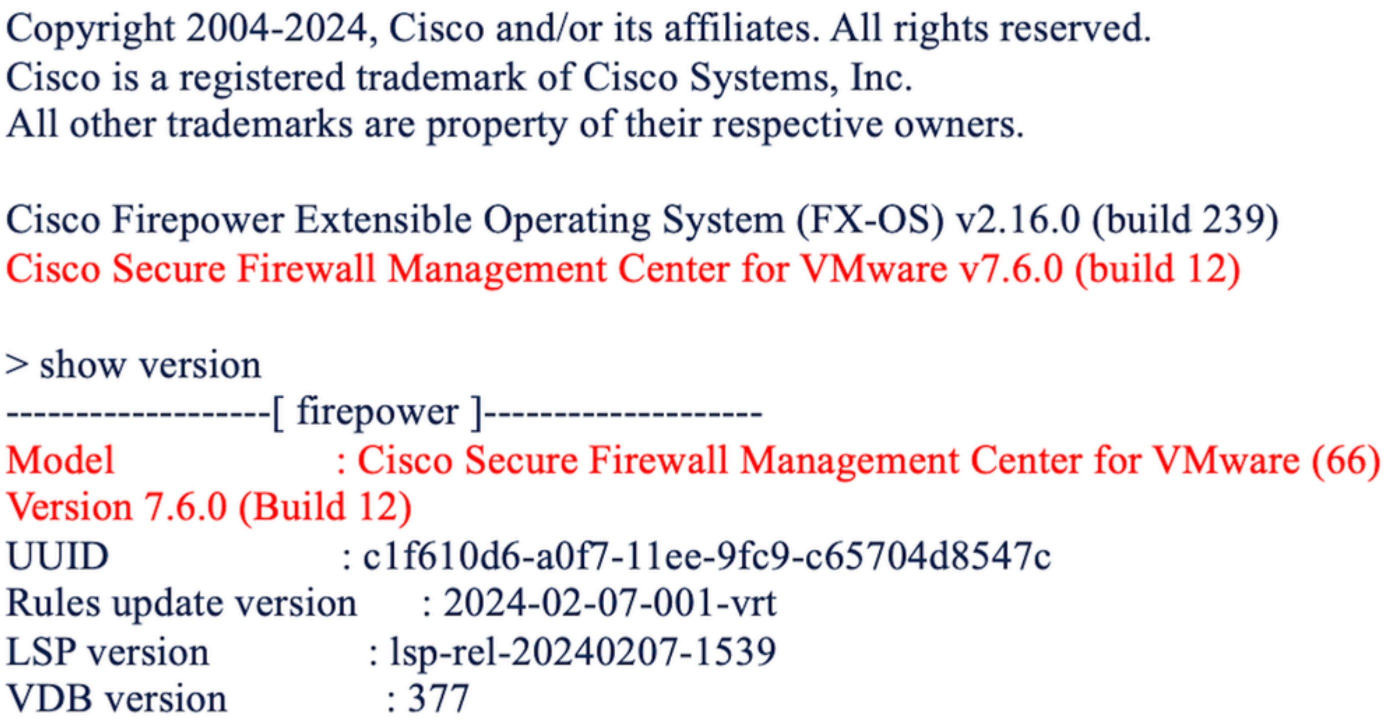
IPv6 Address: Disabled

Current Policies: Health Policy
Firewall Management Center Health Policy

Model Number: 66

CLI Output:

- Full model name is shown with Cisco Secure Firewall branding.

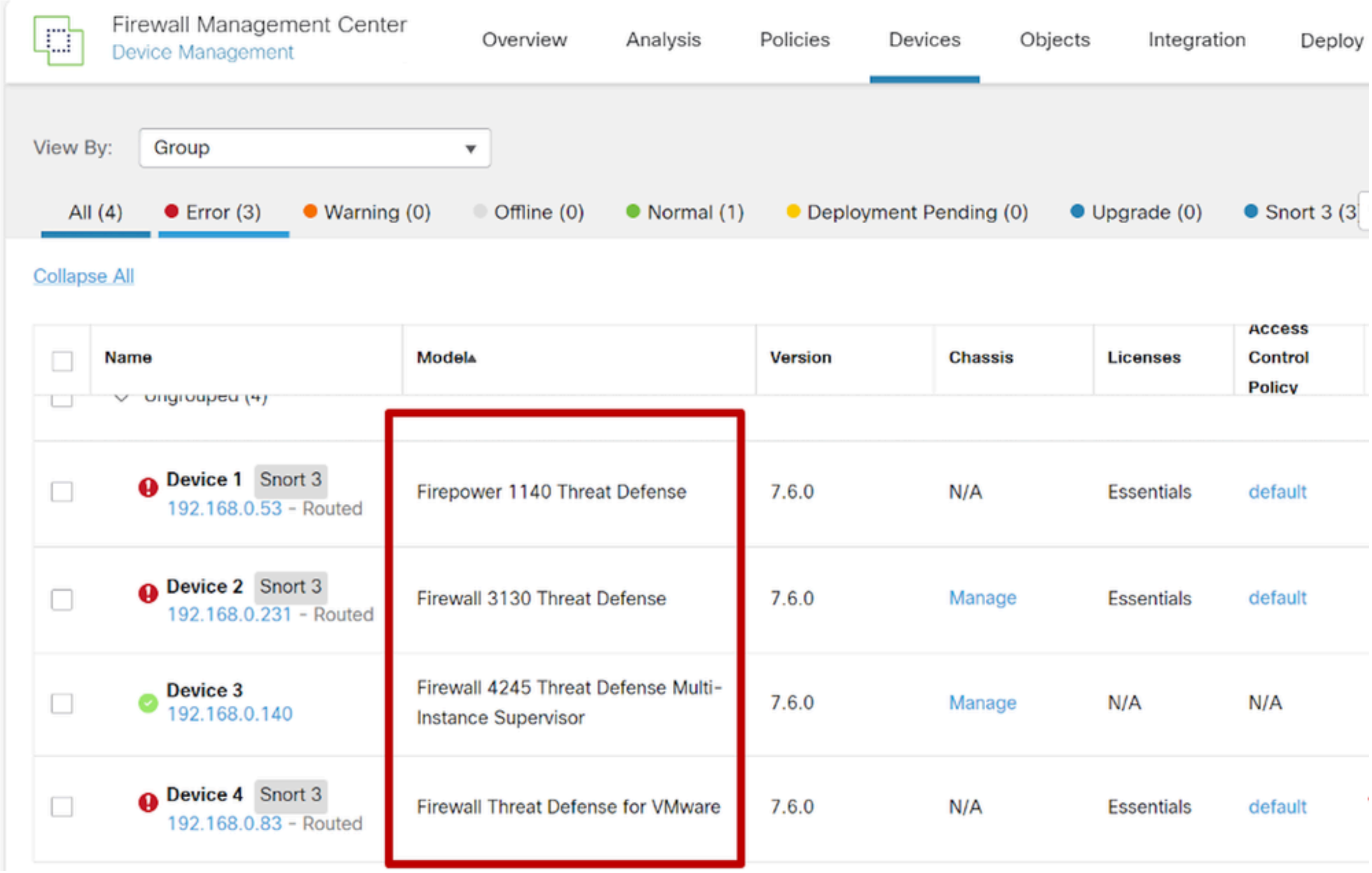


```
Copyright 2004-2024, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Firepower Extensible Operating System (FX-OS) v2.16.0 (build 239)
Cisco Secure Firewall Management Center for VMware v7.6.0 (build 12)

> show version
------------------[ firepower ]-------------------
Model                   : Cisco Secure Firewall Management Center for VMware (66)
Version 7.6.0 (Build 12)
UUID                    : c1f610d6-a0f7-11ee-9fc9-c65704d8547c
Rules update version      : 2024-02-07-001-vrt
LSP version              : lsp-rel-20240207-1539
VDB version               : 377
```

Device Management:

- Managed devices show shortened model names.
- Both Firepower (FPR1140 here) and Secure Firewall Devices (here, 3130, 4215, and FTD on

VMware) can appear together.

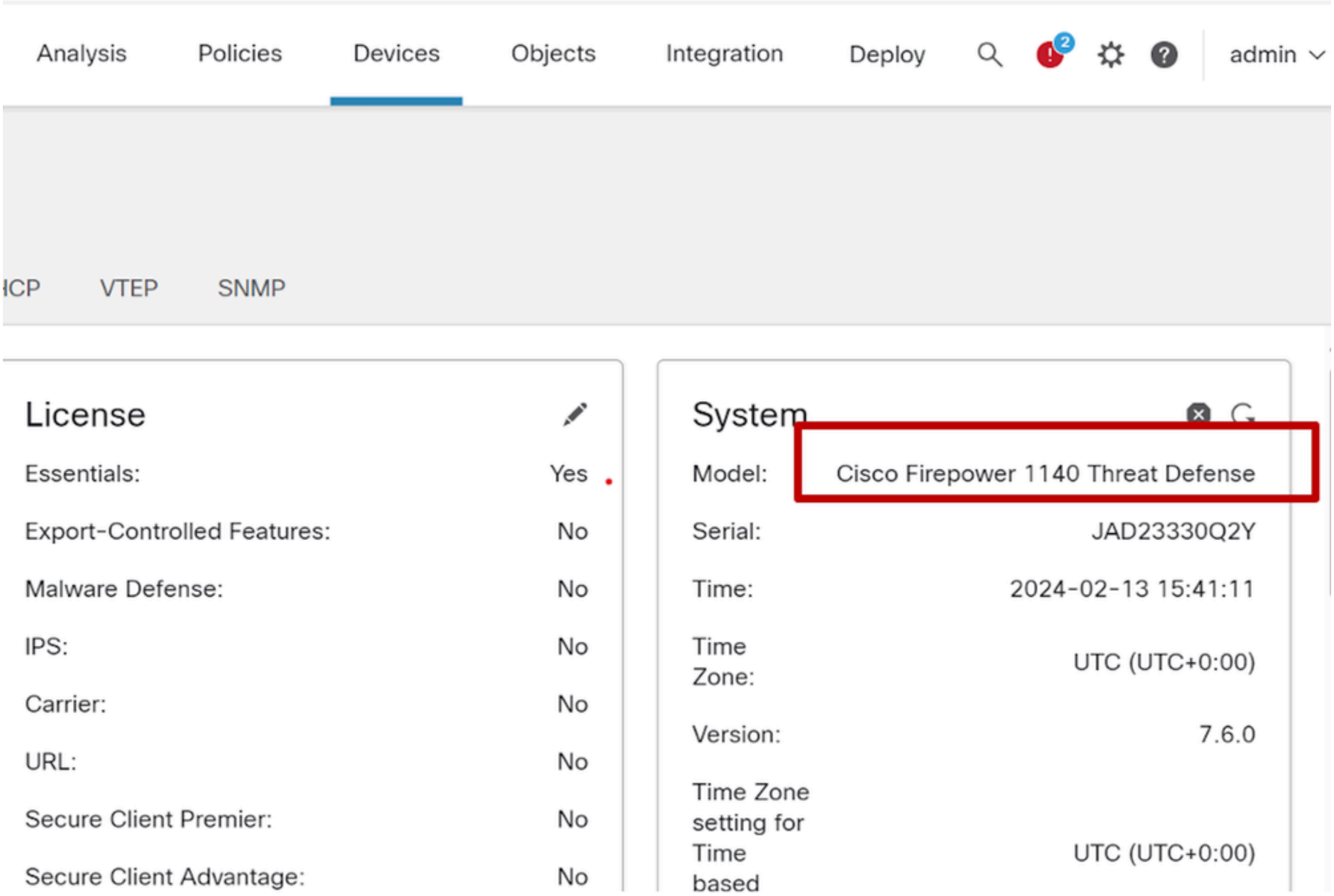


□	Name	Model	Version	Chassis	Licenses	Access Control Policy
□	Ungrouped (4)					
□	Device 1 Snort 3 192.168.0.53 - Routed	Firepower 1140 Threat Defense	7.6.0	N/A	Essentials	default
□	Device 2 Snort 3 192.168.0.231 - Routed	Firewall 3130 Threat Defense	7.6.0	Manage	Essentials	default
□	Device 3 192.168.0.140	Firewall 4245 Threat Defense Multi-Instance Supervisor	7.6.0	Manage	N/A	N/A
□	Device 4 Snort 3 192.168.0.83 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials	default

Firepower Devices Example

Summary status:

- Full model name is shown in device system info
- FP 11XX is shown as Firepower



License

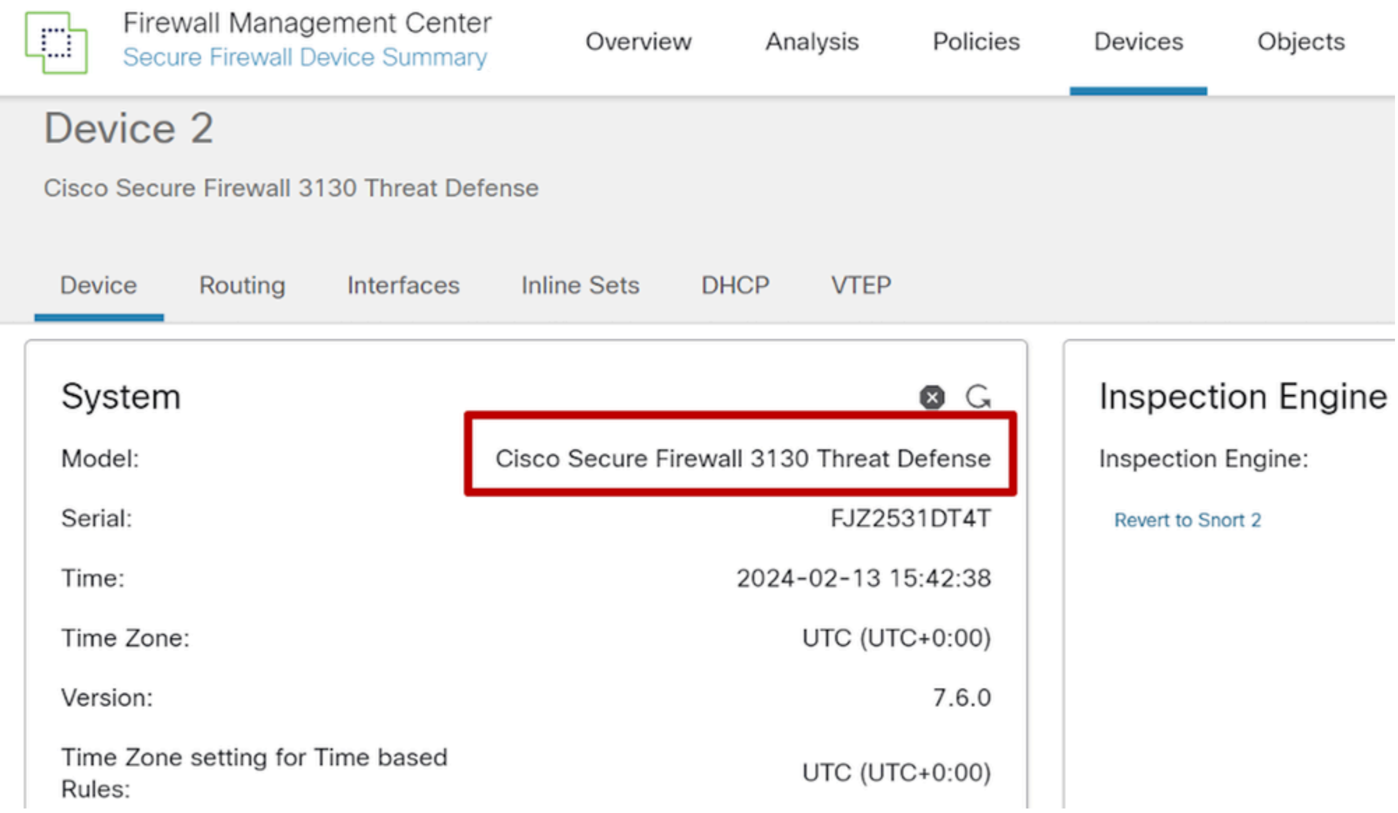
Essentials:	Yes
Export-Controlled Features:	No
Malware Defense:	No
IPS:	No
Carrier:	No
URL:	No
Secure Client Premier:	No
Secure Client Advantage:	No

System

Model:	Cisco Firepower 1140 Threat Defense
Serial:	JAD23330Q2Y
Time:	2024-02-13 15:41:11
Time Zone:	UTC (UTC+0:00)
Version:	7.6.0
Time Zone setting for Time based	UTC (UTC+0:00)

System Details for Secure Firewall Device:

- Full model name is shown in device system info.
- CSF31XX is shown as Cisco Secure Firewall.



Device 2

Cisco Secure Firewall 3130 Threat Defense

System

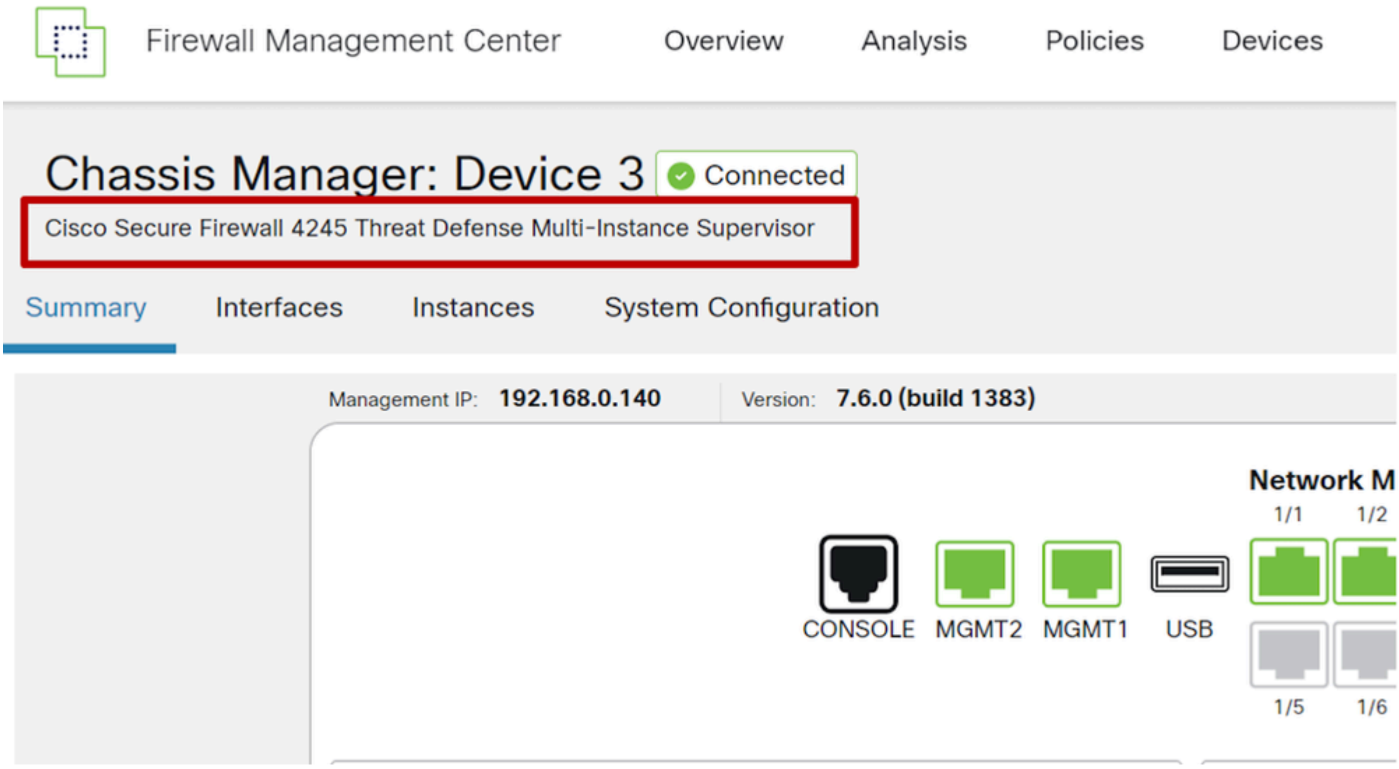
Model:	Cisco Secure Firewall 3130 Threat Defense
Serial:	FJZ2531DT4T
Time:	2024-02-13 15:42:38
Time Zone:	UTC (UTC+0:00)
Version:	7.6.0
Time Zone setting for Time based Rules:	UTC (UTC+0:00)

Inspection Engine

Inspection Engine:

Chassis Manager for 3100 / 4200 in Multi-Instance Mode:

- Full model name is shown in device system info.
- CSF42XX chassis is shown as Cisco Secure Firewall.



Firewall Management Center

Overview Analysis Policies Devices

Chassis Manager: Device 3 Connected

Cisco Secure Firewall 4245 Threat Defense Multi-Instance Supervisor

Summary Interfaces Instances System Configuration

Management IP: 192.168.0.140

Version: 7.6.0 (build 1383)

Firewall Threat Defense Configuration Defaults:

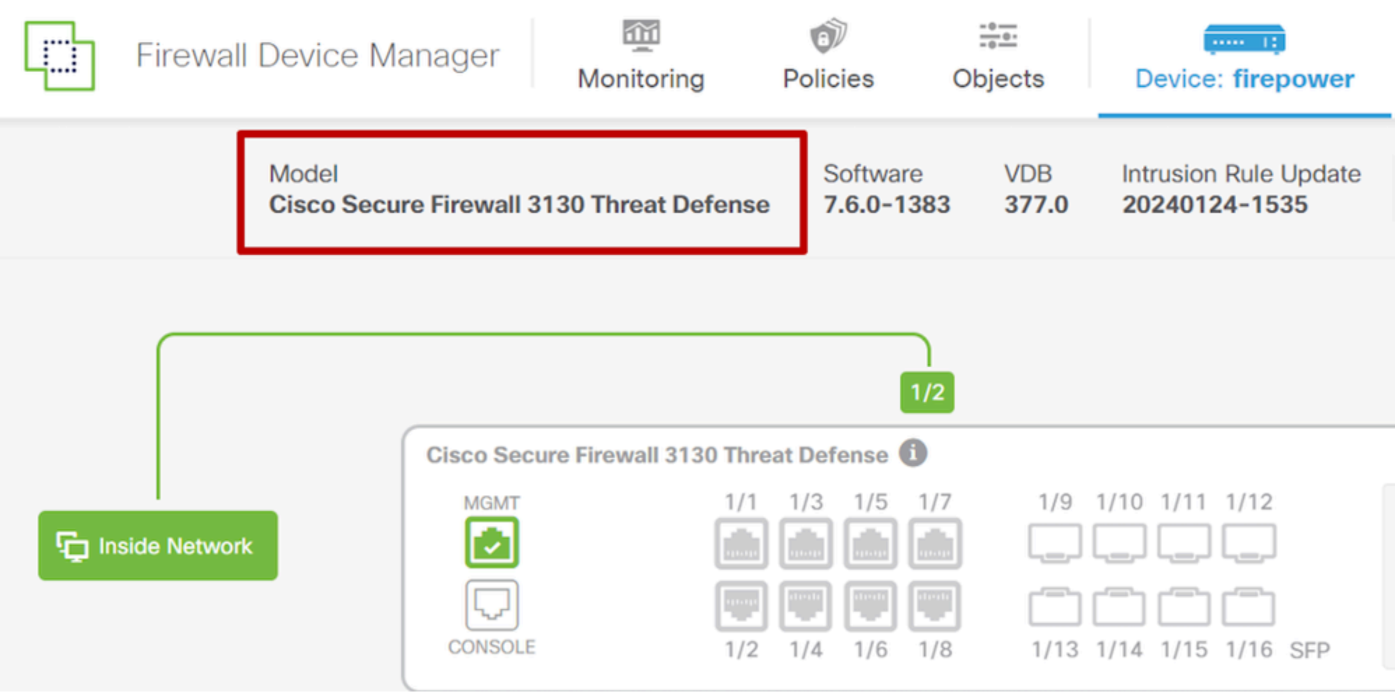
- System hostname default is still firepower,
- We kept firepower, because this does not directly reference the running platform.
- This can be easily changed by the user.

```
Do you want to configure IPv4? (y/n) [y]:

Do you want to configure IPv6? (y/n) [y]: n

Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:

Enter an IPv4 address for the management interface [192.168.0.190]: 192.168.0.231

Enter an IPv4 netmask for the management interface [255.255.255.0]:

Enter the IPv4 default gateway for the management interface [data-interfaces]: 192.168.0.254

Enter a fully qualified hostname for this system [firepower]:

Enter a comma-separated list of DNS servers or 'none' [x.x.x.x]:

Enter a comma-separated list of search domains or 'none' []:

If your networking information has changed, you need to reconnect.
```

Firewall Device Manager Examples

Summary Status:

- Main device page shows full model name with Secure Firewall branding.

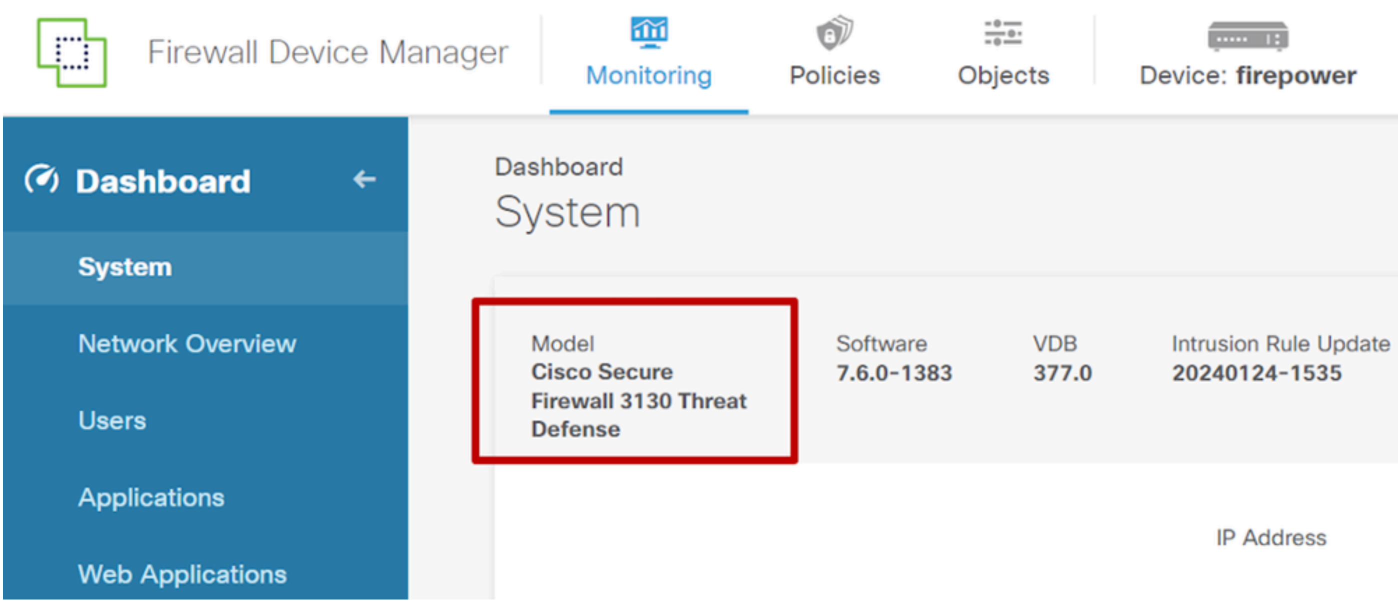


Model
Cisco Secure Firewall 3130 Threat Defense

Software
7.6.0-1383

VDB
377.0

Intrusion Rule Update
20240124-1535



Model
Cisco Secure Firewall 3130 Threat Defense

Software
7.6.0-1383

VDB
377.0

Intrusion Rule Update
20240124-1535

Firewall Threat Defense CLI Output:

- Full model name is shown with Secure Firewall naming.
- This is also shown on SSH logins.
- Other CLI output, such as show version, uses Secure Firewall instead of Firepower.

Manage the device locally? (yes/no) [yes]:

Configuring firewall mode to routed.

Update policy deployment information

  - add device configuration

Successfully performed firstboot initial configuration steps for Secure Firewall Device Manager for Secure Firewall Threat Defense.

```
> show version

-------------------[ firepower ]--------------------

Model                  : Cisco Secure Firewall 3130 Threat Defense (80) Version 7.6.0 (Build 13)

UUID                   : 123ab4d5-e6aa-11bb-ccc7-f888d99f000d

VDB version               : 377

----------------------------------------------------
```

Firewall Device Manager System Monitor:

- System monitoring dashboard also uses correct model name.