

Verify Firepower Software Versions

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Verify Software Versions](#)

[EMC Software Version](#)

[EMC UI](#)

[EMC CLI](#)

[EMC REST-API](#)

[EMC 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 Troubleshoot 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](#)

[EMC UI](#)

[EMC 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](#)

[EMC UI](#)
[EMC 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](#)

[EMC UI](#)
[EMC REST-API](#)
[EDM UI](#)
[EDM REST API](#)
[FTD or Firepower CLI](#)
[FTD or Firepower Module Troubleshoot file](#)

[Vulnerability Database \(VDB\) Version](#)

[EMC UI](#)
[EMC CLI](#)
[EMC REST-API](#)
[EMC Troubleshoot file](#)
[EDM UI](#)
[EDM REST API](#)
[FTD or Firepower Module CLI](#)
[FTD or Firepower Module Troubleshoot file](#)

[Intrusion rule Update Versions](#)

[EMC UI](#)
[EMC CLI](#)
[EMC REST-API](#)
[EMC Troubleshoot file](#)
[EDM UI](#)
[EDM 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

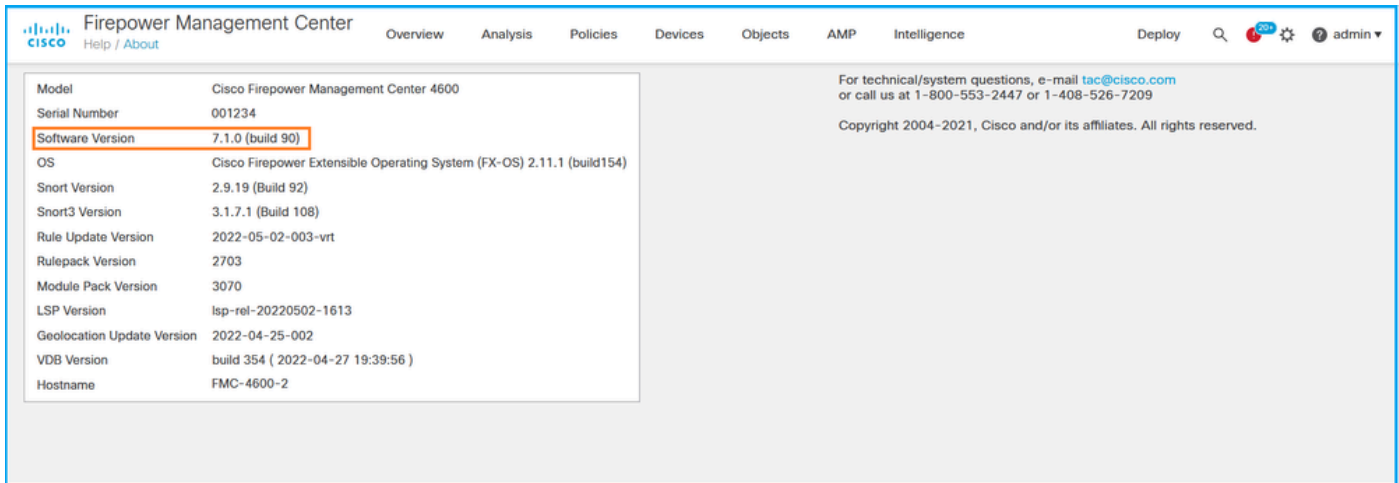
Complete these steps to verify the FMC software version on FMC UI:

1. Choose **Help > About:**

The screenshot shows the Cisco Firepower Management Center (FMC) web interface. The top navigation bar includes the Cisco logo, the title "Firepower Management Center", and several menu items: Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. On the right side of the navigation bar, there are icons for Deploy, Search, a notification bell, a gear for settings, and a user profile labeled "admin". A dropdown menu is open from the settings gear, showing various options. The "About" option is highlighted with a red box and a red number "2".

Name				
Access Controlled User Statistics Provides traffic and intrusion event statistics by user				
Application Statistics Provides traffic and intrusion event statistics by application				
Application Statistics (7.1.0) Provides application statistics	admin	No	No	   
Connection Summary Provides tables and charts of the activity on your monitored network segment organized by different criteria	admin	No	No	   
Detailed Dashboard Provides a detailed view of activity on the appliance	admin	No	No	   
Detailed Dashboard (7.0.0) Provides a detailed view of activity on the appliance	admin	No	No	   
Files Dashboard Provides an overview of Malware and File Events	admin	No	No	   
Security Intelligence Statistics Provides Security Intelligence statistics	admin	No	No	   
Summary Dashboard Provides a summary of activity on the appliance	admin	No	Yes	   

2. Check **Software Version:**



FMC CLI

Complete 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:

```
<#root>
```

```
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:

```
<#root>
```

```
>
```

```
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

Complete 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:

```
<#root>
```

```
# curl -s -k -v -X POST 'https://192.0.2.1/api/fmc_platform/v1/auth/generatetoken' -H 'Authentication: B
```

```
< X-auth-access-token:
```

```
9408fe38-c25c-4472-b7e6-3571bb4e2b8d
```

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

```
<#root>
```

```
#
```

```
curl -k -X GET 'https://192.0.2.1/api/fmc_platform/v1/info/serverversion' -H 'X-auth-access-token: 9408f
```

```
| 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

Complete 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**:

```
<#root>
#
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

Complete 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.

```
<#root>
>
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**:

```
<#root>
admin@fpr2k-1:~$
less /ngfw/var/sf/detection_engines/65455e3a-c879-11ec-869a-900514578f9f/ngfw.rules
```

```
#### ngfw.rules
#####
#
# AC Name      : FTD-ACP-1652807562
# 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

# SRU           : 2022-05-11-001-vrt
# VDB           : 354
#
#####
...

```

FTD or Firepower Module Troubleshoot file

Complete these steps to verify the FMC software 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/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/detection-engines/<UUID>/**
2. Open the **ngfw.rules** file and check row **DC Version**:

```
<#root>
```

```
# pwd
```

```
/var/tmp/results-05-06-2022--163203/file-contents/ngfw/var/sf/detection_engines/5e9fa23a-5429-11ec-891e
```

```
# cat ngfw.rules
```

```
#### ngfw.rules
#####
#
# AC Name      : FTD-ACP-1652807562
# 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

# SRU           : 2022-05-11-001-vrt
# VDB           : 354
#
#####
...

```

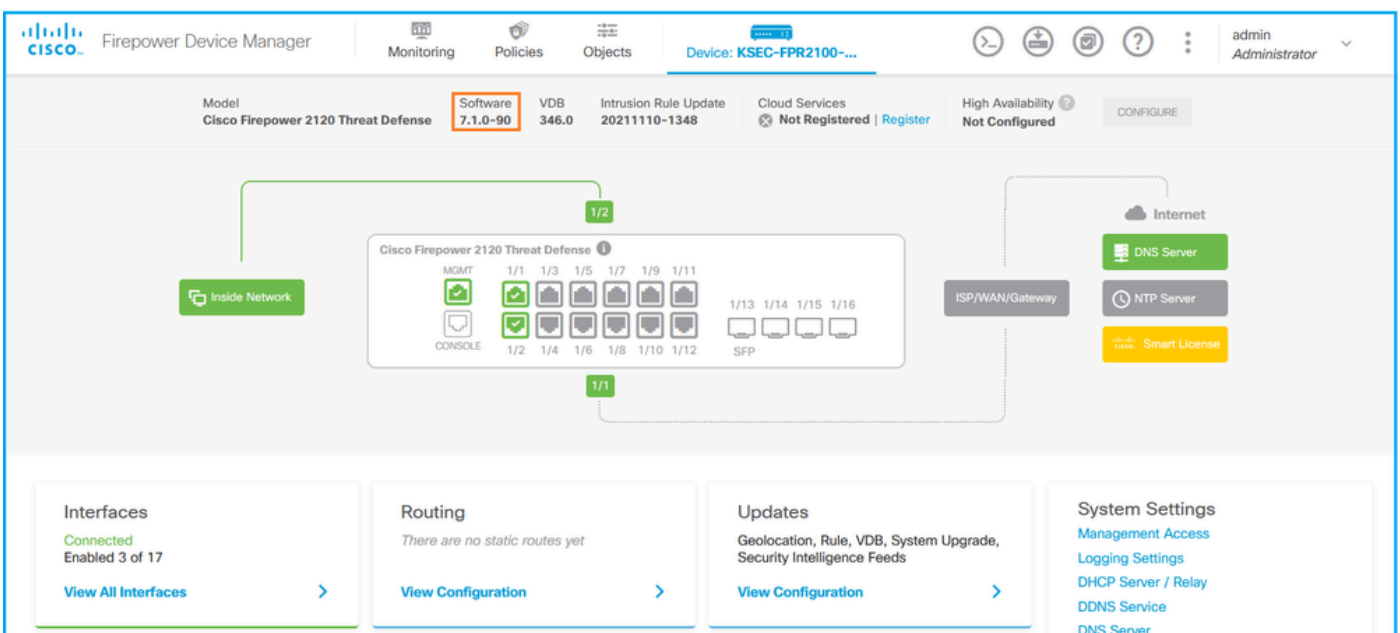
FDM Software Version

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:



FDM REST API

Complete 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:

```
<#root>
```

```
#
```

```
curl -k -X POST --header 'Content-Type: application/json' --header 'Accept: application/json' -d '{"gra
```

```
{
```

```
"
```

```
access_token
```

```
":
```

```
"
```


Complete the steps in the section.

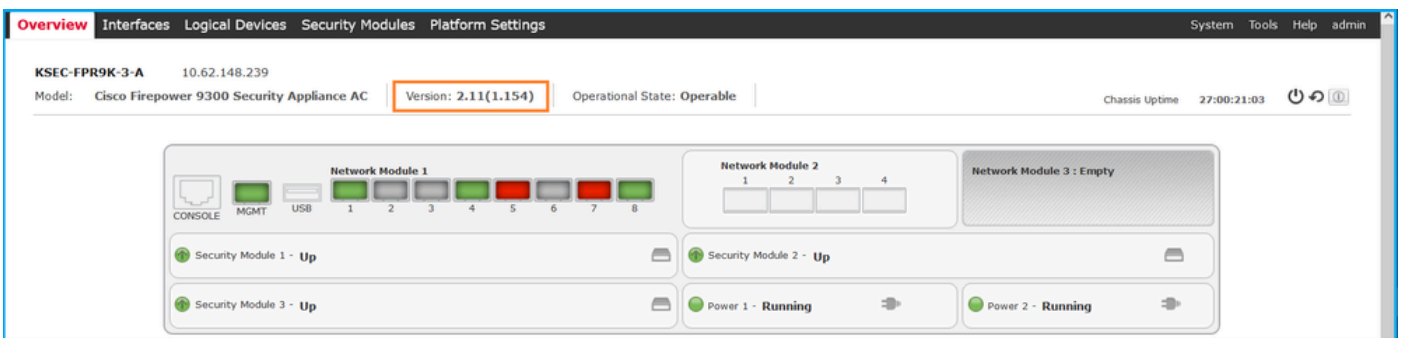
FXOS Software Version

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:



FXOS CLI

Firepower 4100/9300

Complete 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:

```
<#root>
```

```
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

Complete 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:

```
<#root>
```

```
>
```

```
connect fxos
```

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

```
<#root>
```

```
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

Complete 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.

```
<#root>
asa#
connect fxos
```

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

```
<#root>
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

Complete 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.

```
<#root>
```

```
asa#
```

```
connect fxos
```

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

```
<#root>
```

```
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

Complete 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:

```
<#root>
```

```
# curl -k -X POST -H 'USERNAME: admin' -H 'PASSWORD: Cisco123' 'https://192.0.2.100/api/login'
```

```
{
  "refreshPeriod": "0",
  "token": "
1206f6a3032e7bdbbeac07cfdd9d5add5cdd948e4e5f4511535a959aed7e1e2f5
"
}
```

2. Use the token in this query:

```
<#root>
```

```
#
```

```
curl -s -k -X GET -H 'Accept: application/json' -H 'token: 1206f6a3032e7bdbbeac07cfdd9d5add5cdd948e4e5f45'
```

```
"platformBundleName": "fxos-k9.2.11.1.154.SPA",
```

```
"platformBundleVersion": "2.11(1.154)",
```

FXOS SNMP

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

Firepower 4100/9300

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

1. Ensure that SNMP is configured on FXOS. Refer to [Configure SNMP on Firepower NGFW Appliances](#) 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**:

```
<#root>
```

```
#
```

```
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)"  
.1.3.6.1.4.1.9.9.826.1.30.47.1.6.32615 = 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

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

1. Ensure that SNMP is configured on FXOS. Refer to [Configure SNMP on Firepower NGFW Appliances](#) for configuration steps.
2. Poll **.1.3.6.1.2.1.1.1.0** or **SNMPv2-MIB::sysDescr.0**:

```
<#root>
```

```
#
snmpwalk -On -v2c -c cisco 192.0.2.101 SNMPv2-MIB::sysDescr.0

.1.3.6.1.2.1.1.1.0 = STRING: Cisco FirePOWER FPR-2140 Security Appliance,
System Version 2.11(1.146)
```

```
#
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

Complete 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:

```
<#root>
#
pwd

/var/tmp/20220313201802_F241-01-11-FPR-2_BC1_a11/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:

```
<#root>
```

```
#
```

```
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

Complete 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:

```
<#root>
```

```
>
```

```
show version
```

```
-----[
```

```
firepower
```

]-----

```
Model :  
Cisco Firepower 2120 Threat Defense (77)  
Version 7.1.0 (Build 90)  
UUID : 1b324aaa-670e-11ec-ac2b-e000f0bd3ca1  
LSP version : lsp-rel-20220328-1342  
VDB version : 353  
-----
```

FTD SNMP

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

1. Ensure that SNMP is configured and enabled. For FDM-managed FTD, refer to [Configure and troubleshoot SNMP on Firepower FDM](#) for configuration steps. For FMC-managed FTD, refer to [Configure SNMP on Firepower NGFW Appliances](#) for configuration steps.
2. Poll OID **SNMPv2-MIB::sysDescr.0** or OID **.1.3.6.1.2.1.1.1.0.:**

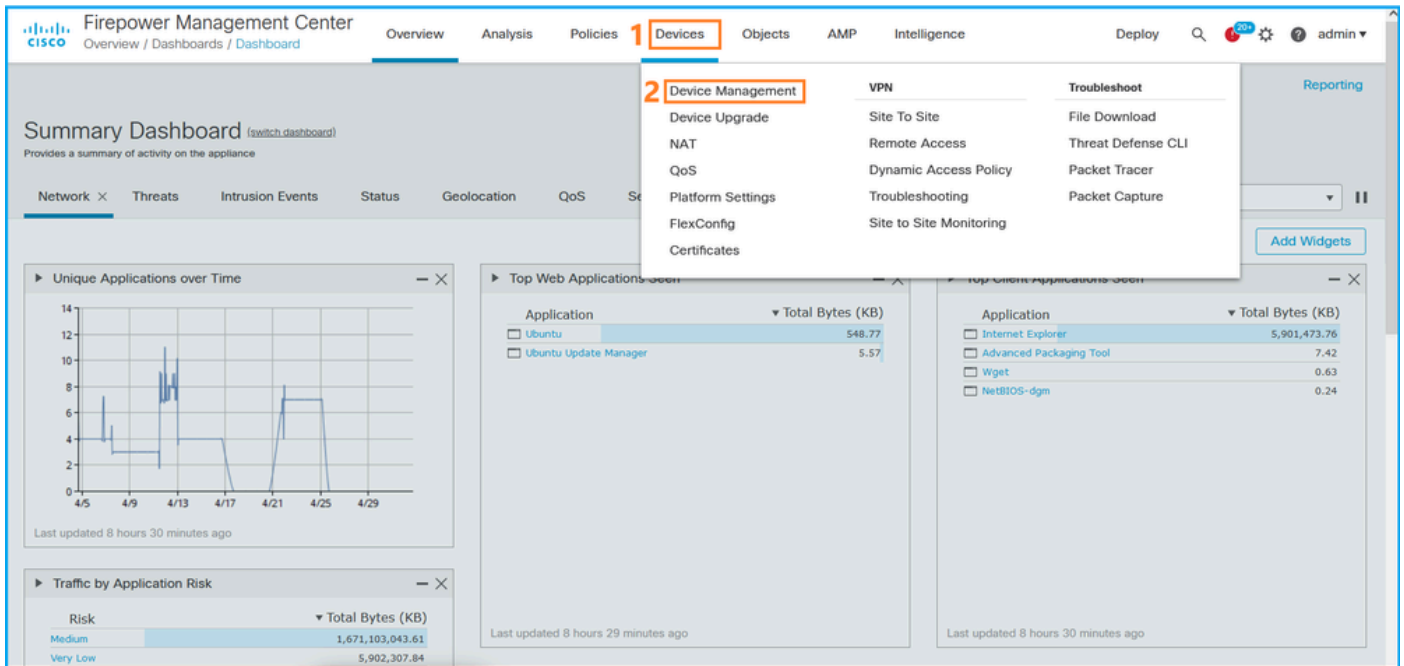
<#root>

```
#  
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)
```

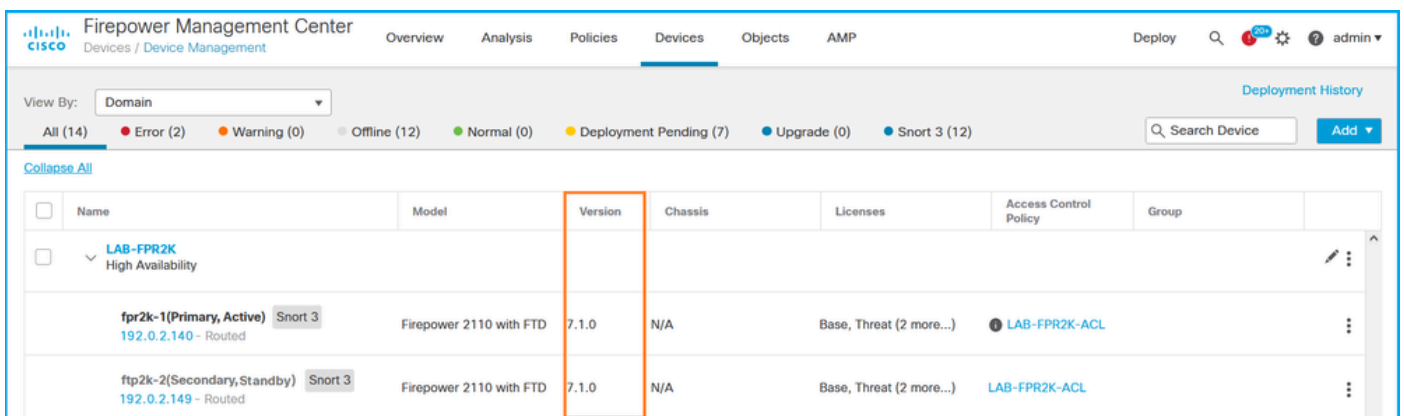
FMC UI

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

1. Choose **Devices > Device Management:**



2. Check the **Version** column:



FMC REST API

Complete 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:

```
<#root>
```

```
# curl -s -k -v -X POST 'https://192.0.2.1/api/fmc_platform/v1/auth/generatetoken' -H 'Authentication: Basic Ym9keS1hbnQ6Ym9keS1hbnQ='
```

```
< X-auth-access-token:
```

```
5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb
```

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:

```

<#root>

#
curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_platform/v1/info/domain' -H 'accept: application/json'

{
  "items": [
    {
      "name": "Global",
      "type": "Domain",
      "uuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f"
    },
    {
      "name": "Global/domain1",

"type": "Domain",
      "uuid": "ef0cf3e9-bb07-8f66-5c4e-000000000001"
    },
    {
      "name": "Global/domain2",
      "type": "Domain",
      "uuid": "341a8f03-f831-c364-b751-000000000001"
    }
  ],
  "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**:

```

<#root>

#
curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-000000000001/devicerecords' -H 'accept: application/json'

{
  "items": [
    {
      "id": "a4752f3c-86cc-11e9-8c9a-a3c958bed664",
      "links": {
        "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-000000000001/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-000000000001/devicerecords/05e9799c-94fc-11ea-ad33-a0032ddb0251"
      },
      "name": "fw1.lab.local",
      "type": "Device"
    }
  ]
}

```

```

    },
    "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-000000000000"
    },
    "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-000000000000"
    },
    "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-000000000000"
    },
    "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-000000000000"
    },
    "name": "fpr2k-1",
    "type": "Device"
  },

```

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

```

<#root>
#
curl -s -k -X GET 'https://192.0.2.1/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/device'
{
  "items": [
    {
      "commandInput": "show version",
      "commandOutput": "-----[ fpr2k-1 ]-----\nModel

Version 7.1.0 (Build 90)

\nUUID           : 0b1a9c94-8ba8-11ec-b2fd-93263934908d\nLSP version       : lsp-rel
      "type": "command"
    }
  ],

```

```
"links": {
  "self": "https://192.0.2.1/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/device",
},
"paging": {
  "count": 1,
  "limit": 25,
  "offset": 0,
  "pages": 1
}
```

FDM UI

Complete the steps in the section.

FDM REST-API

Complete the steps in the section.

FTD Troubleshoot file

Complete 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:**

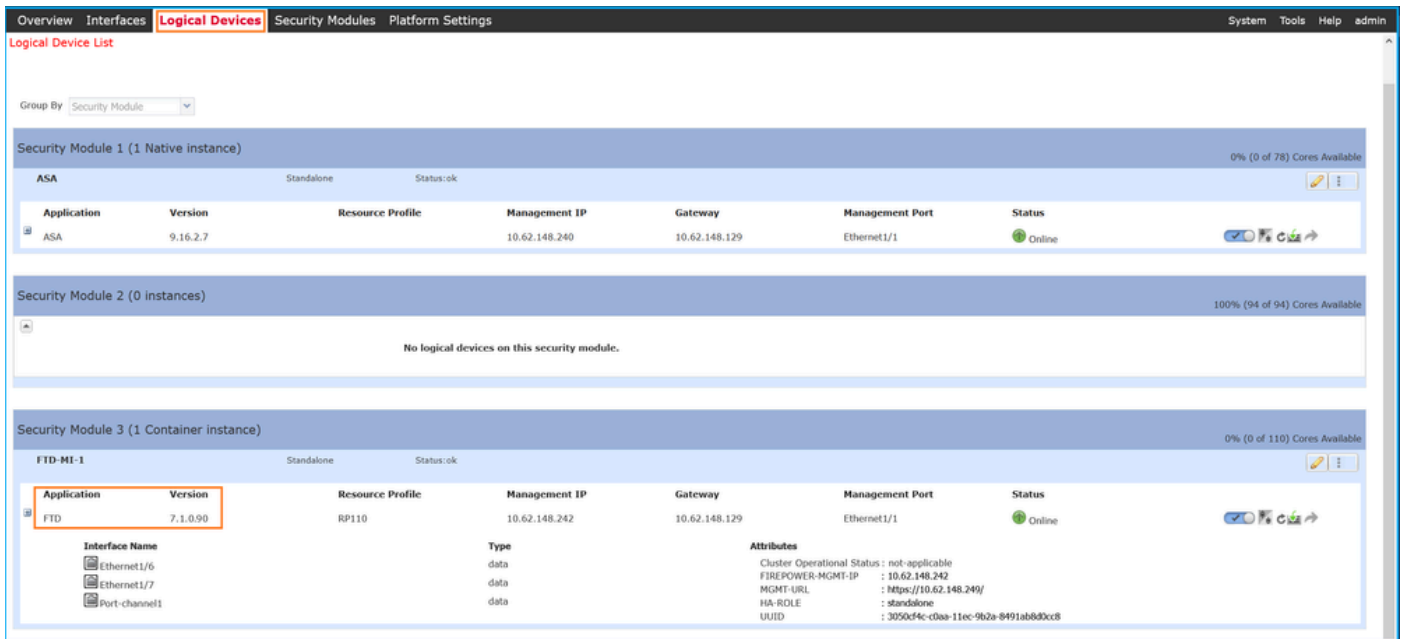
```
<#root>
#
pwd

/var/tmp/results-05-06-2022--199172/dir-archives/etc/sf/
#
cat
"
usr-local-sf-bin-sfcli.pl show version.output
"
-----[ 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
-----
```

FCM UI

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



FXOS CLI

FTD on Firepower 4100/9300

Complete 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:

```
<#root>
```

```
firepower#
```

```
scope ssa
```

```
firepower /ssa #
```

```
show app-instance
```

```
App Name      Identifier Slot ID      Admin State Oper State      Running Version Startup Version Deploy Ty
-----
asa           ASA           1              Enabled   Online          9.16.2.7      9.16.2.7      Native
ftd           FTD-MI-1
  3           Enabled      Online
7.1.0.90
              7.1.0.90      Container     No        RP110          Not Applicable None
```

FTD on Firepower 1000/2100/3100

Complete 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:

```
<#root>
>
connect fxos
```

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

```
<#root>
firepower#
scope ssa
firepower /ssa #
show app-instance
```

Application Name	Slot ID	Admin State	Operational State	Running Version	Startup Version	Default Version
ftd						
1	Enabled	Online				
7.1.0.90						
7.1.0.90	Native		Not Applicable	None		

FXOS REST-API

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

1. Request an authentication token:

```
<#root>
#
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:

```
<#root>
#
curl -s -k -X GET -H 'Accept: application/json' -H 'token: 28821660bc74e418f3fadc443619df0387d69e7b150e0
    "identifier": "
FTD-MI-1
",
    "runningVersion": "
7.1.0.90
",
    "hwCryptoVersion": "2",
    "startupVersion": "7.0.1.84",
    "versionIncompatibleErrorMgr": ""
```

FXOS Chassis show-tech file

Complete 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`**:

```
<#root>
# 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``:

```
<#root>
```

```
# pwd
```

```
/var/tmp/fp2k-1_FPRM/
```

```
# cat tech_support_brief
```

```
...  
`scope ssa`  
`show slot`
```

```
Slot:
```

Slot ID	Log Level	Admin State	Operational State
1	Info	Ok	Online

```
`show app`
```

```
Application:
```

Name	Version	Description	Author	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

Complete 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:

```
<#root>
```

```
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
```

```
Start-up time 1 sec
```

ASA SNMP

Complete 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:**

```
<#root>
```

#

```
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:

```
<#root>
```

```
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

Complete the steps in the section.

FXOS CLI

Complete the steps in the section.

FXOS REST-API

Complete the steps in the section.

FXOS Chassis show-tech file

Complete 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

Complete the steps in the section.

FMC REST-API

Complete the steps in the section.

Firepower Module CLI

Complete 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:

```
<#root>
>
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

Complete 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:**

```
<#root>
#
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
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**:

```
<#root>
asa#
show module sfr details

Getting details from 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:       0.0.0.0
Mgmt web ports:     443
Mgmt TLS enabled:   true
```

ASA show-tech file

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

```
<#root>
```

----- show module sfr detail -----

Getting details from 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: 0.0.0.0
Mgmt web ports: 443
Mgmt TLS enabled: true

Verify Snort, VDB, and SRU Versions

Deep Packet Inspection Engine (Snort) Version

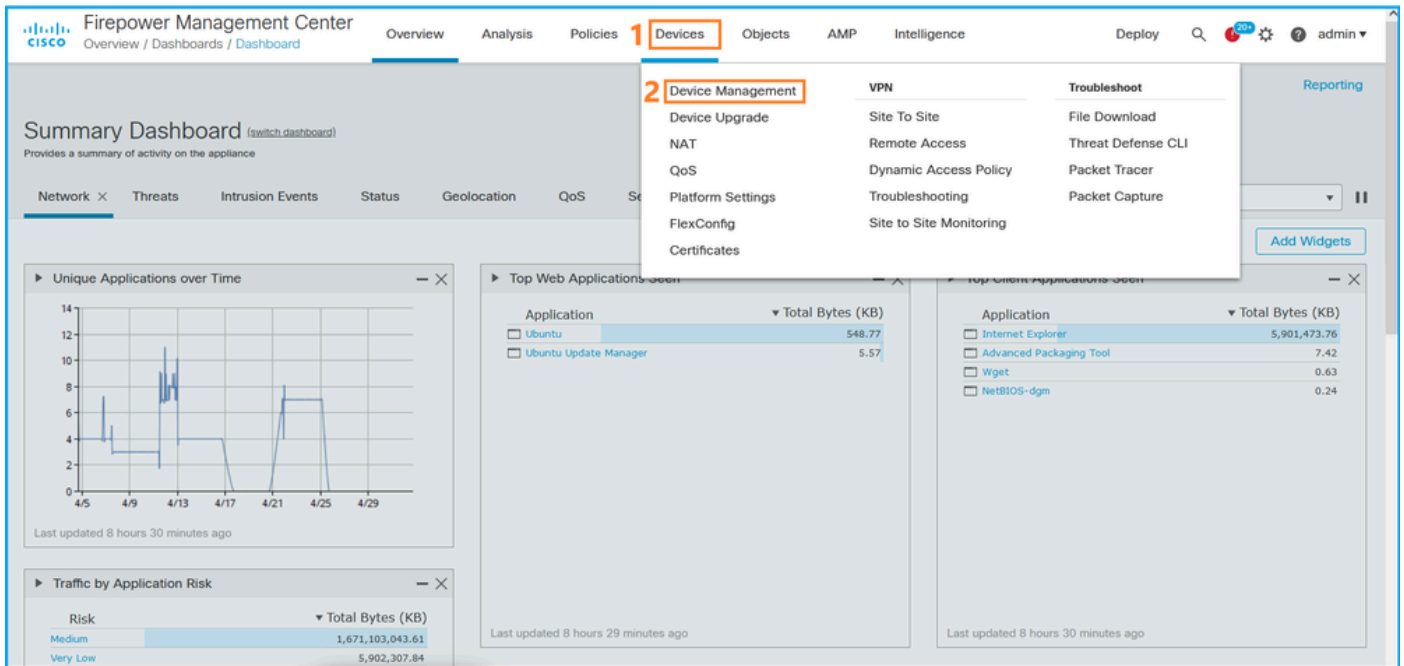
The Snort version can be verified with the use of these options:

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

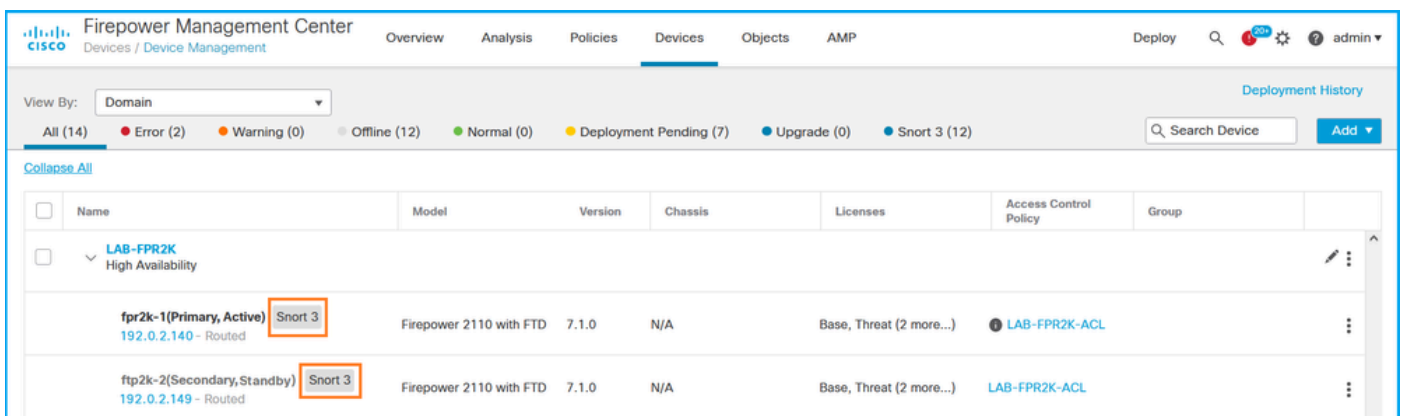
FMC UI

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

1. Choose **Devices > Device Management:**



2. Check the **Snort** label:



FMC REST-API

Complete 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:

```
<#root>
```

```
# curl -s -k -v -X POST 'https://192.0.2.1/api/fmc_platform/v1/auth/generatetoken' -H 'Authentication: Basic Ym9keS9kb290'
```

```
< X-auth-access-token:
```

```
5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb
```

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:

```

<#root>

#
curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_platform/v1/info/domain' -H 'accept: application/json'

{
  "items": [
    {
      "name": "Global",
      "type": "Domain",
      "uuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f"
    },
    {
      "name": "Global/domain1",
      "type": "Domain",
      "uuid": "ef0cf3e9-bb07-8f66-5c4e-000000000001"
    },
    {
      "name": "Global/domain2",
      "type": "Domain",
      "uuid": "341a8f03-f831-c364-b751-000000000001"
    }
  ],
  "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**:

```

<#root>

#
curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-000000000001/devicerecords' -H 'accept: application/json'

{
  "items": [
    {
      "id": "a4752f3c-86cc-11e9-8c9a-a3c958bed664",
      "links": {
        "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-000000000001/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-000000000001/devicerecords/05e9799c-94fc-11ea-ad33-a0032ddb0251"
      },
      "name": "fw1.lab.local",
      "type": "Device"
    }
  ]
}

```

```

    },
    "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-000000000000",
    },
    "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-000000000000",
    },
    "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-000000000000",
    },
    "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-000000000000",
    },
    "name": "fpr2k-1",
    "type": "Device"
  },

```

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

```
<#root>
```

```
#
```

```
curl -s -k -X GET 'https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-000000000001/device'
```

```

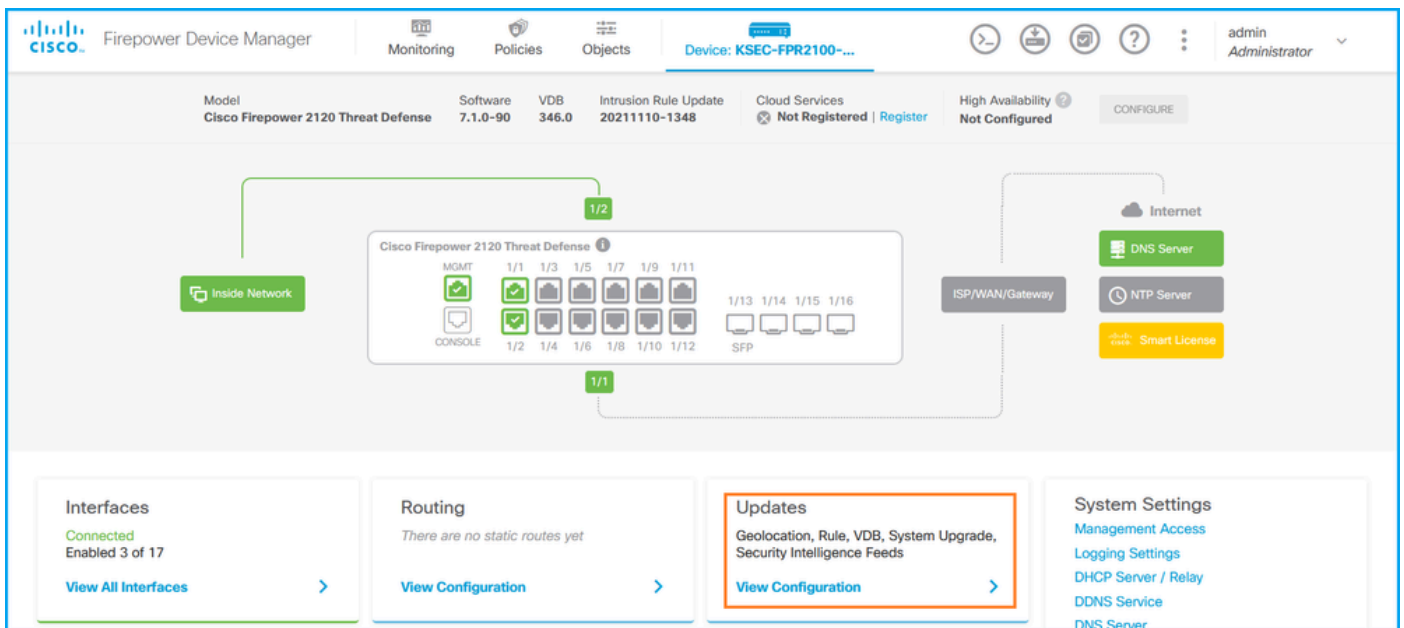
"snortVersion": "3.1.7.1-108",
"snortEngine": "SNORT3",

```

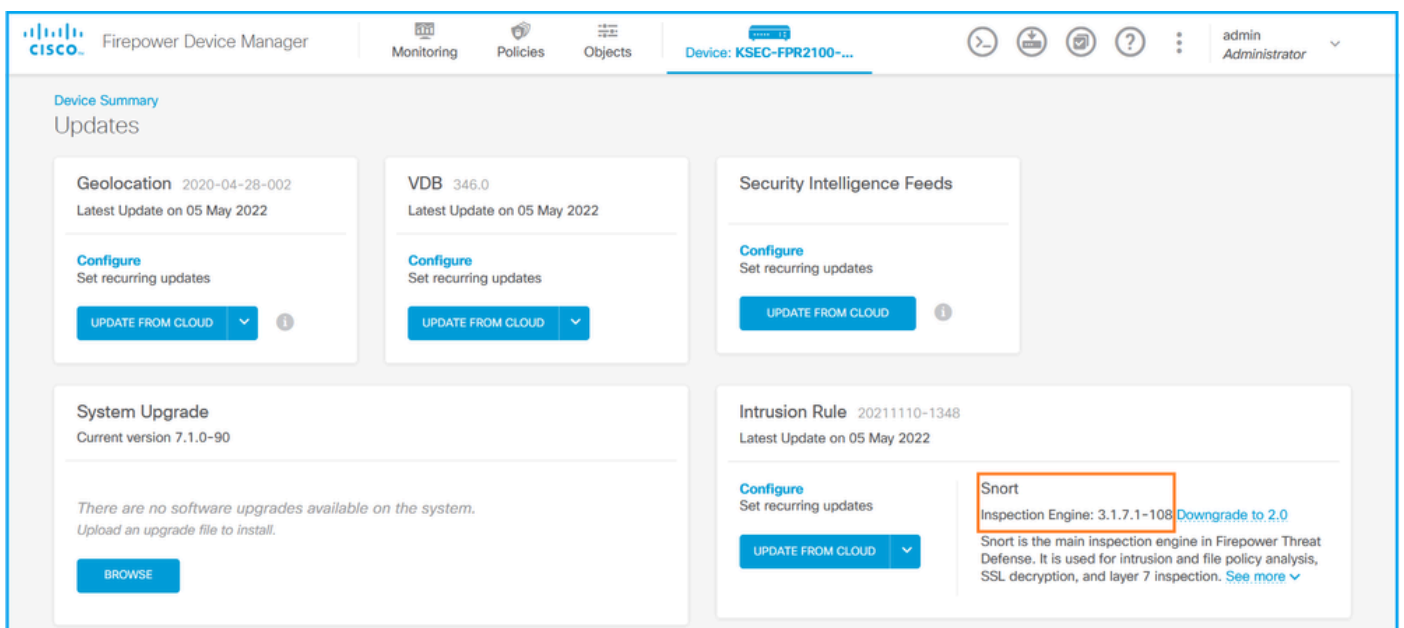
FDM UI

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

1. Go to the **Updates** page:



2. Check **Snort Inspection Engine**:



FDM REST API

Complete 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:

```
<#root>
```

```
#
curl -k -X POST --header 'Content-Type: application/json' --header 'Accept: application/json' -d '{ "grant_type": "password", "username": "admin", "password": "cisco12345" }' https://localhost:8443/oauth2/token

{
  "access_token": "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOiJlMjNTIyNDk5NTcsInN1YiI6ImFkbWluIiwianRpIjoiaW50aW50aW50aW50IiwiaXNjeXQiOiJhbnQ3MmRjNjAtZDBmMi0xMWVjLTk4ZW9kZW9keXNja3o",
  "expires_in": 1800,
  "refresh_expires_in": 2400,
  "refresh_token": "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOiJlMjNTIzOTQxNjksInN1YiI6ImFkbWluIiwianRpIjoiaW50aW50aW50aW50aW50",
  "token_type": "Bearer"
}
```

2. Use the **access_token** value in this query:

```
<#root>
#
curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOiJlMjNTIyNDk5NTcsInN1YiI6ImFkbWluIiwianRpIjoiaW50aW50aW50aW50IiwiaXNjeXQiOiJhbnQ3MmRjNjAtZDBmMi0xMWVjLTk4ZW9kZW9keXNja3o' https://localhost:8443/api/snort

{"snortVersion": {"snortVersion": "3.1.7.1-108", "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:

```
<#root>
>
show snort3 status
Currently running Snort 3
```

The Firepower module supports only Snort 2.

FTD or Firepower Module Troubleshoot file

Complete 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:**

```
<#root>
```

```
#
```

```
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

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

1. Choose **Help > About:**

Name	admin	No	No	🔍 ✎ 🗑️
Access Controlled User Statistics Provides traffic and intrusion event statistics by user				
Application Statistics Provides traffic and intrusion event statistics by application				
Application Statistics (7.1.0) Provides application statistics	admin	No	No	🔍 ✎ 🗑️
Connection Summary Provides tables and charts of the activity on your monitored network segment organized by different criteria	admin	No	No	🔍 ✎ 🗑️
Detailed Dashboard Provides a detailed view of activity on the appliance	admin	No	No	🔍 ✎ 🗑️
Detailed Dashboard (7.0.0) Provides a detailed view of activity on the appliance	admin	No	No	🔍 ✎ 🗑️
Files Dashboard Provides an overview of Malware and File Events	admin	No	No	🔍 ✎ 🗑️
Security Intelligence Statistics Provides Security Intelligence statistics	admin	No	No	🔍 ✎ 🗑️
Summary Dashboard Provides a summary of activity on the appliance	admin	No	Yes	🔍 ✎ 🗑️

2. Check VDB Version:

Model	Cisco Firepower Management Center 4600
Serial Number	001234
Software Version	7.1.0 (build 90)
OS	Cisco Firepower Extensible Operating System (FX-OS) 2.11.1 (build154)
Snort Version	2.9.19 (Build 92)
Snort3 Version	3.1.7.1 (Build 108)
Rule Update Version	2022-05-02-003-vrt
Rulepack Version	2703
Module Pack Version	3070
LSP Version	lsp-rel-20220502-1613
Geolocation Update Version	2022-04-25-002
VDB Version	build 354 (2022-04-27 19:39:56)
Hostname	FMC-4600-2

For technical/system questions, e-mail tac@cisco.com or call us at 1-800-553-2447 or 1-408-526-7209

Copyright 2004-2021, Cisco and/or its affiliates. All rights reserved.

FMC CLI

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

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

```
<#root>
```

```
>
```

```
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

Complete 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:

<#root>

```
# curl -s -k -v -X POST 'https://192.0.2.1/api/fmc_platform/v1/auth/generatetoken' -H 'Authentication: B
```

< X-auth-access-token:

```
7acdb34c-ea85-47bf-83fe-d77b63f012da
```

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:

<#root>

#

```
curl -s -k -X GET 'https://192.0.2.1/api/fmc_platform/v1/info/serverversion' -H 'X-auth-access-token: 7a
```

```
{
  "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

Complete 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`:

```
<#root>
```

```
#
```

```
pwd
```

```
/var/tmp/results-05-06-2022--199172/dir-archives/etc/sf/.versiondb
```

```
#
```

```
cat vdb.conf
```

```
CURRENT_VERSION=4.5.0
```

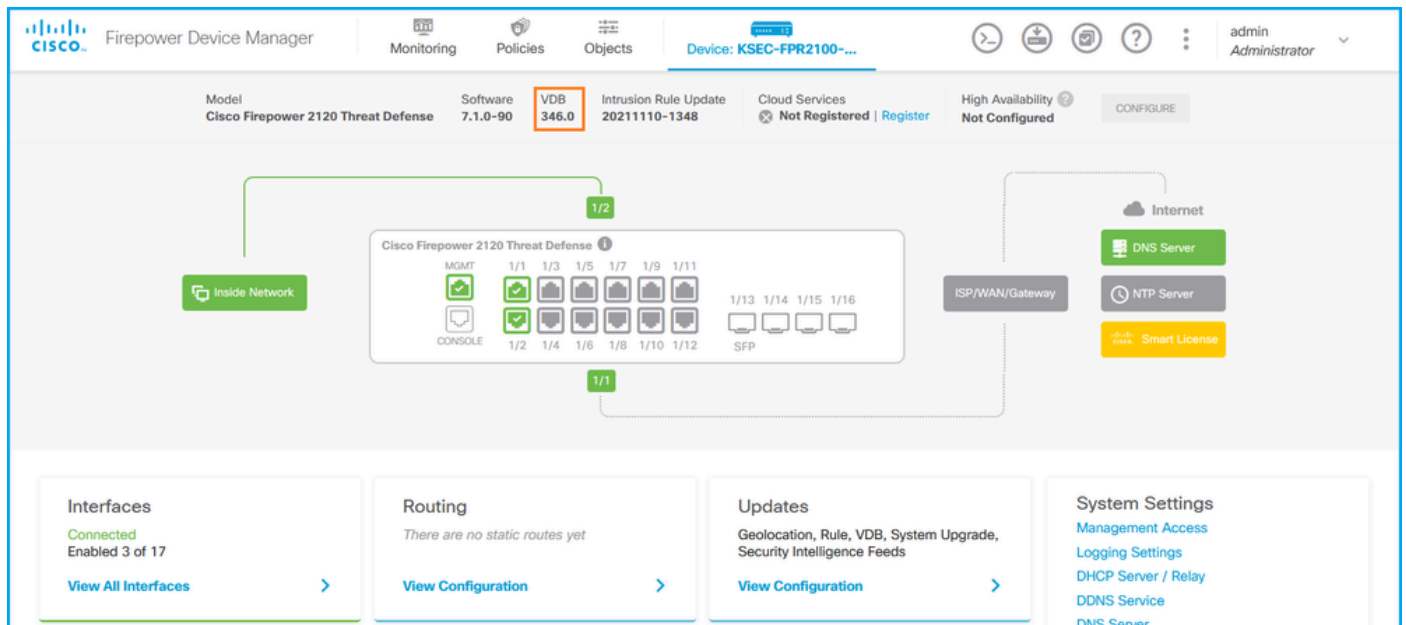
```
CURRENT_BUILD=344
```

```
CURRENT_APPID_VER=82
```

```
CURRENT_NAVL_VER=106
```

FDM UI

On the main page check **VDB**:



FDM REST API

Complete 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:

```
<#root>

#

curl -k -X POST --header 'Content-Type: application/json' --header 'Accept: application/json' -d '{ "grant_type": "password", "username": "admin", "password": "admin", "scope": "vdb:read vdb:write" }'

{
  "access_token": "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIyNTk5NDk5NTcsInN1YiI6ImFkbWl1IiwianRpIjoiaNDk3MmRjNjAtZDBmMi0xMWVjLTk4ZWUyODIiLCJ0eXciOiJ0eXciLCJ1b2wiOiJ0eXciLCJpcyI6ImFkbWl1IiwiaWF0IjoiMjAyMi00NS0wNSJ9",
  "expires_in": 1800,
  "refresh_expires_in": 2400,
  "refresh_token": "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIyNTk5NDk5NTcsInN1YiI6ImFkbWl1IiwianRpIjoiaGU0NGI0MmRjNjAtZDBmMi0xMWVjLTk4ZWUyODIiLCJ0eXciOiJ0eXciLCJ1b2wiOiJ0eXciLCJpcyI6ImFkbWl1IiwiaWF0IjoiMjAyMi00NS0wNSJ9",
  "token_type": "Bearer"
}
```

2. Use the **access_token** value in this query:

```
<#root>

#

curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIyNTk5NDk5NTcsInN1YiI6ImFkbWl1IiwianRpIjoiaNDk3MmRjNjAtZDBmMi0xMWVjLTk4ZWUyODIiLCJ0eXciOiJ0eXciLCJ1b2wiOiJ0eXciLCJpcyI6ImFkbWl1IiwiaWF0IjoiMjAyMi00NS0wNSJ9'

{
  "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

Complete 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:

```
<#root>

>

show 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
```

```
<#root>
```

```
>
```

```
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
```

FTD or Firepower Module Troubleshoot file

Complete 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**:

```
<#root>
```

```
#
```

```
pwd
```

```
/var/tmp/results-05-06-2022--163203/command-outputs/
#
```

```
cat "usr-local-sf-bin-sfcli.pl show version.output"
```

```
-----[ 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
```

```
<#root>
```

```
#
```

```
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
VDB version          :
354
-----
```

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

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

1. Choose **Help > About:**

Name				
Access Controlled User Statistics Provides traffic and intrusion event statistics by user				
Application Statistics Provides traffic and intrusion event statistics by application				
Application Statistics (7.1.0) Provides application statistics	admin	No	No	
Connection Summary Provides tables and charts of the activity on your monitored network segment organized by different criteria	admin	No	No	
Detailed Dashboard Provides a detailed view of activity on the appliance	admin	No	No	
Detailed Dashboard (7.0.0) Provides a detailed view of activity on the appliance	admin	No	No	
Files Dashboard Provides an overview of Malware and File Events	admin	No	No	
Security Intelligence Statistics Provides Security Intelligence statistics	admin	No	No	
Summary Dashboard Provides a summary of activity on the appliance	admin	No	Yes	

2. Check Rule Update Version and LSP Version:

Model	Cisco Firepower Management Center 4600
Serial Number	001234
Software Version	7.1.0 (build 90)
OS	Cisco Firepower Extensible Operating System (FX-OS) 2.11.1 (build154)
Snort Version	2.9.19 (Build 92)
Snort3 Version	3.1.7.1 (Build 108)
Rule Update Version	2022-05-02-003-vrt
Rulepack Version	2703
Module Pack Version	3070
LSP Version	lsp-rel-20220502-1613
Geolocation Update Version	2022-04-25-002
VDB Version	build 354 (2022-04-27 19:39:56)
Hostname	FMC-4600-2

FMC CLI

Complete 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:

```
<#root>
```

```
>
```

```
show version
```

```
-----[ FMC-4600-2.cisco.com ]-----
```

```
Mode] : 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

Complete 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:

```
<#root>
#
curl -s -k -v -X POST 'https://192.0.2.1/api/fmc_platform/v1/auth/generatetoken' -H 'Authentication: Ba
<
X-auth-access-token: 9408fe38-c25c-4472-b7e6-3571bb4e2b8d
```

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

```
<#root>
#
curl -s -k -X GET 'https://192.0.2.1/api/fmc_platform/v1/info/serverversion' -H 'X-auth-access-token: 7a
{
  "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

Complete 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>--xxxxxx/dir-archives/etc/sf/**
2. Open the file **sru_versions.conf** and find the lines with keys **Intrusion_Rules_Update**:

```
<#root>
#
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
```

Complete 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-lsp**

```
<#root>
#
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
19142268      0 lrwxrwxrwx   1 root     root      33 May 11 04:00 /var/sf/lsp/installed-lsp -> /
19138299      4 drwxrwxr-x   5 www      root      4096 May 11 04:01 /var/sf/lsp/lsp-rel-20220510-1
19142266     600 -rwxrwxr-x   1 www      root     614400 May 10 14:55 /var/sf/lsp/lsp-rel-20220510-1
19142234      4 drwxrwxr-x   5 www      root      4096 May 11 04:00 /var/sf/lsp/lsp-rel-20220510-1
19268898      4 drwxrwxr-x   2 www      root      4096 May 10 14:55 /var/sf/lsp/lsp-rel-20220510-1
19138303      4 drwxrwxr-x   6 www      root      4096 May 10 14:51 /var/sf/lsp/lsp-rel-20220510-1
19142269    46640 -rw-r--r--   1 root     root    47759360 May 11 04:01 /var/sf/lsp/lsp-rel-20220510-1
19142267      4 -rwxrwxr-x   1 www      root      238 May 11 04:00 /var/sf/lsp/lsp-rel-20220510-1
```



```
}
```

2. Use the **access_token** value in this query:

```
<#root>
```

```
#
```

```
curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOi
```

```
"sruVersion" : {
```

```
"sruVersion" : "20211110-1348",
```

```
"lastSuccessSRUDate" : "2022-05-12 18:29:00Z",
```

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

```
"type" : "sruversion"
```

FTD or Firepower Module CLI

Complete these steps to verify SRU/LSP 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 **show version** command on CLI:

```
<#root>
```

```
>
```

```
show version
```

```
-----[ FIREPOWER1.cisco.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  
-----
```

```
or
```

```
>
```

```
show version
```

```
-----[ 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
```

```
<#root>
```

```
>
```

```
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

Complete 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/**
2. Open the file **usr-local-sf-bin-sfcli.pl show version.output** and find the line with **SRU/LSP** version:

```
<#root>
```

```
# pwd
```

```
/var/tmp/results-05-06-2022--163203/command-outputs/  
#
```

```
cat "usr-local-sf-bin-sfcli.pl show version.output"
```

```
-----[ FIREPOWER1.cisco.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  
-----
```

```
or
```

```
# pwd
```

```
/var/tmp/results-05-06-2022--163203/command-outputs/
```

```
#
cat "usr-local-sf-bin-sfcli.pl show version.output"
-----[ FIREPOWER1.cisco.com ]-----
Model                : Cisco Firepower 2120 Threat Defense (77) Version 7.1.0 (Build 90)
UUID                 : 70727d06-8ba7-11ec-bfcc-999f61f27102
Rules update version : 2022-05-11-001-vrt
VDB version          : 346
-----
```

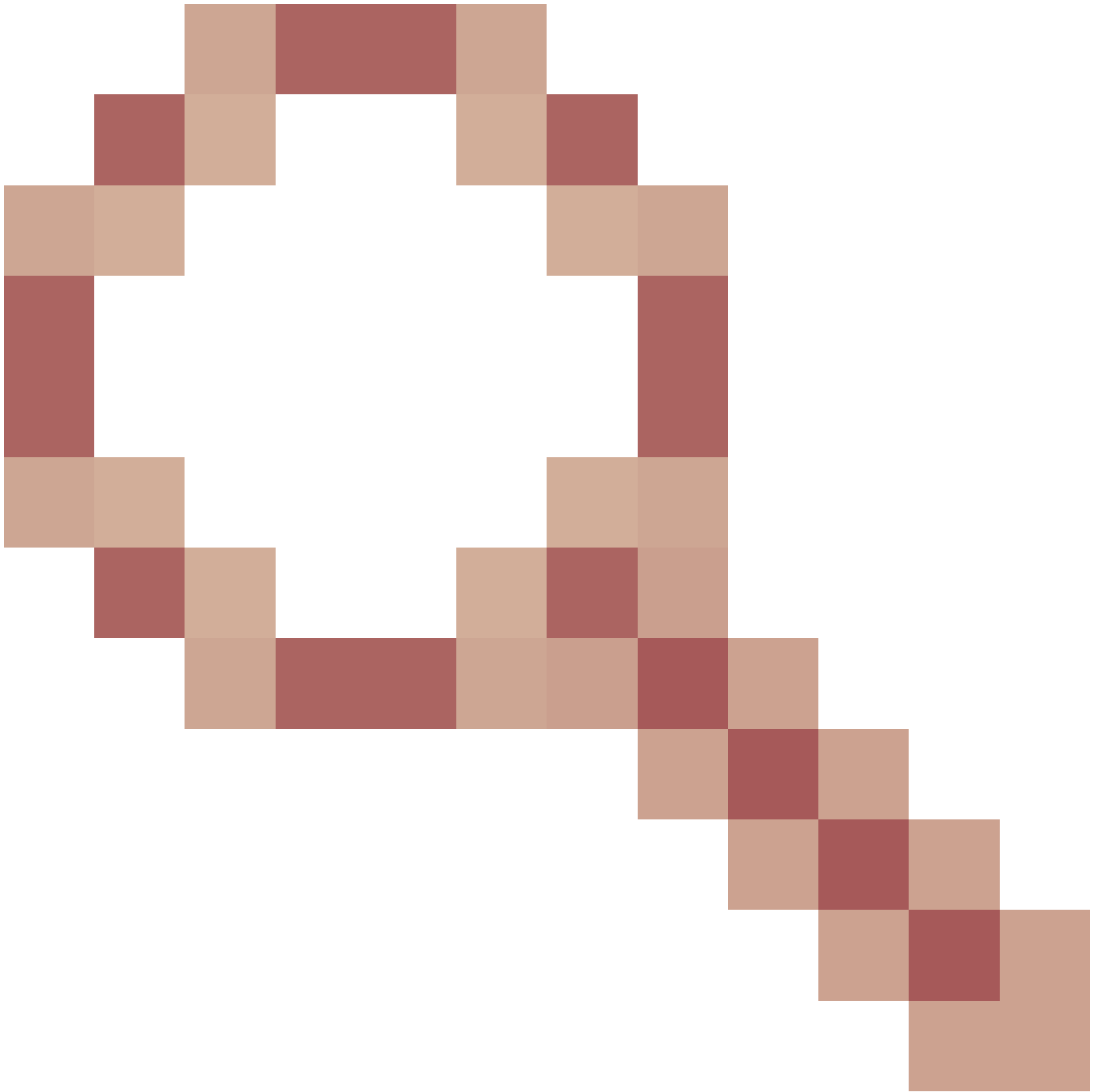
<#root>

```
#
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
VDB version          : 354
-----
```

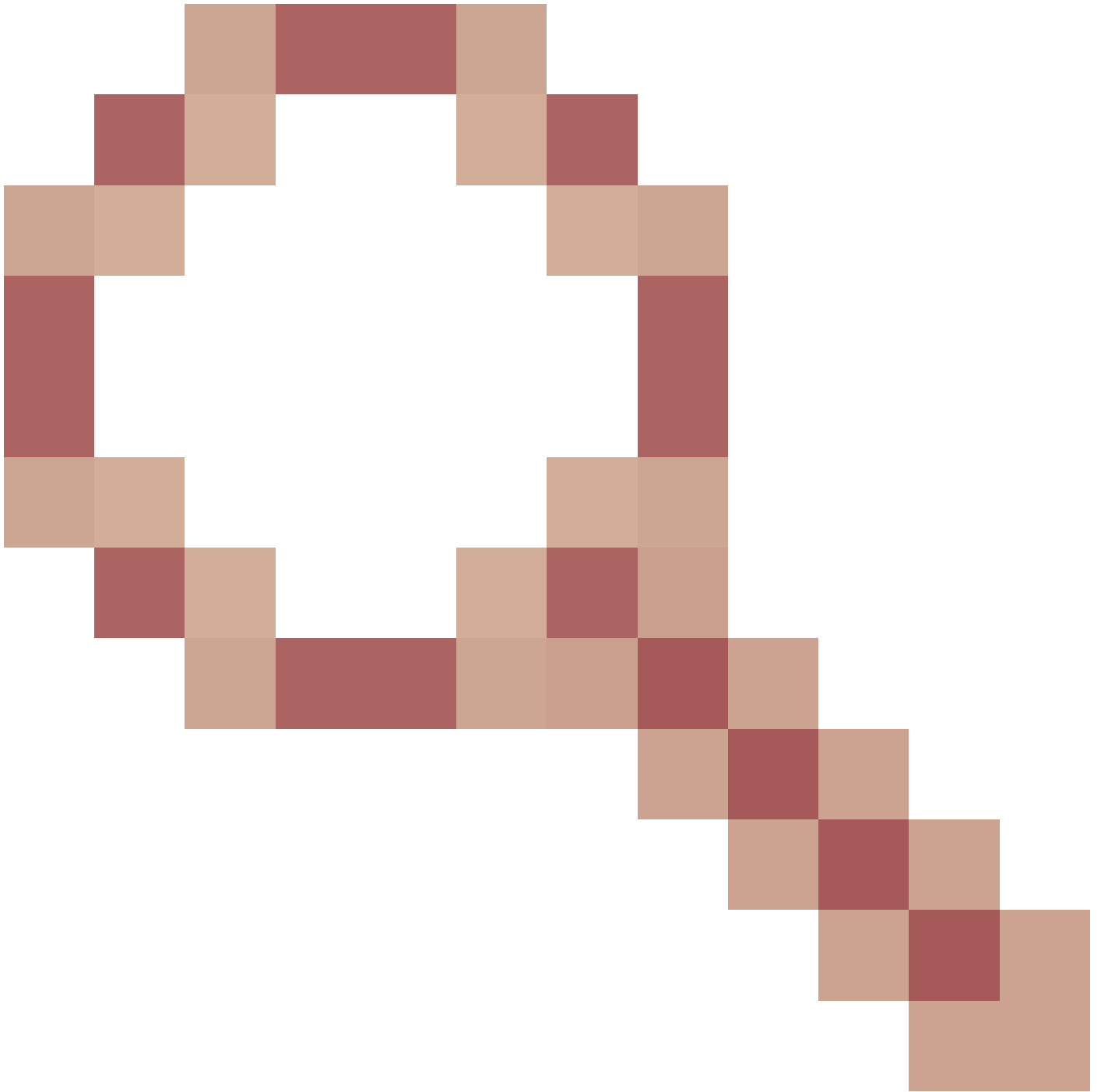
Known Issues

Cisco bug ID [CSCwb34098](#)



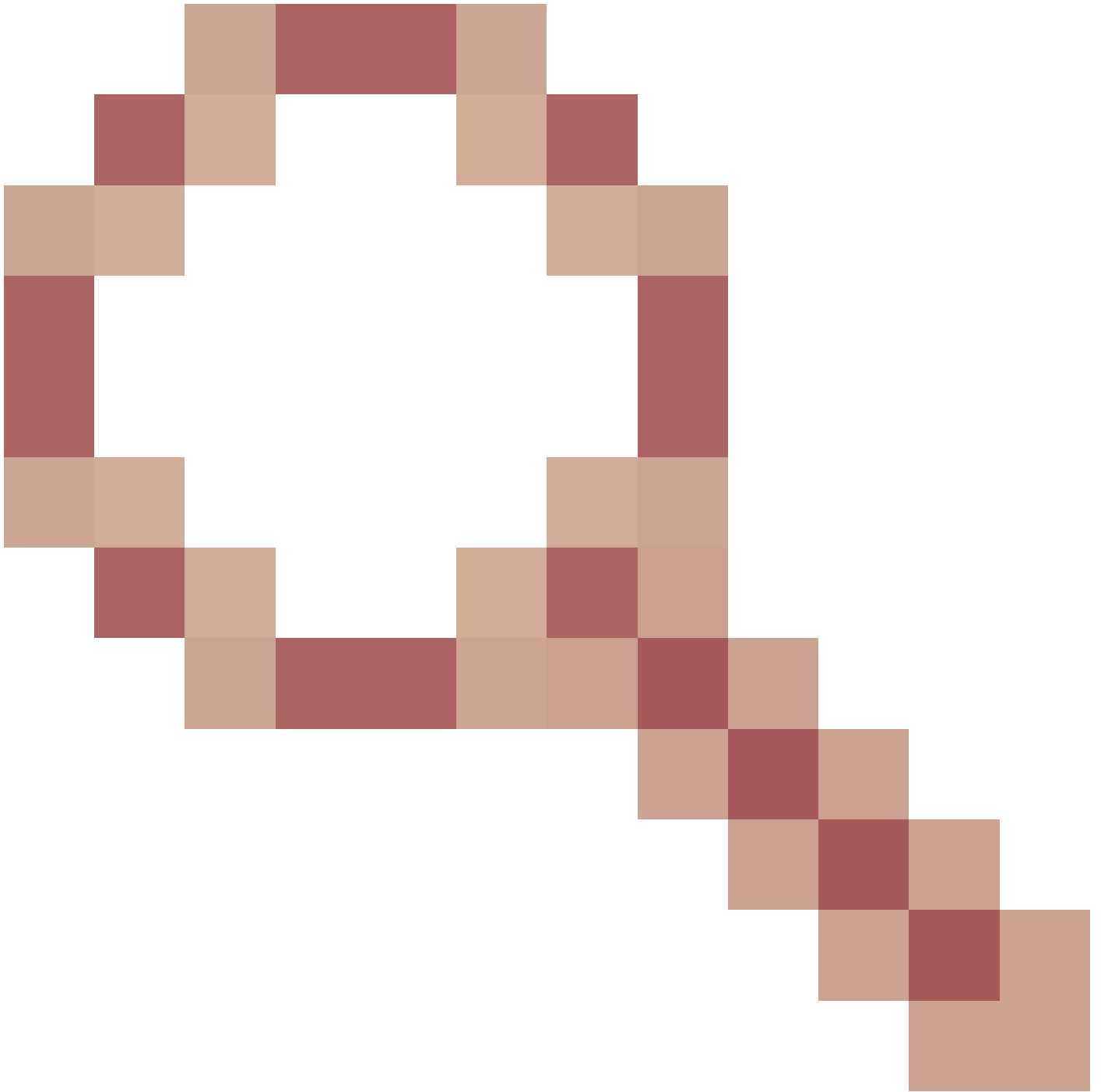
ENH: Show FMC version in 'show managers' command output

Cisco bug ID [CSCve13470](#)



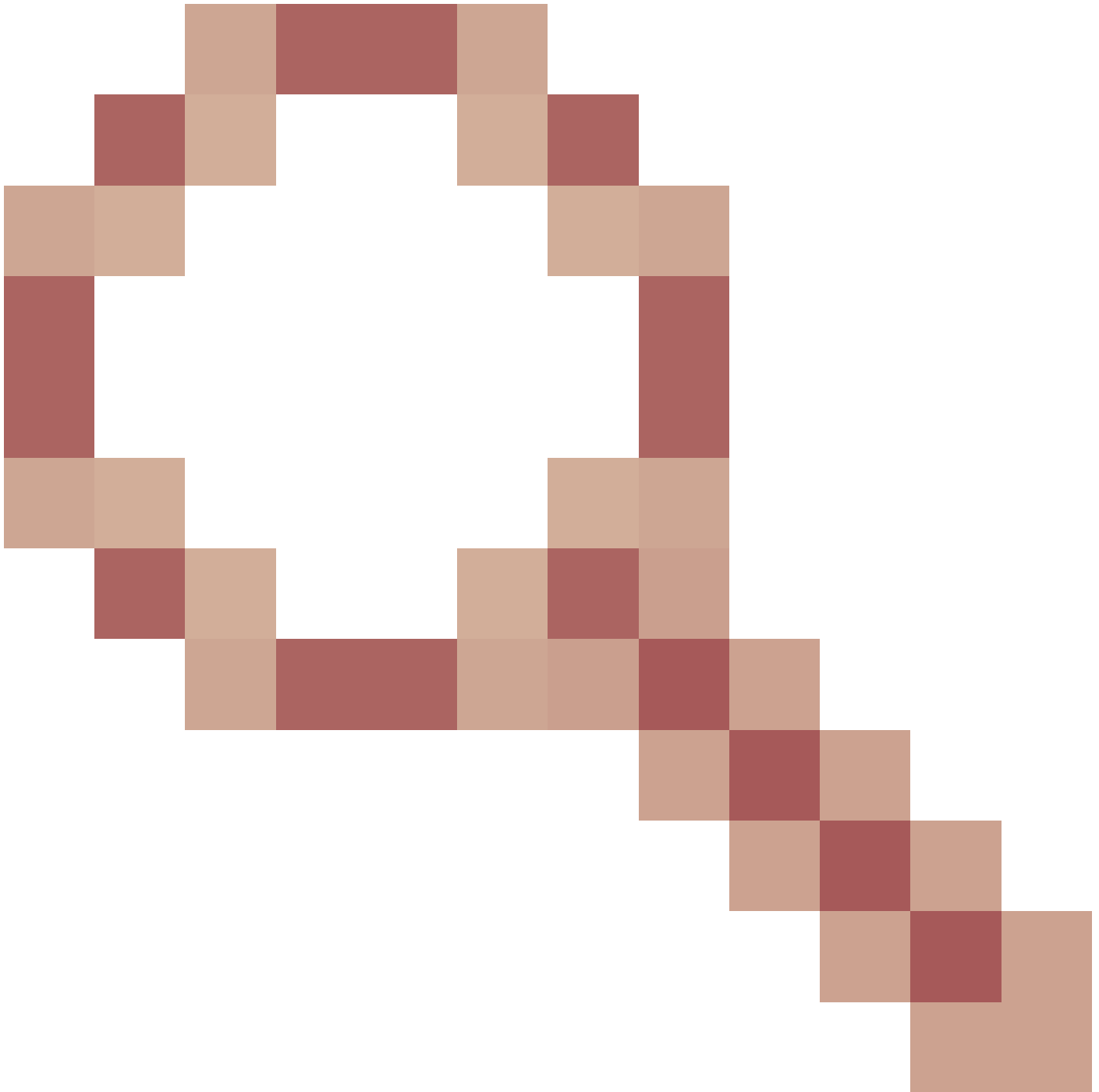
ENH: Enable Software Related OIDs on FirePOWER 6.x

Cisco bug ID [CSCwb85969](#)



ENH: Include output of "show version" FMC CLISH command in troubleshoot file

Cisco bug ID [CSCvu15709](#)



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](#)
- [Configure SNMP on Firepower NGFW Appliances](#)
- [Cisco Firepower Threat Defense REST API Guide](#)
- [Cisco FXOS REST API Reference](#)
- [Cisco ASA Compatibility](#)
- [Firepower 1000/2100 and Secure Firewall 3100 ASA and FXOS Bundle Versions](#)
- [Bundled Components](#)
- [Firepower Troubleshoot File Generation Procedures](#)