# **Verify Firepower Software Versions**

# Contents

Introduction **Prerequisites Requirements Components Used** Verify Software Versions **FMC Software Version FMC UI FMC CLI FMC REST-API FMC Troubleshoot file** FTD or Firepower Module CLI FTD or Firepower Module Troubleshoot file **FDM Software Version** FDM UI **FDM REST API FTD CLI FTD SNMP** FTD Troubleshot file **FXOS Software Version** FCM UI FXOS CLI **FXOS REST-API FXOS SNMP FXOS** Chassis show-tech file **FTD Software Version FTD CLI** FTD SNMP **FMC UI FMC REST API** FDM UI **FDM REST-API** FTD Troubleshoot file FCM UI **FXOS CLI FXOS REST-API** FXOS Chassis show-tech file **ASA Software Version ASA CLI ASA SNMP** ASA show-tech file

FCM UI **FXOS CLI FXOS REST-API FXOS** Chassis show-tech file Firepower Module Software Version **FMC UI FMC REST-API Firepower Module CLI Firepower Module Troubleshoot file** ASA CLI ASA show-tech file Verify Snort, VDB, and SRU Versions Deep Packet Inspection Engine (Snort) Version FMC UI **FMC REST-API** FDM UI **FDM REST API** FTD or Firepower CLI FTD or Firepower Module Troubleshoot file Vulnerability Database (VDB) Version FMC UI FMC CLI **FMC REST-API FMC Troubleshoot file** FDM UI **FDM REST API** FTD or Firepower Module CLI FTD or Firepower Module Troubleshoot file Intrusion rule Update Versions FMC UI FMC CLI **FMC REST-API FMC Troubleshoot file** FDM UI **FDM REST API** FTD or Firepower Module CLI FTD or Firepower Module Troubleshoot file Known Issues **Related Information** 

# Introduction

This document describes the verification of Firepower software versions.

# **Prerequisites**

## Requirements

Basic product knowledge, REST-API, SNMP.

## **Components Used**

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.

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

- Firepower 11xx
- Firepower 21xx
- Firepower 31xx
- Firepower 41xx
- Firepower Management Center (FMC) Version 7.1.x
- Firepower eXtensible Operating System (FXOS) 2.11.1.x
- Firepower Device Manager (FDM) 7.1.x
- Firepower Threat Defense 7.1.x
- ASA 9.17.x

# **Verify Software Versions**

## **FMC Software Version**

The FMC software version can be verified with the use of these options:

- FMC UI
- FMC CLI
- REST API request
- FMC troubleshoot file
- FTD or Firepower module CLI
- FTD or Firepower module troubleshoot file

## FMC UI

Follow these steps to verify the FMC software version on FMC UI:

1. Choose Help > About:

| Firepower Management Center<br>Overview / Dashboards / Management  | Overview         | Analysis           | Policies     | Devices | Objects | AMP | Intellige | nce   |                                      | Deploy                | ۹ (   | 🚰 🗘 🕜 admin 🔻   |
|--|------------------|--------------------|--------------|---------|---------|-----|-----------|---|--------------------------------------|-----------------------|---|---|
| Name           Access Controlled User Statistics<br>Provides traffic and intrusion event statistics by user           Application Statistics<br>Provides traffic and intrusion event statistics by application |                  |                    |              |         |         |     |           | Page-level Help<br>Iow-Tos<br>Documentation on<br>What's New in Thi<br>Software Downloa<br>Secure Firewall Yo | Cisco.com<br>s Release<br>d<br>uTube | s<br>F<br>7<br>2<br>2 | Secure Fire<br>Firepower M<br>Partner Eco<br>Ask a Ques<br>FAC Suppo<br>About | wall on Cisco.com<br>Algration Tool<br>system<br>tion<br>rt Cases |
| Application Statistics (7.1.0)<br>Provides application statistics  |                  |                    |              |         |         |     |           | admin   | No                                   | N                     | 0   | C < / 7   |
| Connection Summary<br>Provides tables and charts of the activity on your monitored no  | etwork segment o | rganized by differ | ent criteria |         |         |     |           | admin   | No                                   | N                     | 0   | C < / 7   |
| Detailed Dashboard<br>Provides a detailed view of activity on the appliance  |                  |                    |              |         |         |     |           | admin   | No                                   | N                     | 0   | C 9/1   |
| Detailed Dashboard (7.0.0)<br>Provides a detailed view of activity on the appliance  |                  |                    |              |         |         |     |           | admin   | No                                   | N                     | 0   | C 9/1   |
| Files Dashboard<br>Provides an overview of Malware and File Events   |                  |                    |              |         |         |     |           | admin   | No                                   | N                     | 0   | C 9/1   |
| Security Intelligence Statistics<br>Provides Security Intelligence statistics  |                  |                    |              |         |         |     |           | admin   | No                                   | N                     | 0   | C < / =   |
| Summary Dashboard<br>Provides a summary of activity on the appliance   |                  |                    |              |         |         |     |           | admin   | No                                   | Ye                    | 95  | Ľ < ∕ ∎   |

#### 2. Check Software Version:

## FMC CLI

Follow these steps to verify the FMC software version on FMC CLI.

1. Access FMC via SSH or console connection. The banner displays the software version:

Cisco Firepower Extensible Operating System (FX-OS) v2.11.0 (build 154) Cisco Secure Firewall Management Center 4600 v7.1.0 (build 90)

#### 2. Run the show version command on CLI:

| > show version           |  |  |  |  |  |  |  |
|--------------------------|--|--|--|--|--|--|--|
| [ FMC-4600-2.cisco.com ] |  |  |  |  |  |  |  |
| Model                    | : Cisco Firepower Management Center 4600 (66) Version 7.1.0 (Build 90) |  |  |  |  |  |  |
| UUID                     | : a10ed34e-d127-11e8-b440-728439d95305                                 |  |  |  |  |  |  |
| Rules update version     | : 2022-05-02-003-vrt   |  |  |  |  |  |  |
| LSP version              | : lsp-rel-20220502-1613  |  |  |  |  |  |  |
| VDB version              | : 354  |  |  |  |  |  |  |
|                          |  |  |  |  |  |  |  |

## **FMC REST-API**

Follow these steps to verify the FMC software version via an FMC REST-API request. Use a REST-API client to verify the software version. In this example, **curl** is used:

1. Request an authentication token:

```
# curl -s -k -v -X POST 'https://192.0.2.1/api/fmc_platform/v1/auth/generatetoken' -H
'Authentication: Basic' -u 'admin:Cisco123' | grep -i X-auth-access-token
<X-auth-access-token: 9408fe38-c25c-4472-b7e6-3571bb4e2b8d
  Use the X-auth-access-token in this query:
# curl -k -X GET 'https://192.0.2.1/api/fmc_platform/v1/info/serverversion' -H 'X-auth-access-
token: 9408fe38-c25c-4472-b7e6-3571bb4e2b8d' | python -m json.tool
{
 "links": {
  "self": "https://192.0.2.1/api/fmc_platform/v1/info/serverversion?offset=0&limit=25"
 },
 "items": [
  {
     "serverVersion": "7.1.0 (build 90)",
     "geoVersion": "2022-04-25-002",
     "vdbVersion": "build 354 ( 2022-04-27 19:39:56 )",
     "sruVersion": "2022-05-04-001-vrt",
     "lspVersion": "lsp-rel-20220504-1121",
     "type": "ServerVersion"
  }
 ],
 "paging": {
   "offset": 0,
  "limit": 25,
   "count": 1,
   "pages": 1
 }
```

**Note**: The part "| **python -m json.tool**" of the command string is used to format output in JSON-style and is optional.

#### **FMC Troubleshoot file**

Follow these steps to verify the FMC software version in the troubleshoot file:

- 1. Open the troubleshoot file and navigate to the folder <filename>.tar/results-<date>-xxxxxx/dir-archives/etc/sf/
- 2. Open the file **ims.conf** and find the lines with keys **SWVERSION** and **SWBUILD**:

```
# pwd
/var/tmp/results-05-06-2022--199172/dir-archives/etc/sf/
# cat ims.conf | grep -E "SWVERSION|SWBUILD"
SWVERSION=7.1.0
SWBUILD=90
```

## FTD or Firepower Module CLI

Follow these steps to verify the FMC software version on FTD CLI or the Firepower module CLI:

- 1. Access FTD via SSH or console connection. In the case of the Firepower module, access the module via SSH, or from the ASA CLI via the **session sfr** command.
- 2. Run the expert command.

> expert
admin@fpr2k-1:~\$

3. Run the **less /ngfw/var/sf/detection\_engines/<UUID>/ngfw.rules** command on FTD or **less /var/sf/detection\_engines/<UUID>/ngfw.rules** command on the Firepower module and check row **DC Version:** 

## FTD or Firepower Module Troubleshoot file

Follow these steps to verify the FMC software version in the FTD or the Firepower module troubleshoot file:

- Open the troubleshoot file and navigate to the folder <filename>-troubleshoot .tar/results-<date>--xxxxxx/file-contents/ngfw/var/sf/detection-engines/<UUID>/ if the file was generated on FTD. For the Firepower module, navigate to the folder <filename>troubleshoot .tar/results-<date>--xxxxxx/file-contents/var/sf/detectionengines/<UUID>/
- 2. Open the ngfw.rules file and check row DC Version:

```
# pwd
/var/tmp/results-05-06-2022--163203/file-contents/ngfw/var/sf/detection_engines/5e9fa23a-5429-
11ec-891e-b19e407404d5
# cat ngfw.rules
#### ngfw.rules
******
#
        : FTD-ACP-1652807562
# AC Name
# Policy Exported : Tue May 17 17:29:43 2022 (UTC)
# File Written : Tue May 17 17:31:10 2022 (UTC)
#
# DC Version : 7.1.0-90 OS: 90
           : 2022-05-11-001-vrt
# SRU
# VDB
           : 354
#
```

## **FDM Software Version**

The FDM software version can be verified with the use of these options:

- FDM UI
- FTD CLI
- FTD SNMP poll
- FTD troubleshoot file
- FDM REST API
- Firepower Chassis Manager (FCM) UI
- FXOS CLI
- FXOS REST API
- FXOS chassis show-tech file

## FDM UI

To verify the software version on FDM UI check **Software** on the main page:

| CISCO. Firepower Device Manager            | 题 ⑦ 註<br>Monitoring Policies Objects  | Device: KSEC-FPR2100  | admin · · · · · · · · · · · · · · · · · · ·              |
|--|---|---|--|
| Model<br>Cisco Firepower 2120 Thro         | Software VDB Intrusion Rule L<br>7.1.0-90 346.0 20211110-134  | Jpdate Cloud Services High Avail<br>8 😵 Not Registered   Register Not Config      | ability CONFIGURE  |
|  | 1/2   |   | d Internet   |
| F Inside Network                           | Cisco Firepower 2120 Threat Defense ①<br>MGMT 1/1 1/3 1/5 1/7 1/9 1/1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 | 1<br>1/13 1/14 1/15 1/16<br>2 SFP   | teway ONTP Server  |
|  | 171<br>   |   |  |
| Interfaces<br>Connected<br>Enabled 3 of 17 | Routing<br>There are no static routes yet   | Updates<br>Geolocation, Rule, VDB, System Upgrade,<br>Security Intelligence Feeds | System Settings<br>Management Access<br>Logging Settings |
| View All Interfaces                        | View Configuration  | View Configuration  | DHCP Server / Relay<br>DDNS Service<br>DNS Server        |

## **FDM REST API**

Follow these steps to verify the FDM software version via an FDM REST-API request. Use a REST-API client to verify the software version. In this example, curl is used:

1. Request an authentication token:

```
# curl -k -X POST --header 'Content-Type: application/json' --header 'Accept: application/json'
-d '{ "grant_type": "password", "username": "admin", "password": "Admin#1324" }'
'https://192.0.2.2/api/fdm/latest/fdm/token'
{
    "access_token":
    "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIyNDk5NTcsInN1YiI6ImFkbWluIiwianRpIjoiNDk3MmRjNjAtZDBmMi0xMW
VjLTk4ZWMtNDdlZTQwODkwMDVjIiwibmJmIjoxNjUyMjQ5OTU3LCJleHAiOjE2NTIyNTE3NTcsInJlZnJlc2hUb2tlbkV4cG
lyZXNBdCI6MTYIMjIIMjM1NzQ1NywidG9rZW5UeXBlIjoiSldUXOFjY2VzcyIsInVzZXJVdWlkIjoiYTU3ZGVmMjgtY2M3MC
0xMWVjLTk4ZWMtzjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJlc2
VybmFtZSI6ImFkbWluIn0.1JLmHddJ2jaVRmpdXF6qg48qdBcyRuit94DLobCJ9LI",
 "expires_in": 1800,
 "refresh_expires_in": 2400,
 "refresh_token":
 "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIzOTQxNjksInN1YiI6ImFkbWluIiwianRpIjoiMGU0NGIXYZQtZDI0Mi0xMW
```

```
VjLTk4ZWMtYTllOTlkZGMwN2Y0IiwibmJmIjoxNjUyMzk0MTY5LCJleHAiOjE2NTIZOTY1NjksImFjY2Vzc1Rva2VuRXhwaX
Jlc0F0IjoxNjUyMzk1OTY5MDcwLCJyZWZyZXNoQ291bnQiOi0xLCJ0b2tlblR5cGUiOiJKV1RfUmVmcmVzaCIsInVzZXJVdW
lkIjoiYTU3ZGVmMjgtY2M3MC0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXN1clJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2
luIjoicGFzc3dvcmQiLCJ1c2VybmFtZSI6ImFkbWluIn0.Avga0-isDjQB527d3QWZQb7AS4a9ea5wlbYUn-A9aPw",
"token_type": "Bearer"
```



2. Use the access token value in this query:

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIyNDk5NTcsInN1Yi16ImFkbWluIiwianRpIjoiNDk3MmRjNjAtZDBmMi0xMWV
jLTk4ZWMtNDdlZTQwODkwMDVjIiwibmJmIjoxNjUyMjQ5OTU3LCJleHAiOjE2NTIyNTE3NTcsInJlZnJlc2hUb2tlbkV4cGl
yZXNBdCI6MTY1MjI1MjM1NzQ1NywidG9rZW5UeXBlIjoiSldUX0FjY2VzcyIsInVzZXJVdWlkIjoiYTU3ZGVmMjgtY2M3MC0
xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJlc2V
ybmFtZSI6ImFkbWluIn0.lJLmHddJ2jaVRmpdXF6qg48qdBcyRuit94DLobCJ9LI'
'https://192.0.2.2/api/fdm/v6/operational/systeminfo/default' | grep -i software
"softwareVersion" : "7.1.0-90",
"softwareVersion" : "7.1.0-90",
```

## FTD CLI

Follow the steps in the section.

## **FTD SNMP**

Follow the steps in the section.

## **FTD Troubleshot file**

Follow the steps in the section.

## FCM UI

FCM is available on Firepower 4100 and Firepower 9300 Series. Follow the steps in the section.

## **FXOS CLI**

Follow the steps in the section.

## **FXOS REST-API**

Follow the steps in the section.

## **FXOS Chassis show-tech file**

Follow the steps in the section.

## **FXOS Software Version**

The FXOS software version can be verified with the use of these options:

- FCM UI (Firepower 4100/9300 only)
- FXOS CLI
- FXOS REST API

- FXOS SNMP poll
- FXOS chassis show-tech file.

## FCM UI

To verify the FXOS software version on FCM UI check Version on the main page:

| Overview Interface                   | s Logical Devices Security Modules Platform Settings  | System   | Tools | Help | admin | î |
|--------------------------------------|---|----------|-------|------|-------|---|
| KSEC-FPR9K-3-A<br>Model: Cisco Firep | 10.62.148.239     Operational State: Operable     Chassis Uptime  | 27:00:21 | :03   | () A | 0     |   |
|                                      | Network Module 1         Network Module 2         Network Module 3 : Empty           CONSOLE         1         2         3         4         5         6         7         8         Network Module 2         1         2         3         4 |          |       |      |       |   |
|                                      | 🗑 Security Module 1 - Up  |          |       |      |       |   |
|                                      | 🕼 Security Module 3 - Up 🔊 🖉 Power 1 - Running 🗇 🖗 Power 2 - Running  |          |       |      |       |   |

## **FXOS CLI**

#### Firepower 4100/9300

Follow these steps to verify the FXOS software version on FXOS CLI:

- 1. Establish a console or SSH connection to the chassis.
- 2. Switch to scope system and run the show firmware monitor command:

```
firepower # scope system
firepower /system # show firmware monitor
FPRM:
   Package-Vers: 2.11(1.154)
  Upgrade-Status: Ready
Fabric Interconnect A:
   Package-Vers: 2.11(1.154)
  Upgrade-Status: Ready
Chassis 1:
  Server 1:
       Package-Vers: 2.11(1.154)
      Upgrade-Status: Ready
  Server 2:
       Package-Vers: 2.11(1.154)
      Upgrade-Status: Ready
   Server 3:
       Package-Vers: 2.11(1.154)
       Upgrade-Status: Ready
```

## Firepower 1000/2100/3100 with FTD

Follow these steps to verify the FXOS software version on FXOS CLI:

1. Establish console connection to the chassis or SSH connection to FTD. In the case of the SSH connection to the FTD, run the **connect fxos** command on FTD CLISH:

#### > connect fxos

2. Switch to the scope system and run the show firmware detail command:

```
firepower # scope system
firepower /system # show firmware detail
Version: 7.1.0-90
Startup-Vers: 7.1.0-90
MANAGER:
  Boot Loader:
      Firmware-Vers: 1012.0200.0213
      Rommon-Vers: 1.0.12
      Fpga-Vers: 2.0.00
      Fpga-Golden-Vers:
       Power-Sequencer-Vers: 2.13
       Firmware-Status: OK
      SSD-Fw-Vers: 0147
   System:
      Running-Vers: 2.11(1.154)
      Platform-Vers: 2.11.1.154
      Package-Vers: 7.1.0-90
       Startup-Vers: 2.11(1.154)
  NPU:
       Running-Vers: 2.11(1.154)
       Platform-Vers: 2.11.1.154
      Package-Vers: 7.1.0-90
      Startup-Vers: 2.11(1.154)
   Service Manager:
      Running-Vers: 2.11(1.154)
       Platform-Vers: 2.11.1.154
       Package-Vers: 7.1.0-90
       Startup-Vers: 2.11(1.154)
```

#### Firepower 1000/3100 with ASA, Firepower 2100 with ASA in appliance mode

Follow these steps to verify the FXOS software version on FXOS CLI:

1. Establish console connection to the chassis or telnet/SSH connection to ASA. In the case of the telnet/SSH connection to ASA, run the **connect fxos** command on ASA CLI.

```
asa# connect fxos
```

2. Switch to the scope system and run the show firmware detail command:

```
firepower # scope system
firepower /system # show firmware detail
Version: 9.17.1
Startup-Vers: 9.17.1
MANAGER:
  Boot Loader:
      Firmware-Vers: 1012.0200.0213
      Rommon-Vers: 1.0.12
      Fpga-Vers: 2.0.00
      Fpga-Golden-Vers:
       Power-Sequencer-Vers: 2.13
      Firmware-Status: OK
       SSD-Fw-Vers: 0147
   System:
       Running-Vers: 2.11(1.154)
       Platform-Vers: 2.11.1.154
```

```
Package-Vers: 9.17.1
Startup-Vers: 2.11(1.154)
NPU:
Running-Vers: 2.11(1.154)
Platform-Vers: 2.11(1.154)
Package-Vers: 9.17.1
Startup-Vers: 2.11(1.154)
Service Manager:
Running-Vers: 2.11(1.154)
Platform-Vers: 2.11.1.154
Package-Vers: 9.17.1
Startup-Vers: 2.11(1.154)
```

#### Firepower 2100 with ASA in platform mode

Follow these steps to verify the FXOS software version on FXOS CLI:

1. Establish SSH or console connection to the chassis or telnet/SSH connection to ASA. In the case of the telnet/SSH connection to ASA, run the **connect fxos** command on ASA CLI.

asa# connect fxos2. Switch to the scope system and run the show firmware detail command:

```
firepower # scope system
firepower /system # show firmware detail
Version: 9.17.1
Startup-Vers: 9.17.1
MANAGER:
  Boot Loader:
      Firmware-Vers: 1012.0200.0213
      Rommon-Vers: 1.0.12
      Fpga-Vers: 2.0.00
      Fpga-Golden-Vers:
      Power-Sequencer-Vers: 2.13
      Firmware-Status: OK
      SSD-Fw-Vers: 0147
   System:
      Running-Vers: 2.11(1.154)
       Platform-Vers: 2.11.1.154
      Package-Vers: 9.17.1
      Startup-Vers: 2.11(1.154)
   NPU:
       Running-Vers: 2.11(1.154)
      Platform-Vers: 2.11.1.154
       Package-Vers: 9.17.1
      Startup-Vers: 2.11(1.154)
   Service Manager:
      Running-Vers: 2.11(1.154)
       Platform-Vers: 2.11.1.154
       Package-Vers: 9.17.1
       Startup-Vers: 2.11(1.154)
```

## **FXOS REST-API**

FXOS REST-API is supported on Firepower 4100/9300 Series.

#### Firepower 4100/9300

Follow these steps to verify the FXOS software version via an FXOS REST-API request. Use a

REST-API client to verify the software version. In this example, curl is used:

1. Request an authentication token:

```
# curl -k -X POST -H 'USERNAME: admin' -H 'PASSWORD: Cisco123' 'https://192.0.2.100/api/login'
{
    "refreshPeriod": "0",
    "token": "1206f6a3032e7bdbeac07cfdd9d5add5cdd948e4e5f4511535a959aed7e1e2f5"
}
2. Use the token in this query:
```

. .

#### **FXOS SNMP**

SNMP configuration on FXOS is supported on Firepower 2100 with ASA in platform mode and Firepower 4100/9300.

#### Firepower 4100/9300

Follow these steps to verify the FXOS software version via SNMP:

- Ensure that SNMP is configured on FXOS. Refer to <u>Configure SNMP on Firepower NGFW</u> <u>Appliances</u> for configuration steps.
- 2. Poll .1.3.6.1.4.1.9.9.826.1.30.47.1.6 or CISCO-FIREPOWER-FIRMWARE-MIB:: cfprFirmwareRunningPackageVersion:

```
# snmpwalk -On -v2c -c cisco 192.0.2.100 .1.3.6.1.4.1.9.9.826.1.30.47.1.6
.1.3.6.1.4.1.9.9.826.1.30.47.1.6.20823 = STRING: "2.11(1.154)"
.1.3.6.1.4.1.9.9.826.1.30.47.1.6.25326 = ""
.1.3.6.1.4.1.9.9.826.1.30.47.1.6.25331 = STRING: "2.11(1.154)"
.1.3.6.1.4.1.9.9.826.1.30.47.1.6.30266 = STRING: "1.0.18"
.1.3.6.1.4.1.9.9.826.1.30.47.1.6.30269 = STRING: "1.0.18"
.1.3.6.1.4.1.9.9.826.1.30.47.1.6.30779 = ""
.1.3.6.1.4.1.9.9.826.1.30.47.1.6.30780 = STRING: "2.11(1.154)"
.1.3.6.1.4.1.9.9.826.1.30.47.1.6.30781 = STRING: "2.11(1.154)"
.1.3.6.1.4.1.9.9.826.1.30.47.1.6.30781 = STRING: "2.11(1.154)"
.1.3.6.1.4.1.9.9.826.1.30.47.1.6.32615 = STRING: "2.11(1.154)"
.1.3.6.1.4.1.9.9.826.1.30.47.1.6.48820 = STRING: "0.0"
```

#### Firepower 2100 with ASA in platform mode

Follow these steps to verify the FXOS software version via SNMP:

- Ensure that SNMP is configured on FXOS. Refer to <u>Configure SNMP on Firepower NGFW</u> <u>Appliances</u> for configuration steps.
- 2. Poll .1.3.6.1.2.1.1.1.0 or SNMPv2-MIB::sysDescr.0:

```
# snmpwalk -On -v2c -c cisco 192.0.2.101 .1.3.6.1.2.1.1.1.0
.1.3.6.1.2.1.1.1.0 = STRING: Cisco FirePOWER FPR-2140 Security Appliance, System Version
2.11(1.146)
```

#### **FXOS Chassis show-tech file**

#### Firepower 4100/9300

Follow these steps to verify the FXOS software version in the FXOS chassis show-tech file:

1. For FXOS versions 2.7 and later, open file sam\_techsupportinfo in <name>\_BC1\_all.tar/ FPRM\_A\_TechSupport.tar.gz/FPRM\_A\_TechSupport.tar

For earlier versions, open file **sam\_techsupportinfo** in **FPRM\_A\_TechSupport.tar.gz/ FPRM\_A\_TechSupport.tar.** 

2. Check the output of the `show firmware monitor` command:

```
# pwd
/var/tmp/20220313201802_F241-01-11-FPR-2_BC1_all/FPRM_A_TechSupport/
# cat sam_techsupportinfo
. . .
`show firmware monitor`
FPRM:
   Package-Vers: 2.11(1.154)
  Upgrade-Status: Ready
Fabric Interconnect A:
   Package-Vers: 2.11(1.154)
  Upgrade-Status: Ready
Chassis 1:
   Server 1:
      Package-Vers: 2.11(1.154)
      Upgrade-Status: Ready
   Server 2:
      Package-Vers: 2.11(1.154)
      Upgrade-Status: Ready
   Server 3:
      Package-Vers: 2.11(1.154)
      Upgrade-Status: Ready
```

## Firepower 1000/2100/3100

- 1. Open file tech\_support\_brief in <name>\_FPRM.tar.gz/<name>\_FPRM.tar
- 2. Check the output of the `show firmware detail` command:

```
# pwd
/var/tmp/fp2k-1_FPRM/
# cat tech_support_brief
...
`show firmware detail`
    Version: 7.1.0-90
    Startup-Vers: 7.1.0-90
MANAGER:
    Boot Loader:
```

```
Firmware-Vers: 1012.0200.0213
    Rommon-Vers: 1.0.12
    Fpga-Vers: 2.0.00
    Fpga-Golden-Vers:
    Power-Sequencer-Vers: 2.13
   Firmware-Status: OK
   SSD-Fw-Vers: 0147
System:
    Running-Vers: 2.11(1.154)
    Platform-Vers: 2.11.1.154
    Package-Vers: 7.1.0-90
   Startup-Vers: 2.11(1.154)
NPU:
    Running-Vers: 2.11(1.154)
    Platform-Vers: 2.11.1.154
    Package-Vers: 7.1.0-90
   Startup-Vers: 2.11(1.154)
Service Manager:
   Running-Vers: 2.11(1.154)
    Platform-Vers: 2.11.1.154
   Package-Vers: 7.1.0-90
    Startup-Vers: 2.11(1.154)
```

## **FTD Software Version**

The FTD software version can be verified with the use of these options:

- FTD CLI
- FTD SNMP poll
- FTD troubleshoot file
- FMC UI
- FMC REST API
- FDM UI
- FDM REST API
- FCM UI
- FXOS CLI
- FXOS REST API
- FXOS Chassis show-tech file

## FTD CLI

Follow these steps to verify the FTD software version on FTD CLI:

- 1. Use these options to access the FTD CLI in accordance with the platform and deployment mode:
- Direct SSH access to FTD all platforms
- Access from the FXOS console CLI (Firepower 1000/2100/3100) via command connect ftd
- Access from the FXOS CLI via commands (Firepower 4100/9300):
   connect module <x> [console|telnet], where x is the slot ID, and then

connect ftd [instance], where the instance is relevant only for multi-instance deployment.

• For virtual FTDs, direct SSH access to FTD, or console access from the hypervisor or cloud

UI

2. Run the **show version** command on CLI:

| firepower ]   |
|---|
| : Cisco Firepower 2120 Threat Defense (77) Version 7.1.0 (Build 90) |
| : 1b324aaa-670e-11ec-ac2b-e000f0bd3ca1                              |
| : lsp-rel-20220328-1342   |
| : 353   |
|   |

#### FTD SNMP

Follow these steps to verify the FTD software version via SNMP:

- Ensure that SNMP is configured and enabled. For FDM-managed FTD, refer to <u>Configure</u> and troubleshoot SNMP on Firepower FDM for configuration steps. For FMC-managed FTD, refer to <u>Configure SNMP on Firepower NGFW Appliances</u> for configuration steps.
- 2. Poll OID SNMPv2-MIB::sysDescr.0 or OID .1.3.6.1.2.1.1.1.0.:

```
# snmpwalk -v2c -c cisco123 192.0.2.2 SNMPv2-MIB::sysDescr.0
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Firepower Threat Defense, Version 7.1.0 (Build 90), ASA
Version 9.17(1)
```

```
# snmpwalk -v2c -c cisco123 192.0.2.2 SNMPv2-MIB::sysDescr.0 .1.3.6.1.2.1.1.1.0
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Firepower Threat Defense, Version 7.1.0 (Build 90), ASA
Version 9.17(1)
```

#### FMC UI

Follow these steps to verify the FTD software version on FMC UI:



1. Choose Devices > Device Management:

2. Check the Version column:

| altali<br>cisco | , Fire         | epower Management Center<br>ices / Device Management       | verview Analysis        | Policies | Devices O      | bjects                      | AMP                   |                          | Deploy  | ୦ 🊱                  | 🕜 admin 🕇    | , |
|-----------------|----------------|--|-------------------------|----------|----------------|-----------------------------|-----------------------|--------------------------|---------|----------------------|--------------|---|
| View E<br>All   | By: [1<br>(14) | Domain v<br>• Error (2) • Warning (0) • Offline            | (12) • Normal (0)       | Deployme | nt Pending (7) | <ul> <li>Upgrade</li> </ul> | e (0) • Snort 3 (12)  |                          | Q, Sear | Deployn<br>ch Device | nent History |   |
| Collaps         | se All         |  |                         |          |                |                             |                       |                          |         |                      |              |   |
|                 | Name           | 0  | Model                   | Version  | Chassis        |                             | Licenses              | Access Control<br>Policy | Group   |                      |              |   |
|                 | $\sim$         | LAB-FPR2K<br>High Availability                             |                         |          |                |                             |                       |                          |         |                      | <b>/:</b>    |   |
|                 |                | fpr2k-1(Primary, Active) Snort 3<br>192.0.2.140 - Routed   | Firepower 2110 with FTD | 7.1.0    | N/A            | E                           | Base, Threat (2 more) | LAB-FPR2K-ACL            |         |                      | :            |   |
|                 |                | ftp2k-2(Secondary,Standby) Snort 3<br>192.0.2.149 - Routed | Firepower 2110 with FTD | 7.1.0    | N/A            | E                           | 3ase, Threat (2 more) | LAB-FPR2K-ACL            |         |                      | :            |   |

## **FMC REST API**

Follow these steps to verify the FTD software version via FMC REST-API. Use a REST-API client to verify the software version. In this example, **curl** is used:

1. Request an authentication token:

```
# curl -s -k -v -X POST 'https://192.0.2.1/api/fmc_platform/v1/auth/generatetoken' -H
'Authentication: Basic' -u 'admin:Cisco123' | grep -i X-auth-access-token
<X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb</pre>
```

2. Identify the domain that contains the device. In the majority of the REST API queries the **domain** parameter is mandatory. Use the **X-auth-access-token in** this query to retrieve the list of domains:

```
# curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_platform/v1/info/domain' -H 'accept:
application/json' -H 'X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m
json.tool
{
    "items": [
        {
            "name": "Global",
            "type": "Domain",
            "uuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f"
        },
        {
            "name": "Global/domain1",
            "type": "Domain",
            "uuid": "ef0cf3e9-bb07-8f66-5c4e-00000000001"
        },
        {
            "name": "Global/domain2",
            "type": "Domain",
            "uuid": "341a8f03-f831-c364-b751-00000000001"
        }
    ],
    "links": {
        "self": "https://192.0.2.1/api/fmc_platform/v1/info/domain?offset=0&limit=25"
    },
    "paging": {
        "count": 3,
        "limit": 25,
        "offset": 0,
        "pages": 1
```

}

}

#### 3. Use the domain UUID to query for the devicerecords:

```
# curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-
0000000001/devices/devicerecords' -H 'accept: application/json' -H 'X-auth-access-token:
5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m json.tool
{
    "items": [
        {
            "id": "a4752f3c-86cc-11e9-8c9a-a3c958bed664",
            "links": {
                "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-
0000000001/devices/devicerecords/a4752f3c-86cc-11e9-8c9a-a3c958bed664"
            },
            "name": "fw1.lab.local",
            "type": "Device"
        },
        {
            "id": "05e9799c-94fc-11ea-ad33-a0032ddb0251",
            "links": {
                "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-
0000000001/devices/devicerecords/05e9799c-94fc-11ea-ad33-a0032ddb0251"
            },
            "name": "fw2.lab.local",
            "type": "Device"
        },
        {
            "id": "c8bef462-49f7-11e8-b2fb-ad9838c6ed90",
            "links": {
                "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-
0000000001/devices/devicerecords/c8bef462-49f7-11e8-b2fb-ad9838c6ed90"
            },
            "name": "fw3.lab.local",
            "type": "Device"
        },
        {
            "id": "3c41913a-b27b-11eb-b131-d2e2ce2a368d",
            "links": {
                "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-
0000000001/devices/devicerecords/3c41913a-b27b-11eb-b131-d2e2ce2a368d"
            },
            "name": "fw4.lab.local",
            "type": "Device"
        },
        {
            "id": "48f7f37c-8cf0-11e9-bf41-fb2d7b740db7",
            "links": {
                "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-
0000000001/devices/devicerecords/48f7f37c-8cf0-11e9-bf41-fb2d7b740db7"
            },
            "name": "fw5.lab.local",
            "type": "Device"
        },
        ſ
            "id": "0b1a9c94-8ba8-11ec-b2fd-93263934908d",
            "links": {
                "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-
0000000001/devices/devicerecords/0b1a9c94-8ba8-11ec-b2fd-93263934908d"
            },
```

```
"name": "fpr2k-1",
    "type": "Device"
},
```

4. Use the domain UUID and the device/container UUID:

```
# curl -s -k -X GET 'https://192.0.2.1/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-
6d9ed49b625f/devices/devicerecords/0b1a9c94-8ba8-11ec-b2fd-
93263934908d/operational/commands?offset=0&limit=25&command=show%20version' -H 'X-auth-access-
token: f3233164-6ab8-4e33-90cc-2612c19571be' | python -m json.tool
{
    "items": [
       {
           "commandInput": "show version",
           "commandOutput": "-----\nModel
: Cisco Firepower 2110 Threat Defense (77) Version 7.1.0 (Build 90) \nUUID
                                                                                           :
                                                             : lsp-rel-20220502-1613\nVDB
0b1a9c94-8ba8-11ec-b2fd-93263934908d\nLSP version
                                                            -----\n\nCisco
                     : 353\n-----
version
Adaptive Security Appliance Software Version 9.17(1) \nSSP Operating System Version
2.11(1.154)\n\nCompiled on Tue 30-Nov-21 19:37 GMT by builders\nSystem image file is
\"disk0:/mnt/boot/installables/switch/fxos-k8-fp2k-npu.2.11.1.154.SPA\"\nConfig file at boot was
\"startup-config\"\n\nfpr2k-1 up 10 days 4 hours\nfailover cluster up 57 days 17 hours\nStart-up
time 37 secs\n\nHardware: FPR-2110, 6588 MB RAM, CPU MIPS 1200 MHz, 1 CPU (6 cores)\n\n\n 1:
                      : address is 000f.b748.4801, irq 0\n 3: Ext: Management1/1
Int: Internal-Data0/1
address is 707d.b9e2.836d, irg 0\n 4: Int: Internal-Data1/1 : address is 0000.0100.0001, irg
0\n 5: Int: Internal-Data1/2 : address is 0000.0300.0001, irq 0\n 6: Int: Internal-Control1/1
: address is 0000.0001.0001, irq 0\n\nSerial Number: JAD213508B6\nConfiguration last modified by
enable_1 at 04:12:18.743 UTC Wed May 4 2022\n",
           "type": "command"
       }
   ],
    "links": {
       "self": "https://192.0.2.1/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-
6d9ed49b625f/devices/devicerecords/0b1a9c94-8ba8-11ec-b2fd-
93263934908d/operational/commands?offset=0&limit=25&command=show version"
   },
    "paging": {
       "count": 1,
       "limit": 25,
       "offset": 0,
       "pages": 1
    }
```

## FDM UI

Follow the steps in the section.

## **FDM REST-API**

Follow the steps in the section.

## **FTD Troubleshoot file**

Follow these steps to verify the FTD software version in the FTD troubleshoot file:

- 1. Open the troubleshoot file and navigate to the folder **<filename>-troubleshoot .tar/results-<date>--xxxxxx/command-outputs/**
- 2. Open the file usr-local-sf-bin-sfcli.pl show version.output and find the line with Model:

| <pre># pwd /var/tmp/results-05-06-202 # cat "usr-local-sf-bin-sf</pre> | 2199172/dir-archives/et   | cc/sf/<br>it"  |           |             |         |
|--|---------------------------|----------------|-----------|-------------|---------|
| [ fpr2   | k-1 ]                     | Model : Cisco  | Firepower | 2110 Threat | Defense |
| UUID   | : 0b1a9c94-8ba8-11ec-b2fd | l-93263934908d |           |             |         |
| LSP version  | : lsp-rel-20220510-1044   |                |           |             |         |
| VDB version  | : 354                     |                |           |             |         |

## FCM UI

For FTD on Firepower 4100/9300 use the FCM and check the **Version** in the **Logical Devices** tab:

| Overview Interfaces      | Logical Devices     | Security Modules | Platform Settings  |                                       |                 |  |              | System Tools Help admin         |
|--------------------------|---------------------|------------------|--------------------|---------------------------------------|-----------------|--|--------------|---------------------------------|
| Logical Device List      |                     |                  |                    |                                       |                 |  |              | ^                               |
|                          |                     |                  |                    |                                       |                 |  |              |                                 |
| Group By Consulty Module |                     |                  |                    |                                       |                 |  |              |                                 |
| Security Module          | *                   |                  |                    |                                       |                 |  |              |                                 |
| Security Module 1 (1 M   | Native instance)    |                  |                    |                                       |                 |  |              | 0% (0 of 78) Cores Available    |
| ASA                      |                     | Standalone       | Status:ok          |                                       |                 |  |              |                                 |
|                          |                     |                  |                    |                                       |                 |  |              |                                 |
| Application              | Version             | Resource         | Profile            | Management IP                         | Gateway         | Management Port                            | Status       |                                 |
| <sup>BI</sup> ASA        | 9.16.2.7            |                  |                    | 10.62.148.240                         | 10.62.148.129   | Ethernet1/1                                | Online       | 🚾 ) 🎋 C 🕍 🤌                     |
|                          |                     |                  |                    |                                       |                 |  |              |                                 |
| Security Module 2 (0 i   | nstances)           |                  |                    |                                       |                 |  |              | 1000 (04 of 04) Cores Available |
|                          |                     |                  |                    |                                       |                 |  |              | 100% (94 0194) Cores Avanable   |
|                          |                     |                  | No logical devices | on this security module.              |                 |  |              |                                 |
|                          |                     |                  | _                  | · · · · · · · · · · · · · · · · · · · |                 |  |              |                                 |
|                          |                     |                  |                    |                                       |                 |  |              |                                 |
|                          |                     |                  |                    |                                       |                 |  |              |                                 |
| Security Module 3 (1 0   | Container Instance) |                  |                    |                                       |                 |  |              | 0% (0 of 110) Cores Available   |
| FTD-MI-1                 |                     | Standalone       | Status:ok          |                                       |                 |  |              | 2 I                             |
| Application              | Version             | Resource         | Profile            | Management IP                         | Gateway         | Management Port                            | Status       |                                 |
| B FTD                    | 7.1.0.90            | RP110            |                    | 10.62.148.242                         | 10.62.148.129   | Ethernet1/1                                | Online       | 🚾 🎋 c 🔬 🖈                       |
| Interface Nam            | ve                  |                  | т                  | уре                                   | Attributes      |  |              |                                 |
| Ethernet1/               | 6                   |                  | d                  | lata                                  | Cluster Operat  | ional Status : not-applicable              |              |                                 |
| Ethernet1/               | 7                   |                  | d                  | ata                                   | MGMT-URL        | : https://10.62.148.249/                   |              |                                 |
| Port-chann               | el1                 |                  | d                  | ata                                   | HA-ROLE<br>UUID | : standalone<br>: 3050cf4c-c0aa-11ec-9b2a- | 8491ab8d0cc8 |                                 |
| E                        |                     |                  |                    |                                       |                 |  |              |                                 |

## **FXOS CLI**

#### FTD on Firepower 4100/9300

Follow these steps to verify the FTD software version on FXOS CLI:

- 1. Establish a console or SSH connection to the chassis.
- 2. Switch to the scope ssa and run the show app-instance command:

| firepow  | er# <b>scope s</b> | sa          |                 |               |                 |                   |
|----------|--------------------|-------------|-----------------|---------------|-----------------|-------------------|
| firepow  | er /ssa <b># s</b> | show app-in | stance          |               |                 |                   |
| App Name | e Identif          | ier Slot I  | D Admin Stat    | te Oper State | Running Versior | n Startup Version |
| Deploy ' | Type Turbo         | Mode Profi  | le Name Cluster | r State Clu   | ster Role       |                   |
|          |                    |             |                 |               |                 |                   |
| asa      | <br>ASA            | <br>1       | Enabled         | Online        | 9 16 2 7        | 9 16 2 7          |
| usu      | ASA                | 1           | LIADIEU         | OUTTILE       | J. 10. 2. 1     | J. I.O. Z /       |

| Native    | No       | Not Applicable None |         |               |          |          |  |  |
|-----------|----------|---------------------|---------|---------------|----------|----------|--|--|
| ftđ       | FTD-MI-1 | 3                   | Enabled | Online        | 7.1.0.90 | 7.1.0.90 |  |  |
| Container | No       | RP110               | Not App | olicable None |          |          |  |  |

#### FTD on Firepower 1000/2100/3100

Follow these steps to verify the FTD software version on FXOS CLI:

1. Establish a console connection to the chassis or SSH connection to the FTD In the case of the SSH connection to the FTD, run the **connect fxos** command on FTD CLISH:

> connect fxos

2. Switch to the scope ssa and run the show app-instance command:

firepower# scope ssa
firepower /ssa # show app-instance

| Application Na | ame      | Slot ID   | Admin State      | Operat | ional State  | Running  | Version | Startup  |   |
|----------------|----------|-----------|------------------|--------|--------------|----------|---------|----------|---|
| Version Deploy | у Туре Р | rofile Na | ame Cluster Oper | State  | Cluster Role |          |         |          |   |
|                |          |           |                  |        |              |          |         |          | • |
| ftd            |          | 1         | Enabled          | Online | 2            | 7.1.0.90 | )       | 7.1.0.90 |   |
| Native         |          | Not A     | Applicable       | None   |              |          |         |          |   |

#### **FXOS REST-API**

Follow these steps to verify the FTD software version via an FXOS REST-API:

1. Request an authentication token:

```
# curl -s -k -X POST -H 'USERNAME: admin' -H 'PASSWORD: cisco' 'https://192.0.2.100/api/login'
{
    "refreshPeriod": "0",
    "token": "28821660bc74e418f3fadc443619df0387d69e7b150e035f688bed9d347b4838"
}
```

2. Use the token in this query and ensure to specify the slot ID where the FTD is installed:

## **FXOS Chassis show-tech file**

Follow these steps to verify the FTD software version in the FXOS chassis show-tech file:

#### FTD on Firepower 4100/9300

1. For FXOS versions 2.7 and later, open file **sam\_techsupportinfo** in **<name>\_BC1\_all.tar/ FPRM\_A\_TechSupport.tar.gz/FPRM\_A\_TechSupport.tar** 

For earlier versions, open file **sam\_techsupportinfo** in **FPRM\_A\_TechSupport.tar.gz/ FPRM\_A\_TechSupport.tar.** 

2. Check the section for each slot under the `show slot expand detail`:

```
# pwd
/var/tmp/20220313201802_F241-01-11-FPR-2_BC1_all/FPRM_A_TechSupport/
# cat sam_techsupportinfo
...
`show slot expand detail`
Slot: Slot ID: 3 Log Level: Info Admin State: Ok Oper State: Online Disk Format State: Ok Disk
Format Status: 100% Clear Log Data: Available Error Msg: Application Instance: App Name: ftd
Identifier: FTD-MI-1
Admin State: Enabled
Oper State: Online
Running Version: 7.1.0.90
Startup Version: 7.1.0.90
Deploy Type: Container
```

```
. . .
```

FTD on Firepower 1000/2100/3100

- 1. Open file tech\_support\_brief in <name>\_FPRM.tar.gz/<name>\_FPRM.tar
- 2. Check the sections `scope ssa` and `show slot `:

```
# pwd
/var/tmp/fp2k-1_FPRM/
# cat tech_support_brief
. . .
`scope ssa` `show slot`
Slot:
   Slot ID Log Level Admin State Operational State
       ----- ------
           Info Ok
                            Online
   1
`show app`
Application:
          Version Description Author
  Name
                                    Deploy Type CSP Type Is Default App
   _____ _____
  ftd
           7.1.0.90 N/A cisco
                                    Native
                                              Application Yes
`show app-instance detail`
  Application Name: ftd
  Slot ID: 1
  Admin State: Enabled
  Operational State: Online
  Running Version: 7.1.0.90
   Startup Version: 7.1.0.90
```

## **ASA Software Version**

The ASA software version can be verified with the use of these options:

- ASA CLI
- ASA SNMP poll
- ASA show-tech file
- FCM UI
- FXOS CLI
- FXOS REST API
- FXOS chassis show-tech file

## ASA CLI

Follow these steps to verify the ASA software version on ASA CLI:

1. Use these options to access the ASA CLI in accordance with the platform and deployment mode:

- Direct telnet/SSH access to ASA on Firepower 1000/3100 and Firepower 2100 in appliance mode
- Access from FXOS console CLI on Firepower 2100 in platform mode and connect to ASA via
   the connect asa command
- Access from FXOS CLI via commands (Firepower 4100/9300):

## connect module <x> [console|telnet], where x is the slot ID, and then connect asa

- For virtual ASA, direct SSH access to ASA, or console access from the hypervisor or cloud UI
- 2. Run the show version command:

```
ciscoasa# show version
Cisco Adaptive Security Appliance Software Version 9.17(1)
SSP Operating System Version 2.11(1.154)
Device Manager Version 7.17(1)
Compiled on Tue 30-Nov-21 19:37 GMT by builders
System image file is "disk0:/mnt/boot/installables/switch/fxos-k8-fp2k-npu.2.11.1.154.SPA"
Config file at boot was "startup-config"
ciscoasa up 4 hours 40 mins
```

ciscoasa up 4 hours 40 min: Start-up time 1 sec

## ASA SNMP

Follow these steps to verify the ASA software version via SNMP:

- 1. Ensure that SNMP is configured and enabled.
- 2. Use SNMP client to poll OID SNMPv2-MIB::sysDescr.0 or OID .1.3.6.1.2.1.1.1.0:

```
# snmpwalk -v2c -c cisco123 192.0.2.2 SNMPv2-MIB::sysDescr.0
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Adaptive Security Appliance Version 9.17(1)
```

# snmpwalk -v2c -c cisco123 192.0.2.2 SNMPv2-MIB::sysDescr.0 .1.3.6.1.2.1.1.1.0
SNMPv2-MIB::sysDescr.0 = Cisco Adaptive Security Appliance Version 9.17(1)

## ASA show-tech file

Search for the line with the Cisco Adaptive Security Appliance Software Version string:

```
Cisco Adaptive Security Appliance Software Version 9.17(1)
SSP Operating System Version 2.11(1.154)
Device Manager Version 7.17(1)
...
```

## FCM UI

Follow the steps in the section.

## **FXOS CLI**

Follow the steps in the section.

## **FXOS REST-API**

Follow the steps in the section.

## **FXOS** Chassis show-tech file

Follow the steps in the section.

## **Firepower Module Software Version**

The Firepower module on ASA is the new name for the older Sourcefire modules or SFR.

Its software version can be verified with the use of these options:

- FMC UI
- FMC REST-API
- Firepower module CLI
- Firepower module troubleshoot file
- ASA CLI
- ASA show-tech file

## FMC UI

Follow the steps in the section.

## **FMC REST-API**

Follow the steps in the section.

## **Firepower Module CLI**

Follow these steps to verify the Firepower module software version on the module CLI:

- 1. Connect to the module via SSH or from the ASA CLI via the **session sfr** command.
- 2. Run the **show version** command:

| > show version       |   |                                       |
|----------------------|---|---------------------------------------|
| [ sfr1 ]             |   |                                       |
| Model                | : | ASA5516 (72) Version 7.1.0 (Build 90) |
| UUID                 | : | c049dad8-c42e-11e9-986d-bdeff3ce399e  |
| Rules update version | : | 2022-05-10-001-vrt                    |
| VDB version          | : | 354                                   |
|                      |   |                                       |

#### **Firepower Module Troubleshoot file**

Follow these steps to verify the Firepower module software version in the module troubleshoot file:

- 1. Open the troubleshoot file and navigate to the folder **<filename>-troubleshoot .tar/results-<date>--xxxxxx/command-outputs/**
- 2. Open the file usr-local-sf-bin-sfcli.pl show version.output and find the line with Model:

| # pwd   |   |  |  |  |  |  |  |
|---|---|--|--|--|--|--|--|
| 'var/tmp/results-05-12-2022199172/command-outputs     |   |  |  |  |  |  |  |
| t cat "usr-local-sf-bin-sfcli.pl show version.output" |   |  |  |  |  |  |  |
| [ sfr1  | ] Model : ASA5516 (72) Version 7.1.0 (Build 90) |  |  |  |  |  |  |
| UUID  | : c049dad8-c42e-11e9-986d-bdeff3ce399e          |  |  |  |  |  |  |
| LSP version   | : 2022-05-10-001-vrt                            |  |  |  |  |  |  |
| VDB version   | : 354   |  |  |  |  |  |  |
|   |   |  |  |  |  |  |  |

## ASA CLI

Run the show module sfr details command on the ASA CLI and check the Software version:

| asa# show module sf  | c details                          |
|----------------------|------------------------------------|
| Getting details from | n the Service Module, please wait  |
|                      |                                    |
| Card Type:           | FirePOWER Services Software Module |
| Model:               | ASA5516                            |
| Hardware version:    | N/A                                |
| Serial Number:       | JAD222103XA                        |
| Firmware version:    | N/A                                |
| Software version:    | 7.1.0-90                           |
| MAC Address Range:   | 7872.5dce.b3b2 to 7872.5dce.b3b2   |
| App. name:           | ASA FirePOWER                      |
| App. Status:         | Up                                 |
| App. Status Desc:    | Normal Operation                   |
| App. version:        | 7.1.0-90                           |
| Data Plane Status:   | Up                                 |
| Console session:     | Ready                              |
| Status:              | Up                                 |
| DC addr:             | No DC Configured                   |
| Mgmt IP addr:        | 192.168.45.45                      |
| Mgmt Network mask:   | 255.255.255.0                      |
| Mgmt Gateway:        | 0.0.0                              |

Mgmt web ports: 443 Mgmt TLS enabled: true

#### ASA show-tech file

Search for the line with the show module sfr detail string:

----- show module sfr detail ------Getting details from the Service Module, please wait... Card Type: FirePOWER Services Software Module ASA5516 Model: Hardware version: N/A Serial Number: JAD222103XA Firmware version: N/A Software version: 7.1.0-90 MAC Address Range: 7872.5dce.b3b2 to 7872.5dce.b3b2 ASA FirePOWER App. Status: Up App. Status Desc: Normal Operation App. version: 7.1.0-90 Data Plane Status: Up Ready Console session: Status: Up No DC Configured DC addr: Mgmt IP addr: 192.168.45.45 Mgmt Network mask: 255.255.255.0 Mgmt Gateway: 0.0.0.0 Mgmt web ports: 443 Mgmt TLS enabled: true

# Verify Snort, VDB, and SRU Versions

# **Deep Packet Inspection Engine (Snort) Version**

The Snort version can be verified with the use of these options:

- FMC UI
- FMC REST-API
- FDM UI
- FDM REST API
- FTD or Firepower module CLI
- FTD or Firepower module troubleshoot file

#### FMC UI

Follow these steps to verify the FTD Snort version on FMC UI:

1. Choose Devices > Device Management:



## 2. Check the Snort label:

| cisco D              | Firepower Management Center o  | verview Analysis        | Policies | Devices Objects       | AMP                    |                          | Deploy Q 🌮 🔅                 | Ø admin ▼            |
|----------------------|--|-------------------------|----------|-----------------------|------------------------|--------------------------|------------------------------|----------------------|
| View By:<br>All (14) | Domain   Error (2)   Warning (0)  Offline  | (12) • Normal (0)       | Deployme | nt Pending (7) • Upgr | ade (0) • Snort 3 (12) |                          | Deployme<br>Q. Search Device | ent History<br>Add 🔻 |
| Collapse Al          | ll in the second se |                         |          |                       |                        |                          |                              |                      |
| Na                   | ame  | Model                   | Version  | Chassis               | Licenses               | Access Control<br>Policy | Group                        |                      |
|                      | LAB-FPR2K<br>High Availability   |                         |          |                       |                        |                          |                              | <pre>/: ^</pre>      |
|                      | fpr2k-1(Primary, Active) Snort 3<br>192.0.2.140 - Routed   | Firepower 2110 with FTD | 7.1.0    | N/A                   | Base, Threat (2 more)  | LAB-FPR2K-ACL            |                              | :                    |
|                      | ftp2k-2(Secondary,Standby) Snort 3<br>192.0.2.149 - Routed   | Firepower 2110 with FTD | 7.1.0    | N/A                   | Base, Threat (2 more)  | LAB-FPR2K-ACL            |                              | :                    |

## **FMC REST-API**

Follow these steps to verify the FTD Snort version via FMC REST-API. Use a REST-API client to verify the software version. In this example, curl is used:

1. Request an authentication token:

```
# curl -s -k -v -X POST 'https://192.0.2.1/api/fmc_platform/v1/auth/generatetoken' -H
'Authentication: Basic' -u 'admin:Cisco123' | grep -i X-auth-access-token
<X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb</pre>
```

2. Identify the domain that contains the device. In the majority of the REST API queries the **domain** parameter is mandatory. Use the **X-auth-access-token in** this query to retrieve the list of domains:

```
# curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_platform/v1/info/domain' -H 'accept:
application/json' -H 'X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m
json.tool
```

"items": [

{

```
{
        "name": "Global",
        "type": "Domain",
        "uuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f"
    },
    {
        "name": "Global/domain1",
        "type": "Domain",
        "uuid": "ef0cf3e9-bb07-8f66-5c4e-00000000001"
    },
    {
        "name": "Global/domain2",
        "type": "Domain",
        "uuid": "341a8f03-f831-c364-b751-00000000001"
    }
],
"links": {
    "self": "https://192.0.2.1/api/fmc_platform/v1/info/domain?offset=0&limit=25"
},
"paging": {
    "count": 3,
    "limit": 25,
    "offset": 0,
    "pages": 1
}
```

3. Use the domain UUID to query for the devicerecords:

}

```
# curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-
0000000001/devices/devicerecords' -H 'accept: application/json' -H 'X-auth-access-token:
5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m json.tool
{
    "items": [
        {
            "id": "a4752f3c-86cc-11e9-8c9a-a3c958bed664",
            "links": {
                "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-
0000000001/devices/devicerecords/a4752f3c-86cc-11e9-8c9a-a3c958bed664"
            },
            "name": "fw1.lab.local",
            "type": "Device"
        },
        {
            "id": "05e9799c-94fc-11ea-ad33-a0032ddb0251",
            "links": {
                "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-
0000000001/devices/devicerecords/05e9799c-94fc-11ea-ad33-a0032ddb0251"
            },
            "name": "fw2.lab.local",
            "type": "Device"
        },
        {
            "id": "c8bef462-49f7-11e8-b2fb-ad9838c6ed90",
            "links": {
                "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-
00000000001/devices/devicerecords/c8bef462-49f7-11e8-b2fb-ad9838c6ed90"
            },
            "name": "fw3.lab.local",
            "type": "Device"
```

```
},
        {
            "id": "3c41913a-b27b-11eb-b131-d2e2ce2a368d",
            "links": {
                "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-
0000000001/devices/devicerecords/3c41913a-b27b-11eb-b131-d2e2ce2a368d"
            },
            "name": "fw4.lab.local",
            "type": "Device"
        },
        {
            "id": "48f7f37c-8cf0-11e9-bf41-fb2d7b740db7",
            "links": {
                "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-
0000000001/devices/devicerecords/48f7f37c-8cf0-11e9-bf41-fb2d7b740db7"
            },
            "name": "fw5.lab.local",
            "type": "Device"
        },
        {
            "id": "0b1a9c94-8ba8-11ec-b2fd-93263934908d",
            "links": {
                "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-
0000000001/devices/devicerecords/0b1a9c94-8ba8-11ec-b2fd-93263934908d"
            },
            "name": "fpr2k-1",
            "type": "Device"
        },
```

4. Use the domain UUID and the device/container UUID in this request:

```
# curl -s -k -X GET 'https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-
00000000001/devices/devicerecords/0b1a9c94-8ba8-11ec-b2fd-93263934908d' -H 'X-auth-access-
token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb ' | python -m json.tool | grep -i snort
```

```
"snortVersion": "3.1.7.1-108",
"snortEngine": "SNORT3",
```

#### FDM UI

Follow these steps to verify the FTD Snort version on FDM UI:

1. Go to the Updates page:

| CISCO. Firepower Device Manager                                   | Monitoring Policies Objects  | Device: KSEC-FPR2100  | ) 🙆 😨 ? 👬 admin<br>Administrator  |
|---|--|---|---|
| Model<br>Cisco Firepower 2120 Thre                                | Software VDB Intrusion Rule<br>at Defense 7.1.0-90 346.0 20211110-13 | Update Cloud Services High A<br>348 🐼 Not Registered   Register Not Ce                                  | Availability C CONFIGURE  |
|   | 1/2<br>Cisco Firepower 2120 Threat Defense 🕕                         |   | Internet  |
| C Inside Network  | MOMT 1/1 1/3 1/5 1/7 1/9 1   | //1<br>1/13 1/14 1/15 1/16<br>1/12 SFP  | N/Gateway O NTP Server  |
|   | 1/1  |   |   |
| Interfaces<br>Connected<br>Enabled 3 of 17<br>View All Interfaces | Routing There are no static routes yet View Configuration            | Updates<br>Geolocation, Rule, VDB, System Upgrade,<br>Security Intelligence Feeds<br>View Configuration | System Settings<br>Management Access<br>Logging Settings<br>DHCP Server / Relay<br>DDNS Service |

## 2. Check Snort Inspection Engine:

| CISCO. Firepower Device Manager  | 题<br>Monitoring           | Ø<br>Policies      | Objects | Devic | ce: KSEC-FPR2100  | (>)                               |  | 0  | ?  | :                                | admin<br>Administrator  | ~  |
|--|---------------------------|--------------------|---------|-------|---|-----------------------------------|--|--|--|----------------------------------|---|----|
| Device Summary<br>Updates  |                           |                    |         |       |   |                                   |  |  |  |                                  |   |    |
| Geolocation 2020-04-28-002<br>Latest Update on 05 May 2022                               | VDB 346.<br>Latest Upda   | 0<br>ite on 05 May | 2022    |       | Security Intelligence Feeds                                 |                                   |  |  |  |                                  |   |    |
| Configure<br>Set recurring updates   | Configure<br>Set recurrin | g updates          |         |       | Configure<br>Set recurring updates                          |                                   |  |  |  |                                  |   |    |
| UPDATE FROM CLOUD  | UPDATE F                  | ROM CLOUD          | ~       |       | UPDATE FROM CLOUD   |                                   |  |  |  |                                  |   |    |
| System Upgrade<br>Current version 7.1.0-90   |                           |                    |         |       | Intrusion Rule 20211110-134<br>Latest Update on 05 May 2022 | 8                                 |  |  |  |                                  |   |    |
| There are no software upgrades available<br>Upload an upgrade file to install.<br>BROWSE | e on the system.          |                    |         |       | Configure<br>Set recurring updates<br>UPDATE FROM CLOUD     | Sno<br>Insp<br>Sno<br>Defe<br>SSL | ort<br>ection E<br>rt is the<br>ense. It i<br>decryp | ingine: 3<br>main ins<br>s used f<br>tion, and | 3.1.7.1-1<br>spection<br>or intrusi<br>l layer 7 i | 08 Down<br>engine in<br>on and f | ngrade to 2.0<br>n Firepower Threa<br>file policy analysis,<br>on. See more V | t, |

## **FDM REST API**

Follow these steps to verify the Snort version via an FDM REST-API request. Use a REST-API client to verify the software version. In this example, curl is used:

1. Request an authentication token:

```
# curl -k -X POST --header 'Content-Type: application/json' --header 'Accept: application/json'
-d '{ "grant_type": "password", "username": "admin", "password": "Admin#1324" }'
'https://192.0.2.2/api/fdm/latest/fdm/token'
{
    "access_token":
    "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIyNDk5NTcsInN1YiI6ImFkbWluIiwianRpIjoiNDk3MmRjNjAtZDBmMi0xMW
VjLTk4ZWMtNDdlZTQwODkwMDVjIiwibmJmIjoxNjUyMjQ5OTU3LCJleHAiOjE2NTIyNTE3NTcsInJlZnJlc2hUb2tlbkV4cG
lyZXNBdCI6MTY1MjI1MjM1NzQ1NywidG9rZW5UeXBlIjoiSldUX0FjY2VzcyIsInVzZXJVdWlkIjoiYTU3ZGVmMjgtY2M3MC
0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2
VybmFtZS16ImFkbWluIn0.lJLmHddJ2jaVRmpdXF6qg48qdBcyRuit94DLobCJ9LI",
```

```
"expires_in": 1800,
"refresh_expires_in": 2400,
"refresh_token":
"eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIzOTQxNjksInN1YiI6ImFkbWluIiwianRpIjoiMGU0NGIxYzQtZDIOMi0xMW
VjLTk4ZWMtYTllOT1kZGMwN2Y0IiwibmJmIjoxNjUyMzk0MTY5LCJleHAiOjE2NTIzOTY1NjksImFjY2Vzc1Rva2VuRXhwaX
Jlc0F0IjoxNjUyMzk1OTY5MDcwLCJyZWZyZXNoQ291bnQiOi0xLCJ0b2t1b1R5cGUiOiJKV1RfUmVmcmVzaCIsInVzZXJVdW
lkIjoiYTU3ZGVmMjgtY2M3Mc0xMWVjLTk4ZWMtZjk40DExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2
luIjoicGFzc3dvcmQiLCJ1c2VybmFtZSI6ImFkbWluIn0.Avga0-isDjQB527d3QWZQb7AS4a9ea5wlbYUn-A9aPw",
"token_type": "Bearer"
}
```

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIONDU3ODksInN1YiI6ImFkbWluIiwianRpIjoiM2U1Njg0YjYtZDJiYS0xMWV
jLTk4ZWMtZGI2YjRiYTM1MTU2IiwibmJmIjoxNjUyNDQ1Nzg5LCJleHAiOjE2NTIONDc1ODksInJlZnJlc2hUb2tlbkV4cGl
yZXNBdCI6MTY1MjQ0ODE4OTMyNSwidG9rZW5UeXB1IjoiSldUX0FjY2VzcyIsInVzZXJVdWlkIjoiYTU3ZGVmMjgtY2M3MC0
xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2V
ybmFtZSI6ImFkbWluIn0.kXtsUu3_WWtOWu9w0mSDfJjwcyiVCa5dgyzNjCGnlF4'
'https://10.62.148.181/api/fdm/v6/operational/systeminfo/default' | grep -i snort
"snortVersion" : { "snortVersion" : "3.1.7.1-108",
```

```
"snortversion" : { "snortversion" : "3.1./.1-108",
"snortPackage" : "/ngfw/var/sf/snort-3.1.7.1-108/snort-75-3.1.7.1-108-daq14.tar.bz2",
"type" : "snortversion
```

## **FTD or Firepower CLI**

On FTD CLI run the show snort3 status command:

> show snort3 status Currently running Snort 3 The Firepower module supports only Snort 2.

## FTD or Firepower Module Troubleshoot file

Follow these steps to verify the Snort version in the FTD troubleshoot file:

- 1. Open the troubleshoot file and navigate to the folder <filename>-troubleshoot .tar/results-<date>--xxxxxx/command-outputs
- 2. Open the file usr-local-sf-bin-sfcli.pl show snort3.output:

```
# pwd
/var/tmp/results-05-06-2022--163203/command-outputs
# cat "usr-local-sf-bin-sfcli.pl show snort3.output"
Output of /ngfw/usr/local/sf/bin/sfcli.pl show snort3:
Currently running Snort 3
The Firepower module supports only Snort 2.
```

## **Vulnerability Database (VDB) Version**

The VDB version can be verified with the use of these options:

```
• FMC UI
```

• FMC REST-API

- FMC troubleshoot file
- FDM UI
- FDM REST API
- FTD CLI
- FTD or Firepower module troubleshoot file

## FMC UI

Follow these steps to verify the VDB version on FMC UI:

## 1. Choose Help > About:

| Firepower Management Center<br>Overview / Dashboards / Management  | Overview         | Analysis          | Policies     | Devices | Objects | AMP Ir | telligen                  | ce   |                                    | Deploy           | ۹ 🎸  | ି 🕼 🕜 admin 🔻   |
|--|------------------|-------------------|--------------|---------|---------|--------|---------------------------|--|------------------------------------|------------------|--|---|
| Name           Access Controlled User Statistics<br>Provides traffic and intrusion event statistics by user           Application Statistics<br>Provides traffic and intrusion event statistics by application |                  |                   |              |         |         |        | Pa<br>He<br>W<br>Se<br>Se | age-level Help<br>ow-Tos<br>ocumentation on<br>hat's New in This<br>oftware Download<br>ecure Firewall You | Cisco.com<br>Release<br>1<br>JTube | 2 <mark>-</mark> | Secure Firewa<br>Firepower Mig<br>Partner Ecosy<br>Ask a Questic<br>TAC Support<br>About | all on Cisco.com<br>gration Tool<br>stem<br>in<br>Cases |
| Application Statistics (7.1.0)<br>Provides application statistics  |                  |                   |              |         |         |        |                           | admin  | No                                 | N                | lo   | C . / .   |
| Connection Summary<br>Provides tables and charts of the activity on your monitored net   | twork segment or | ganized by differ | ent criteria |         |         |        |                           | admin  | No                                 | N                | lo   | 12 Q / 1  |
| Detailed Dashboard<br>Provides a detailed view of activity on the appliance  |                  |                   |              |         |         |        |                           | admin  | No                                 | N                | lo   | 12 Q / 1  |
| Detailed Dashboard (7.0.0)<br>Provides a detailed view of activity on the appliance  |                  |                   |              |         |         |        |                           | admin  | No                                 | N                | lo   | CQ/T  |
| Files Dashboard<br>Provides an overview of Malware and File Events   |                  |                   |              |         |         |        |                           | admin  | No                                 | N                | lo   | C Q / T   |
| Security Intelligence Statistics<br>Provides Security Intelligence statistics  |                  |                   |              |         |         |        |                           | admin  | No                                 | N                | lo   | Ľ<∕₹  |
| Summary Dashboard<br>Provides a summary of activity on the appliance   |                  |                   |              |         |         |        |                           | admin  | No                                 | Y                | es   | C < / 7   |

## 2. Check VDB Version:

| Firepower Man   | nagement Center  | Overview                                      | Analysis     | Policies      | Devices | Objects | AMP                          | Intelligence   | Deploy  | Q        | ¢ 😜  | 🕜 admin 🔻 |
|---|--|---|--------------|---------------|---------|---------|------------------------------|--|---|----------|------|-----------|
| Model<br>Serial Number<br>Software Version<br>OS<br>Snort Version<br>Rule Update Version<br>Rulepack Version<br>Module Pack Version<br>LSP Version<br>Geolocation Update Version<br>VDB Version<br>Hostname | Cisco Firepower Manageme<br>001234<br>7.1.0 (build 90)<br>Cisco Firepower Extensible<br>2.9.19 (Build 92)<br>3.1.7.1 (Build 108)<br>2022-05-02-003-vrt<br>2703<br>3070<br>Isp-rel-20220502-1613<br>2022-04-25-002<br>build 354 (2022-04-27 19:<br>FMC-4600-2 | nt Center 4600<br>Operating System<br>39:56 ) | (FX-OS) 2.11 | .1 (build154) |         |         | For tec<br>or call<br>Copyri | chnical/system questions, e<br>us at 1-800-553-2447 or 1-<br>ight 2004-2021, Cisco and/o | nail tac@cisco.com<br>408-526-7209<br>r its affiliates. All right | B reserv | ved. |           |

## FMC CLI

Follow these steps to verify the VDB version on FMC CLI:

- 1. Access FMC via SSH or console connection.
- 2. Run the **show version** command:

#### **FMC REST-API**

Follow these steps to verify the VDB version via an FMC REST-API. Use a REST-API client to verify the software version. In this example, curl is used:

1. Request an authentication token:

```
# curl -s -k -v -X POST 'https://192.0.2.1/api/fmc_platform/v1/auth/generatetoken' -H
'Authentication: Basic' -u 'admin:Cisco123' | grep -i X-auth-access-token
<X-auth-access-token: 7acdb34c-ea85-47bf-83fe-d77b63f012da</pre>
```

2. Identify the domain that contains the device. In the majority of the REST API queries the **domain** parameter is mandatory. Use the **X-auth-access-token in** this query to retrieve the list of domains:

```
# curl -s -k -X GET 'https://192.0.2.1/api/fmc_platform/v1/info/serverversion' -H 'X-auth-
access-token: 7acdb34c-ea85-47bf-83fe-d77b63f012da' | python -m json.tool
{
    "items": [
        {
            "geoVersion": "2022-05-09-001",
            "lspVersion": "lsp-rel-20220510-1044",
            "serverVersion": "7.1.0 (build 90)",
            "sruVersion": "2022-05-10-001-vrt",
            "type": "ServerVersion",
            "vdbVersion": "build 354 ( 2022-04-27 19:39:56 )"
        }
    ],
    "links": {
        "self": "https://10.62.184.21/api/fmc_platform/v1/info/serverversion?offset=0&limit=25"
    },
    "paging": {
        "count": 1,
        "limit": 25,
        "offset": 0,
        "pages": 1
    }
}
```

## **FMC Troubleshoot file**

Follow these steps to verify the VDB version in the FMC troubleshoot file:

- 1. Open the troubleshoot file and navigate to the folder <filename>-troubleshoot .tar/results-<date>--xxxxxx/dir-archives/etc/sf/.versiondb
- 2. Open the file vdb.conf and find the line with the key CURRENT\_BUILD:

# pwd
/var/tmp/results-05-06-2022--199172/dir-archives/etc/sf/.versiondb
# cat vdb.conf
CURRENT\_VERSION=4.5.0
CURRENT\_BUILD=344
CURRENT\_APPID\_VER=82
CURRENT\_NAVL\_VER=106

## **FDM UI**

#### On the main page check VDB:



## **FDM REST API**

Follow these steps to verify the VDB version via an FDM REST-API request. Use a REST-API client to verify the software version. In this example, curl is used:

1. Request an authentication token:

```
# curl -k -X POST --header 'Content-Type: application/json' --header 'Accept: application/json'
-d '{ "grant_type": "password", "username": "admin", "password": "Admin#1324" }'
'https://192.0.2.2/api/fdm/latest/fdm/token'
{
"access_token":
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIyNDk5NTcsInN1YiI6ImFkbWluIiwianRpIjoiNDk3MmRjNjAtZDBmMi0xMW "
VjLTk4ZWMtNDdlZTQwODkwMDVjIiwibmJmIjoxNjUyMjQ5OTU3LCJleHAiOjE2NTIyNTE3NTcsInJlZnJlc2hUb2tlbkV4cG
lyZXNBdCI6MTY1MjI1MjM1NzQ1NywidG9rZW5UeXBlIjoiSldUX0FjY2VzcyIsInVzZXJVdWlkIjoiYTU3ZGVmMjgtY2M3MC
0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXN1clJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2
VybmFtZSI6ImFkbWluIn0.lJLmHddJ2jaVRmpdXF6qg48qdBcyRuit94DLobCJ9LI",
"expires_in": 1800,
"refresh_expires_in": 2400,
"refresh_token":
"eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIzOTQxNjksInN1YiI6ImFkbWluIiwianRpIjoiMGU0NGIxYzQtZDI0Mi0xMW
VjLTk4ZWMtYTllOTlkZGMwN2Y0IiwibmJmIjoxNjUyMzk0MTY5LCJleHAiOjE2NTIzOTY1NjksImFjY2Vzc1Rva2VuRXhwaX
Jlc0F0IjoxNjUyMzk10TY5MDcwLCJyZWZyZXNoQ291bnQiOi0xLCJ0b2tlblR5cGUiOiJKV1RfUmVmcmVzaCIsInVzZXJVdW
lkIjoiYTU3ZGVmMjgtY2M3MC0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2
luIjoicGFzc3dvcmQiLCJ1c2VybmFtZSI6ImFkbWluIn0.Avga0-isDjQB527d3QWZQb7AS4a9ea5wlbYUn-A9aPw",
"token_type": "Bearer"
```

2. Use the access\_token value in this query:

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer
eyJhbGciOiJIUZI1NiJ9.eyJpYXQiOjE2NTIONDU3ODksInN1YiI6ImFkbWluIiwianRpIjoiM2U1NjgOYjYtZDJiYSOxMWV
jLTk4ZWMtZGI2YjRiYTM1MTU2IiwibmJmIjoxNjUyNDQ1Nzg5LCJleHAiOjE2NTIONDc1ODksInJlZnJlc2hUb2tlbkV4cGl
yZXNBdCI6MTY1MjQ0ODE4OTMyNSwidG9rZW5UeXBlIjoiSldUXOFjY2VzcyIsInVzZXJVdWlkIjoiYTU3ZGVmMjgtY2M3MCO
xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2V
ybmFtZSI6ImFkbWluIn0.kXtsUu3_WWtOWu9w0mSDfJjwcyiVCa5dgyzNjCGnlF4'
'https://10.62.148.181/api/fdm/v6/operational/systeminfo/default' | grep -i vdb
    "vdbVersion" : {
    "lastSuccessVDBDate" : "2022-05-05 12:44:09Z",
    "vdbCurrentVersion" : "346",
    "vdbCurrentBuild" : "0",
    "vdbReleaseDate" : "2021-08-24 21:48:15",
    "type" : "vdbversion"
```

#### **FTD or Firepower Module CLI**

Follow these steps to verify the VDB version on the FTD CLI or on the Firepower module (SFR) CLI:

- 1. Access FTD via SSH or console connection. In the case of the Firepower module, access the module via SSH, or from the ASA CLI via the **session sfr** command.
- 2. Run the show version command on CLI:

| > show version               |   |
|------------------------------|---|
| [ f]                         | pr2k-1 ]  |
| Model                        | : Cisco Firepower 2110 Threat Defense (77) Version 7.1.0 (Build 90) |
| UUID                         | : 0b1a9c94-8ba8-11ec-b2fd-93263934908d                              |
| LSP version                  | : lsp-rel-20220510-1044   |
| VDB version                  | : 354   |
| > show version               |   |
| <pre>&gt; show version</pre> |   |
| [ sfr1                       |   |
| Model                        | : ASA5516 (72) Version 7.1.0 (Build 90)                             |
| UUID                         | : c049dad8-c42e-11e9-986d-bdeff3ce399e                              |
| Rules update version         | : 2022-05-10-001-vrt  |
| VDB version                  | : 354   |
|                              |   |

## FTD or Firepower Module Troubleshoot file

Follow these steps to verify the VDB version in the FTD or the Firepower module troubleshoot file:

- 1. Open the troubleshoot file and navigate to the folder **<filename>-troubleshoot.tar/results-**<date>--xxxxxx/command-outputs/
- 2. Open the file **usr-local-sf-bin-sfcli.pl show version.output** and find the line with the **VDB version**:

| [           | fpr2k-1 ]   |
|-------------|---|
| Model       | : Cisco Firepower 2110 Threat Defense (77) Version 7.1.0 (Build 90) |
| UUID        | : 0b1a9c94-8ba8-11ec-b2fd-93263934908d                              |
| LSP version | : lsp-rel-20220510-1044   |
| VDB version | : 354   |

#### # pwd

## **Intrusion rule Update Versions**

The intrusion rule updates provide new and updated intrusion rules and preprocessor rules, modified states for installed rules, and modified default intrusion policy settings.

The secure rule updates (SRU) are applicable to Snort version 2, and the Lightweight Security Package (LSP) updates are applicable to Snort version 3.

The SRU/LSP software version can be verified with the use of these options:

- FMC UI
- FMC REST-API
- FMC troubleshoot file
- FDM UI
- FDM REST API
- FTD or Firepower module CLI
- FTD or Firepower module troubleshoot file

## **FMC UI**

Follow these steps to verify SRU/LSP versions on FMC UI:

1. Choose **Help > About:** 

| Firepower Management Center<br>Overview / Dashboards / Management  | Overview         | Analysis          | Policies     | Devices | Objects | AMP | Intellig | gence   |                                      | Deploy                       | ۹ 🌢  | 🚰 🎝 1 🕜 admin 🔻   |
|--|------------------|-------------------|--------------|---------|---------|-----|----------|---|--------------------------------------|------------------------------|--|---|
| Name           Access Controlled User Statistics<br>Provides traffic and intrusion event statistics by user           Application Statistics<br>Provides traffic and intrusion event statistics by application |                  |                   |              |         |         |     |          | Page-level Help<br>How-Tos<br>Documentation on<br>What's New in Thi<br>Software Downloa<br>Secure Firewall Yo | Cisco.com<br>s Release<br>d<br>uTube | S<br>F<br>A<br>T<br>T<br>2 A | ecure Firen<br>irepower N<br>artner Eco<br>sk a Quest<br>AC Suppor | wall on Cisco.com<br>Aigration Tool<br>system<br>tion<br>rt Cases |
| Application Statistics (7.1.0)<br>Provides application statistics  |                  |                   |              |         |         |     |          | admin   | No                                   | No                           |  | C < ≠ ₹   |
| Connection Summary<br>Provides tables and charts of the activity on your monitored ne  | twork segment or | ganized by differ | ent criteria |         |         |     |          | admin   | No                                   | No                           | ,<br>,   | 12 Q / 1  |
| Detailed Dashboard<br>Provides a detailed view of activity on the appliance  |                  |                   |              |         |         |     |          | admin   | No                                   | No                           | þ  | 12 Q / 1  |
| Detailed Dashboard (7.0.0)<br>Provides a detailed view of activity on the appliance  |                  |                   |              |         |         |     |          | admin   | No                                   | No                           | 0  | 12 Q / 1  |
| Files Dashboard<br>Provides an overview of Malware and File Events   |                  |                   |              |         |         |     |          | admin   | No                                   | N                            | <b>b</b>   | 12 Q / 1  |
| Security Intelligence Statistics<br>Provides Security Intelligence statistics  |                  |                   |              |         |         |     |          | admin   | No                                   | No                           | 0  | 12 Q / 1  |
| Summary Dashboard<br>Provides a summary of activity on the appliance   |                  |                   |              |         |         |     |          | admin   | No                                   | Ye                           | s  |   |

## 2. Check Rule Update Version and LSP Version:



## FMC CLI

Follow these steps to verify SRU/LSP versions on FMC CLI:

- 1. Access FMC via SSH or console connection.
- 2. Run the show version command on CLI:

## **FMC REST-API**

Follow these steps to verify the software version via a REST-API request. Use a REST-API client to verify the software version. In this example, **curl** is used:

1. Request an authentication token:

# curl -s -k -v -X POST 'https://192.0.2.1/api/fmc\_platform/v1/auth/generatetoken' -H
'Authentication: Basic' -u 'admin:Cisco123' | grep -i X-auth-access-token

```
< X-auth-access-token: 9408fe38-c25c-4472-b7e6-3571bb4e2b8d
```

2. Use the X-auth-access-token in this query:

```
# curl -s -k -X GET 'https://192.0.2.1/api/fmc_platform/v1/info/serverversion' -H 'X-auth-
access-token: 7acdb34c-ea85-47bf-83fe-d77b63f012da' | python -m json.tool
{
    "items": [
        {
            "geoVersion": "2022-05-09-001",
            "lspVersion": "lsp-rel-20220510-1044",
            "serverVersion": "7.1.0 (build 90)",
            "sruVersion": "2022-05-10-001-vrt",
            "type": "ServerVersion",
            "vdbVersion": "build 354 ( 2022-04-27 19:39:56 )"
        }
    ],
    "links": {
        "self": "https://10.62.184.21/api/fmc_platform/v1/info/serverversion?offset=0&limit=25"
    },
    "paging": {
        "count": 1,
        "limit": 25,
        "offset": 0,
        "pages": 1
    }
}
```

## **FMC Troubleshoot file**

Follow these steps to verify the SRU version in the FMC troubleshoot file:

- 1. Open the troubleshoot file and go to folder <filename>.tar/results-<date>--xxxxx/dirarchives/etc/sf/
- 2. Open the file sru\_versions.conf and find the lines with keys Intrusion\_Rules\_Update:

```
# pwd
/var/tmp/results-05-06-2022--199172/dir-archives/etc/sf/
# cat sru_versions.conf
Intrusion_Rules_Update=2022-04-25-003-vrt
Rule_Pack=2699
Sourcefire_Decoder_Rule_Pack=2088
Sourcefire_Policy_Pack=2763
Module_Pack=3066
snort=2.9.16-4022
```

Follow these steps to verify LSP version in the FMC troubleshoot file:

- 1. Open the troubleshoot file and go to folder <filename>.tar/results-<date>-xxxxxx/command-outputs
- 2. Open file find var-sf-lsp -maxdepth 2 -ls.output and check the line with /var/sf/lsp/active-

# pwd /var/tmp/results-05-06-2022--199172/command-outputs # cat "find var-sf-lsp -maxdepth 2 -ls.output" . . . Output of find /var/sf/lsp -maxdepth 2 -ls: 19138123 4 drwxrwxr-x 3 www root 4096 May 11 04:01 /var/sf/lsp 33 May 11 04:00 /var/sf/lsp/installed-19142268 0 lrwxrwxrwx 1 root root lsp -> /var/sf/lsp/lsp-rel-20220510-1044 4096 May 11 04:01 /var/sf/lsp/lsp-rel-19138299 4 drwxrwxr-x 5 www root 20220510-1044 19142266 600 -rwxrwxr-x 1 www 614400 May 10 14:55 /var/sf/lsp/lsp-relroot 20220510-1044/lsp.icdb.RELEASE.tar 4096 May 11 04:00 /var/sf/lsp/lsp-rel-19142234 4 drwxrwxr-x 5 www root 20220510-1044/ntd\_metadata 19268898 4 drwxrwxr-x 4096 May 10 14:55 /var/sf/lsp/lsp-rel-2 www root 20220510-1044/icdb 19138303 4 drwxrwxr-x 4096 May 10 14:51 /var/sf/lsp/lsp-rel-6 www root 20220510-1044/talos\_content 19142269 46640 -rw-r--r--1 root 47759360 May 11 04:01 /var/sf/lsp/lsp-relroot 20220510-1044/lsp-rel-20220510-1044.tar.xz.REL.tar 238 May 11 04:00 /var/sf/lsp/lsp-rel-19142267 4 -rwxrwxr-x 1 www root 20220510-1044/.snort-versions 26 May 10 14:51 /var/sf/lsp/lsp-rel-19142265 4 -rwxrwxr-x 1 พาพาพา root 20220510-1044/lspd\_ver.properties 260 -rw-r--r--264403 Feb 12 03:32 /var/sf/lsp/pigtail-19139198 1 root root all-1644636642.log 33 May 11 04:01 /var/sf/lsp/active-lsp 0 lrwxrwxrwx 1 root 19142270 root -> /var/sf/lsp/lsp-rel-20220510-1044

## FDM UI

On the main page check Intrusion Rule Update:



## **FDM REST API**

Follow these steps to verify the VDB version via an FDM REST-API request. Use a REST-API

client to verify the software version. In this example, curl is used:

1. Request an authentication token:

```
# curl -k -X POST --header 'Content-Type: application/json' --header 'Accept: application/json'
-d '{ "grant_type": "password", "username": "admin", "password": "Admin#1324" }'
'https://192.0.2.2/api/fdm/latest/fdm/token'
{
"access_token":
"eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIyNDk5NTcsInN1YiI6ImFkbWluIiwianRpIjoiNDk3MmRjNjAtZDBmMi0xMW
VjLTk4ZWMtNDdlZTQwODkwMDVjIiwibmJmIjoxNjUyMjQ5OTU3LCJleHAiOjE2NTIyNTE3NTcsInJlZnJlc2hUb2tlbkV4cG
lyZXNBdCI6MTY1MjI1MjM1NzQ1NywidG9rZW5UeXBlIjoiSldUX0FjY2VzcyIsInVzZXJVdWlkIjoiYTU3ZGVmMjgtY2M3MC
0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXN1clJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2
VybmFtZSI6ImFkbWluIn0.1JLmHddJ2jaVRmpdXF6qg48qdBcyRuit94DLobCJ9LI",
"expires_in": 1800,
"refresh_expires_in": 2400,
"refresh_token":
"eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIzOTQxNjksInN1YiI6ImFkbWluIiwianRpIjoiMGU0NGIxYzQtZDI0Mi0xMW
VjLTk4ZWMtYTllOTlkZGMwN2Y0IiwibmJmIjoxNjUyMzk0MTY5LCJleHAiOjE2NTIzOTY1NjksImFjY2Vzc1Rva2VuRXhwaX
Jlc0F0IjoxNjUyMzk10TY5MDcwLCJyZWZyZXNoQ291bnQi0i0xLCJ0b2tlblR5cGUi0iJKV1RfUmVmcmVzaCIsInVzZXJVdW
lkIjoiYTU3ZGVmMjgtY2M3MC0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2
luIjoicGFzc3dvcmQiLCJ1c2VybmFtZSI6ImFkbWluIn0.Avga0-isDjQB527d3QWZQb7AS4a9ea5wlbYUn-A9aPw",
"token_type": "Bearer"
}
```

2. Use the access\_token value in this query:

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIONDU3ODksInN1YiI6ImFkbWluIiwianRpIjoiM2U1NjgOYjYtZDJiYSOxMWV
jLTk4ZWMtZGI2YjRiYTM1MTU2IiwibmJmIjoxNjUyNDQ1Nzg5LCJleHAiOjE2NTIONDc1ODksInJlZnJlc2hUb2tlbkV4cG1
yZXNBdCI6MTY1MjQ0ODE4OTMyNSwidG9rZW5UeXBlIjoiSldUXOFjY2VzcyIsInVzZXJVdWlkIjoiYTU3ZGVmMjgtY2M3MCO
xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2V
ybmFtZSI6ImFkbWluIn0.kXtsUu3_WWtOWu9w0mSDfJjwcyiVCa5dgyzNjCGnlF4'
'https://10.62.148.181/api/fdm/v6/operational/systeminfo/default' | grep -Ei "sru|lsp"
    "sruVersion" : {
        "sruVersion" : "20211110-1348",
        "lastSuccessSRUDate" : "2022-05-12 18:29:00Z",
```

```
"type" : "sruversion"
FTD or Firepower Module CLI
```

"lspVersions" : [ "20211110-1348" ],

Follow these steps to verify SRU/LSP version on FTD CLI or the Firepower module CLI:

- Access FTD via SSH or console connection. In the case of the Firepower module, access the module via SSH, or from the ASA CLI via the **session sfr** command.
- 2. Run the show version command on CLI:

| > show version  |   |
|-----------------|---|
| [ FIREPOWER1.c: | isco.com ]  |
| Model           | : Cisco Firepower 2120 Threat Defense (77) Version 7.1.0 (Build 90) |
| UUID            | : 1cbe9952-cc6f-11ec-b63a-ae4636e42209                              |
| LSP version     | : lsp-rel-20211110-1348   |
| VDB version     | : 346   |
|                 |   |

------[FIREPOWER1.cisco.com]------Model : Cisco Firepower 2120 Threat Defense (77) Version 7.1.0 (Build 90) UUID : 1cbe9952-cc6f-11ec-b63a-ae4636e42209 Rules update version : 2022-05-11-001-vrt VDB version : 346

#### > show version

| [ sfr1 ]             |   |                                       |
|----------------------|---|---------------------------------------|
| Model                | : | ASA5516 (72) Version 7.1.0 (Build 90) |
| UUID                 | : | c049dad8-c42e-11e9-986d-bdeff3ce399e  |
| Rules update version | : | 2022-05-10-001-vrt                    |
| VDB version          | : | 354                                   |
|                      |   |                                       |

**Note**: The "**show version**" command shows the SRU update version if Snort 2 is used. For Snort 3 LSP version is shown.

#### FTD or Firepower Module Troubleshoot file

Follow these steps to verify SRU/LSP versions in the FTD or Firepower module troubleshoot file:

- 1. Open the troubleshoot file and go to folder <filename>-troubleshoot.tar/results-<date>-xxxxxx/command-outputs/
- Open the file usr-local-sf-bin-sfcli.pl show version.output and find the line with SRU/LSP version:

```
# pwd
/var/tmp/results-05-06-2022--163203/command-outputs/
# cat "usr-local-sf-bin-sfcli.pl show version.output"
-----[ FIREPOWER1.cisco.com ]-----
                     : Cisco Firepower 2120 Threat Defense (77) Version 7.1.0 (Build 90)
Model
                      : 1cbe9952-cc6f-11ec-b63a-ae4636e42209
UUID
                      : lsp-rel-20211110-1348
LSP version
                      : 346
VDB version
_____
or
# pwd
/var/tmp/results-05-06-2022--163203/command-outputs/
# cat "usr-local-sf-bin-sfcli.pl show version.output"
-----[ FIREPOWER1.cisco.com ]------
                      : Cisco Firepower 2120 Threat Defense (77) Version 7.1.0 (Build 90)
Model
                      : 70727d06-8ba7-11ec-bfcc-999f61f27102
UUID
                    : 2022-05-11-001-vrt
Rules update version
VDB version
                      : 346
_____
# pwd
/var/tmp/results-05-12-2022--199172/command-outputs
# cat "usr-local-sf-bin-sfcli.pl show version.output"
-----[ sfr1 ]----- Model : ASA5516 (72) Version 7.1.0 (Build 90) UUID :
c049dad8-c42e-11e9-986d-bdeff3ce399e Rules update version : 2022-05-10-001-vrt
```

: 354

VDB version

# **Known Issues**

Cisco bug ID <u>CSCwb34098</u> ENH: Show FMC version in 'show managers' command output

Cisco bug ID <u>CSCve13470</u> ENH: Enable Software Related OIDs on FirePOWER 6.x

Cisco bug ID <u>CSCwb85969</u> ENH: Include output of "show version" FMC CLISH command in troubleshoot file

Cisco bug ID <u>CSCvu15709</u> ENH: Support for SNMP OIDs to poll SRU/VDB/GEO location versions on Firepower platforms

# **Related Information**

- Secure Firewall Management Center REST API Quick Start Guide, Version 7.1
- <u>Configure SNMP on Firepower NGFW Appliances</u>
- <u>Cisco Firepower Threat Defense REST API Guide</u>
- <u>Cisco FXOS REST API Reference</u>
- <u>Cisco ASA Compatibility</u>
- Firepower 1000/2100 and Secure Firewall 3100 ASA and FXOS Bundle Versions
- Bundled Components
- Firepower Troubleshoot File Generation Procedures