

# Überprüfen Sie die Firepower-Softwareversionen

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Softwareversionen überprüfen](#)

[FMC-Softwareversion](#)

[FMC-Benutzeroberfläche](#)

[FMC-CLI](#)

[FMC REST-API](#)

[FMC-Fehlerbehebungsdatei](#)

[FTD- oder FirePOWER-Modul-CLI](#)

[FTD- oder FirePOWER-Modul Fehlerbehebungsdatei](#)

[FDM-Softwareversion](#)

[FDM-Benutzeroberfläche](#)

[FDM REST-API](#)

[FTD-CLI](#)

[FTD-SNMP](#)

[FTD Fehlerbehebungsdatei](#)

[FXOS-Softwareversion](#)

[FCM-Benutzeroberfläche](#)

[FXOS-CLI](#)

[FXOS REST-API](#)

[FXOS-SNMP](#)

[FXOS-Chassis-Show-Tech-Datei](#)

[FTD-Softwareversion](#)

[FTD-CLI](#)

[FTD-SNMP](#)

[FMC-Benutzeroberfläche](#)

[FMC REST-API](#)

[FDM-Benutzeroberfläche](#)

[FDM REST-API](#)

[FTD-Fehlerbehebungsdatei](#)

[FCM-Benutzeroberfläche](#)

[FXOS-CLI](#)

[FXOS REST-API](#)

[FXOS-Chassis-Show-Tech-Datei](#)

[ASA Softwareversion](#)

[ASA-CLI](#)

[ASA-SNMP](#)

[ASA-Showtech-Datei](#)

[FCM-Benutzeroberfläche](#)  
[FXOS-CLI](#)  
[FXOS REST-API](#)  
[FXOS-Chassis-Show-Tech-Datei](#)  
[Softwareversion des FirePOWER-Moduls](#)  
[FMC-Benutzeroberfläche](#)  
[FMC REST-API](#)  
[FirePOWER-Modul-CLI](#)  
[Fehlerbehebungsdatei für das FirePOWER-Modul](#)  
[ASA-CLI](#)  
[ASA-Showtech-Datei](#)  
[Überprüfen der Versionen Snort, VDB und SRU](#)  
[Deep Packet Inspection Engine \(Snort\)-Version](#)  
[FMC-Benutzeroberfläche](#)  
[FMC REST-API](#)  
[FDM-Benutzeroberfläche](#)  
[FDM REST-API](#)  
[FTD oder FirePOWER CLI](#)  
[FTD- oder FirePOWER-Modul Fehlerbehebungsdatei](#)  
[VDB-Version \(Vulnerability Database\)](#)  
[FMC-Benutzeroberfläche](#)  
[FMC-CLI](#)  
[FMC REST-API](#)  
[FMC-Fehlerbehebungsdatei](#)  
[FDM-Benutzeroberfläche](#)  
[FDM REST-API](#)  
[FTD- oder FirePOWER-Modul-CLI](#)  
[FTD- oder FirePOWER-Modul Fehlerbehebungsdatei](#)  
[Aktualisierungsversionen für Angriffsregeln](#)  
[FMC-Benutzeroberfläche](#)  
[FMC-CLI](#)  
[FMC REST-API](#)  
[FMC-Fehlerbehebungsdatei](#)  
[FDM-Benutzeroberfläche](#)  
[FDM REST-API](#)  
[FTD- oder FirePOWER-Modul-CLI](#)  
[FTD- oder FirePOWER-Modul Fehlerbehebungsdatei](#)  
[Bekannte Probleme](#)  
[Zugehörige Informationen](#)

## **Einleitung**

Dieses Dokument beschreibt die Verifizierung von Firepower-Softwareversionen.

## **Voraussetzungen**

## Anforderungen

Grundlegende Produktkenntnisse, REST-API, SNMP.

## Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

## Softwareversionen überprüfen

### FMC-Softwareversion

Die FMC-Softwareversion kann mithilfe der folgenden Optionen überprüft werden:

- FMC-Benutzeroberfläche
- FMC-CLI
- REST-API-Anforderung
- FMC-Fehlerbehebungsdatei
- FTD- oder FirePOWER-Modul-CLI
- FTD- oder FirePOWER-Modul zur Fehlerbehebung

### FMC-Benutzeroberfläche

Gehen Sie folgendermaßen vor, um die FMC-Softwareversion auf der FMC-Benutzeroberfläche zu überprüfen:

1. Wählen Sie **Hilfe > Info**:

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. Softwareversion überprüfen:

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

Befolgen Sie diese Schritte, um die FMC-Softwareversion auf der FMC-CLI zu überprüfen.

1. Zugriff auf FMC über SSH oder Konsolenverbindung. Das Banner zeigt die Softwareversion an:

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

2. Führen Sie den Befehl **show version** auf CLI aus:

```
> 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

Befolgen Sie diese Schritte, um die FMC-Softwareversion über eine FMC REST-API-Anfrage zu überprüfen. Verwenden Sie einen REST-API-Client, um die Softwareversion zu überprüfen. In diesem Beispiel wird **curl** verwendet:

### 1. Authentifizierungstoken anfordern:

```
# 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. Verwenden Sie das X-auth-access-Token in dieser Abfrage:

```
# 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
  }
}
```

**Anmerkung:** Der Teil "`| python -m json.tool`" der Befehlszeichenfolge dient zur Formatierung der Ausgabe im JSON-Stil und ist optional.

## FMC-Fehlerbehebungsdatei

Gehen Sie folgendermaßen vor, um die FMC-Softwareversion in der Fehlerbehebungsdatei zu überprüfen:

1. Öffnen Sie die Fehlerbehebungsdatei, und navigieren Sie zum Ordner `<Dateiname>.tar/results-<date>—xxxxxx/dir-archives/etc/sf/`.
2. Öffnen Sie die Datei `ims.conf` und suchen Sie die Zeilen mit den Schlüsseln **SWVERSION** und **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- oder FirePOWER-Modul-CLI

Gehen Sie folgendermaßen vor, um die FMC-Softwareversion auf der FTD-CLI oder der FirePOWER-Modul-CLI zu überprüfen:

1. Zugriff auf FTD über SSH oder Konsolenverbindung. Im Fall des FirePOWER-Moduls greifen Sie über SSH auf das Modul oder über den Befehl **session sfr** von der ASA CLI zu.
2. Führen Sie den Befehl **experte** aus.

```
> expert
admin@fpr2k-1:~$
```

3. Führen Sie den Befehl **less /ngfw/var/sf/detect\_engines/<UUID>/ngfw.rules** auf FTD oder **weniger /var/sf/detect\_engines/<UUID>/ngfw.rules** auf dem Firepower-Modul aus, und überprüfen Sie die Zeile **DC-Version**:

```
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- oder FirePOWER-Modul Fehlerbehebungsdatei

Führen Sie die folgenden Schritte aus, um die FMC-Softwareversion in der FTD- oder FirePOWER-Modul-Fehlerbehebungsdatei zu überprüfen:

1. Öffnen Sie die Fehlerbehebungsdatei, und navigieren Sie zum Ordner **<Dateiname>-troubleshoot.tar/results-<date>—xxxxxx/file-content/ngfw/var/sf/detect\_engines/<UUID>/**, wenn die Datei in FTD generiert wurde. Navigieren Sie für das FirePOWER-Modul zum Ordner **<Dateiname>-troubleshoot.tar/results-<date>—xxxxxx/file-content/var/sf/detect\_engines/<UUID>/**
2. Öffnen Sie die **Datei ngfw.rules**, und überprüfen Sie die Zeile **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 #####
#
# 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
#
```

#####  
...

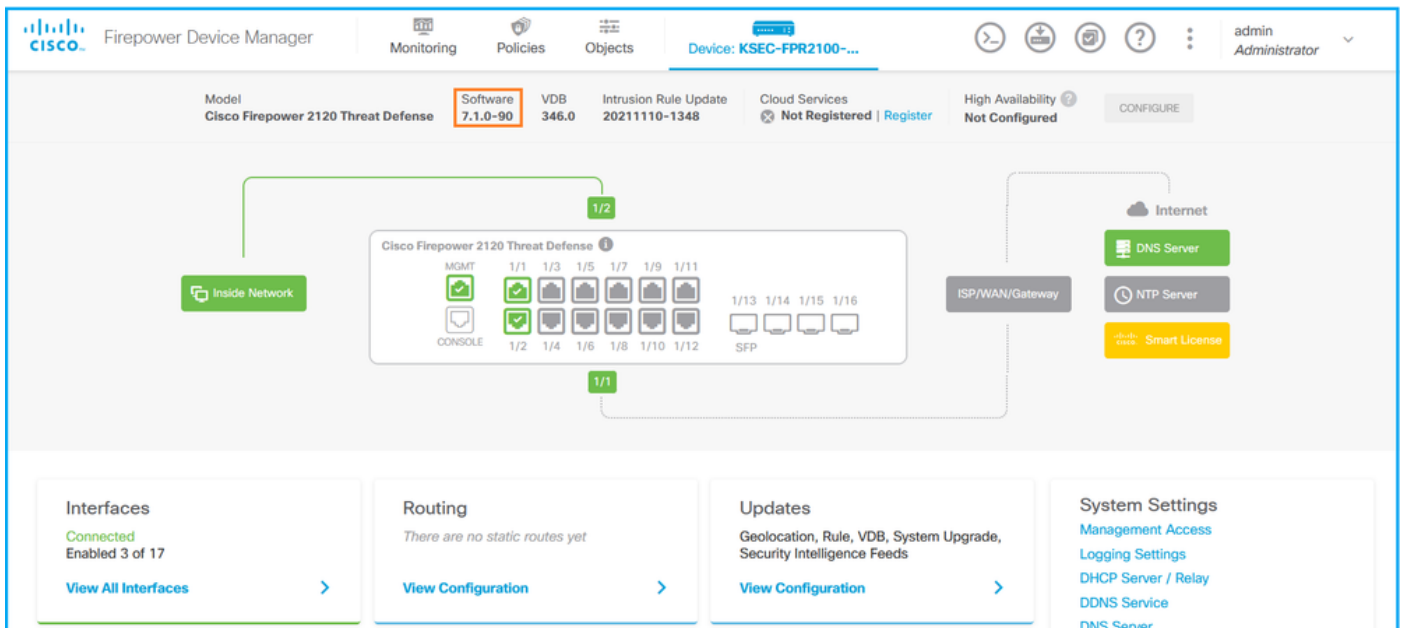
## FDM-Softwareversion

Die FDM-Softwareversion kann mithilfe der folgenden Optionen verifiziert werden:

- FDM-Benutzeroberfläche
- FTD-CLI
- FTD-SNMP-Umfrage
- FTD-Fehlerbehebungsdatei
- FDM REST-API
- FCM-Benutzeroberfläche (FirePOWER Chassis Manager)
- FXOS-CLI
- FXOS REST-API
- FXOS-Chassis-Show-Tech-Datei

## FDM-Benutzeroberfläche

So überprüfen Sie die Softwareversion auf der FDM-Benutzeroberfläche auf der Hauptseite **Software**:



## FDM REST-API

Befolgen Sie diese Schritte, um die FDM-Softwareversion über eine FDM-REST-API-Anfrage zu überprüfen. Verwenden Sie einen REST-API-Client, um die Softwareversion zu überprüfen. In diesem Beispiel wird curl verwendet:

1. Authentifizierungstoken anfordern:

```
# 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.eyJpYXQiOjE2NTIyNDk5NTcsInN1YiI6ImFkbWluIiwianRpIjojNDk3MmRjNjAtZDBmMi0xMWVjLTk4ZWMtNDdlZTQwODkwMDVjIiwibmJmIjoxNjUyMjQ5OTU3LCJleHAiOjE2NTIyNTE3NTcsInJlZnJlc2hUb2t1bkV4cGlyZXNbdCI6MTY1MjI1MjM1NzQ1NywidG9rZW5UeXB1Ijois1dUX0FjY2VzcyIsInVzZXJvdWlkIjoiyTU3ZGVmMjgtY2M3MC0xMWVjLTk4ZWMtZjk4ODExNjNjZWlwiwidXN1c1JvbGUiOiJST0xFOX0FETU0Iiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2VybmFtZSI6ImFkbWluIn0.1JLmHddJ2jaVRmpdXF6gg48qdBcyRuit94DLobCJ9LI" ,
"expires_in": 1800,
"refresh_expires_in": 2400,
"refresh_token":
"eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIyOTQxNjksInN1YiI6ImFkbWluIiwianRpIjojMGU0NGIxYzQtZDI0Mi0xMWVjLTk4ZWMtYTl1OTlkZGMwN2Y0IiwibmJmIjoxNjUyMzk0MTY5LCJleHAiOjE2NTIyOTY1NjksImFjY2VzcyIsInVzZXJvdWlkIjoiyTU3ZGVmMjgtY2M3MC0xMWVjLTk4ZWMtZjk4ODExNjNjZWlwiwidXN1c1JvbGUiOiJST0xFOX0FETU0Iiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2VybmFtZSI6ImFkbWluIn0.Avga0-isDjQB527d3QWZQb7AS4a9ea5wlbYUn-A9aPw" ,
"token_type": "Bearer"
}

```

2. Verwenden Sie den Wert für das Zugriffstoken in dieser Abfrage:

```

# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIyNDk5NTcsInN1YiI6ImFkbWluIiwianRpIjojNDk3MmRjNjAtZDBmMi0xMWVjLTk4ZWMtNDdlZTQwODkwMDVjIiwibmJmIjoxNjUyMjQ5OTU3LCJleHAiOjE2NTIyNTE3NTcsInJlZnJlc2hUb2t1bkV4cGlyZXNbdCI6MTY1MjI1MjM1NzQ1NywidG9rZW5UeXB1Ijois1dUX0FjY2VzcyIsInVzZXJvdWlkIjoiyTU3ZGVmMjgtY2M3MC0xMWVjLTk4ZWMtZjk4ODExNjNjZWlwiwidXN1c1JvbGUiOiJST0xFOX0FETU0Iiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2VybmFtZSI6ImFkbWluIn0.1JLmHddJ2jaVRmpdXF6gg48qdBcyRuit94DLobCJ9LI'
'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

Befolgen Sie die Schritte im Abschnitt.

### FTD-SNMP

Befolgen Sie die Schritte im Abschnitt.

### FTD Fehlerbehebungsdatei

Befolgen Sie die Schritte im Abschnitt.

### FCM-Benutzeroberfläche

FCM ist für Firepower der Serien 4100 und 9300 verfügbar. Befolgen Sie die Schritte im Abschnitt.

### FXOS-CLI

Befolgen Sie die Schritte im Abschnitt.

### FXOS REST-API

Befolgen Sie die Schritte im Abschnitt.

### FXOS-Chassis-Show-Tech-Datei

Befolgen Sie die Schritte im Abschnitt.



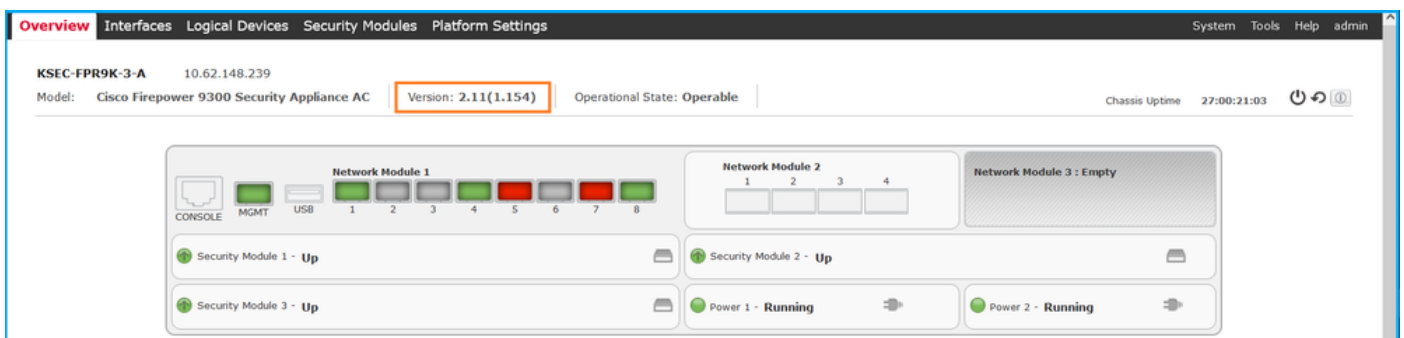
## FXOS-Softwareversion

Die FXOS-Softwareversion kann mithilfe der folgenden Optionen überprüft werden:

- FCM-Benutzeroberfläche (nur FirePOWER 4100/9300)
- FXOS-CLI
- FXOS REST-API
- FXOS-SNMP-Umfrage
- FXOS Chassis-Show-Tech-Datei.

## FCM-Benutzeroberfläche

So überprüfen Sie die FXOS-Softwareversion auf der FCM-Benutzeroberfläche **Version** auf der Hauptseite:



## FXOS-CLI

### FirePOWER 4100/9300

Gehen Sie folgendermaßen vor, um die FXOS-Softwareversion auf der FXOS-CLI zu überprüfen:

1. Stellen Sie eine Konsolen- oder SSH-Verbindung zum Chassis her.
2. Wechseln Sie zum **System für den Geltungsbereich** und führen Sie den Befehl **show firmware monitor** aus:

```
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 mit FTD

Gehen Sie folgendermaßen vor, um die FXOS-Softwareversion auf der FXOS-CLI zu überprüfen:

1. Stellen Sie eine Konsolenverbindung zum Chassis oder eine SSH-Verbindung zum FTD her. Bei einer SSH-Verbindung mit der FTD führen Sie den Befehl **connect fxos** auf der FTD-CLISH aus:

```
> connect fxos
```

2. Wechseln Sie zum **Bereichssystem**, und führen Sie den Befehl **show firmware detail** aus:

```
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 mit ASA, Firepower 2100 mit ASA im Appliance-Modus

Gehen Sie folgendermaßen vor, um die FXOS-Softwareversion auf der FXOS-CLI zu überprüfen:

1. Stellen Sie eine Konsolenverbindung zum Chassis oder zur Telnet-/SSH-Verbindung zur ASA her.

Bei einer Telnet-/SSH-Verbindung mit ASA führen Sie den Befehl **connect fxos** auf der ASA CLI aus.

```
asa# connect fxos
```

2. Wechseln Sie zum **Bereichssystem**, und führen Sie den Befehl **show firmware detail** aus:

```
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 mit ASA im Plattform-Modus

Gehen Sie folgendermaßen vor, um die FXOS-Softwareversion auf der FXOS-CLI zu überprüfen:

1. Stellen Sie eine SSH- oder Konsolenverbindung zum Chassis oder zur Telnet-/SSH-Verbindung zur ASA her.

Bei einer Telnet-/SSH-Verbindung mit ASA führen Sie den Befehl **connect fxos** auf der ASA CLI aus.

```
asa# connect fxos
```

2. Wechseln Sie zum **Bereichssystem**, und führen Sie den Befehl **show firmware detail** aus:

```
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

Die FXOS REST-API wird von der Serie FirePOWER 4100/9300 unterstützt.

### FirePOWER 4100/9300

Befolgen Sie diese Schritte, um die FXOS-Softwareversion über eine FXOS-REST-API-Anfrage zu überprüfen. Verwenden Sie einen REST-API-Client, um die Softwareversion zu überprüfen. In diesem Beispiel wird curl verwendet:

1. Authentifizierungstoken anfordern:

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

2. Verwenden Sie das Token in dieser Abfrage:

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'token:
1206f6a3032e7bdbeac07cfdd9d5add5cdd948e4e5f4511535a959aed7e1e2f5'
'https://192.0.2.100/api/sys/firmware/install-platform-fw' | grep -i platformBundle
  "platformBundleName": "fxos-k9.2.11.1.154.SPA",
  "platformBundleVersion": "2.11(1.154)",
```

## FXOS-SNMP

Die SNMP-Konfiguration auf FXOS wird auf FirePOWER 2100 mit ASA im Plattformmodus und Firepower 4100/9300 unterstützt.

### FirePOWER 4100/9300

Führen Sie die folgenden Schritte aus, um die FXOS-Softwareversion über SNMP zu überprüfen:

1. Stellen Sie sicher, dass SNMP auf FXOS konfiguriert ist. Konfigurationsschritte finden Sie unter [SNMP auf FirePOWER NGFW-Appliances konfigurieren](#).
2. Umfrage **.1.3.6.1.4.1.9.9.826.1.30.47.1.6** oder **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)"  
.1.3.6.1.4.1.9.9.826.1.30.47.1.6.32615 = 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 mit ASA im Plattform-Modus

Führen Sie die folgenden Schritte aus, um die FXOS-Softwareversion über SNMP zu überprüfen:

1. Stellen Sie sicher, dass SNMP auf FXOS konfiguriert ist. Konfigurationsschritte finden Sie unter [SNMP auf FirePOWER NGFW-Appliances konfigurieren](#).
2. Umfrage **.1.3.6.1.2.1.1.1.0** oder **SNMPv2-MIB::sysDescr.0**:

```
# 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-Datei

### FirePOWER 4100/9300

Gehen Sie folgendermaßen vor, um die FXOS-Softwareversion in der show-tech-Datei des FXOS-Chassis zu überprüfen:

1. Öffnen Sie für FXOS-Versionen 2.7 und höher die Datei **sam\_techsupportinfo** in **<name>\_BC1\_all.tar/ FPRM\_A\_TechSupport.tar.gz/FPRM\_A\_TechSupport.tar**

Für ältere Versionen öffnen Sie die Datei **sam\_techsupportinfo** in **FPRM\_A\_TechSupport.tar.gz/ FPRM\_A\_TechSupport.tar**.

2. Überprüfen Sie die Ausgabe des Befehls **"show firmware monitor"**:

```
# 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. Öffnen Sie die Datei `tech_support_brief` in `<name>_FPRM.tar.gz/<name>_FPRM.tar`.
2. Überprüfen Sie die Ausgabe des Befehls `"show firmware detail"`:

```
# 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-Softwareversion

Die FTD-Softwareversion kann mit folgenden Optionen verifiziert werden:

- FTD-CLI
- FTD-SNMP-Umfrage
- FTD-Fehlerbehebungsdatei
- FMC-Benutzeroberfläche
- FMC REST-API
- FDM-Benutzeroberfläche
- FDM REST-API
- FCM-Benutzeroberfläche
- FXOS-CLI
- FXOS REST-API

- FXOS-Chassis-Show-Tech-Datei

## FTD-CLI

Befolgen Sie diese Schritte, um die FTD-Softwareversion auf der FTD-CLI zu überprüfen:

1. Verwenden Sie die folgenden Optionen, um in Übereinstimmung mit dem Plattform- und Bereitstellungsmodus auf die FTD-CLI zuzugreifen:

- Direkter SSH-Zugriff auf FTD - alle Plattformen
- Zugriff von der FXOS-Konsolen-CLI (Firepower 1000/2100/3100) über Befehl **connect ftd**
- Zugriff von der FXOS-CLI über Befehle (Firepower 4100/9300):  
**connect module <x> [console|telnet]**, wobei x die Steckplatz-ID ist, und

**connect ftd [instance]**, wobei die Instanz nur für die Bereitstellung mehrerer Instanzen relevant ist.

- Für virtuelle FTDs direkter SSH-Zugriff auf FTD oder Konsolenzugriff über Hypervisor oder Cloud-Benutzeroberfläche

2. Führen Sie den Befehl **show version** auf CLI aus:

```
> 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

Befolgen Sie diese Schritte, um die FTD-Softwareversion über SNMP zu überprüfen:

1. Stellen Sie sicher, dass SNMP konfiguriert und aktiviert ist. Informationen zu FDM-verwalteten FTD finden Sie unter [Konfigurieren und Beheben von SNMP auf FirePOWER FDM](#) für Konfigurationsschritte. Informationen zu FMC-verwalteten FTD finden Sie unter [Konfigurieren von SNMP auf Firepower NGFW-Appliances](#) für Konfigurationsschritte.
2. Umfrage OID **SNMPv2-MIB::sysDescr.0** oder 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-Benutzeroberfläche

Gehen Sie folgendermaßen vor, um die FTD-Softwareversion auf der FMC-Benutzeroberfläche zu überprüfen:

## 1. Wählen Sie Geräte > Gerätemanagement:

The screenshot shows the Cisco Firepower Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices' (highlighted with a red box and labeled '1'), 'Objects', 'AMP', and 'Intelligence'. A dropdown menu is open under 'Devices', with 'Device Management' highlighted (labeled '2'). The dashboard displays several widgets: 'Unique Applications over Time' (line chart), 'Top Web Applications' (table), 'Top Client Applications' (table), and 'Traffic by Application Risk' (table).

## 2. Überprüfen Sie die Spalte Version:

The screenshot shows the 'Devices' page in the FMC. The 'Version' column in the device list is highlighted with a red box. The table below shows the following data:

Name	Model	Version	Chassis	Licenses	Access Control Policy	Group
LAB-FPR2K High Availability						
fpr2k-1(Primary, Active) Snort 3 192.0.2.140 - Routed	Firepower 2110 with FTD	7.1.0	N/A	Base, Threat (2 more...)	LAB-FPR2K-ACL	
fpr2k-2(Secondary, Standby) Snort 3 192.0.2.149 - Routed	Firepower 2110 with FTD	7.1.0	N/A	Base, Threat (2 more...)	LAB-FPR2K-ACL	

## FMC REST-API

Befolgen Sie diese Schritte, um die FTD-Softwareversion über FMC REST-API zu überprüfen. Verwenden Sie einen REST-API-Client, um die Softwareversion zu überprüfen. In diesem Beispiel wird **curl** verwendet:

### 1. Authentifizierungstoken anfordern:

```
# 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
```

2. Identifizieren Sie die Domäne, die das Gerät enthält. Bei den meisten REST API-Abfragen ist der **Domänenparameter** obligatorisch. Verwenden Sie das **X-auth-access-Token** in dieser Abfrage, um die Liste der Domänen abzurufen:

```
# 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-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. Verwenden Sie die Domänen-UUID, um nach den **Geräterecords** zu suchen:

```

# curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-000000000001/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-000000000001/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-000000000001/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-000000000001/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-000000000001/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-000000000001/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-000000000001/devices/devicerecords/0b1a9c94-8ba8-11ec-b2fd-93263934908d"
    },
    "name": "fpr2k-1",
    "type": "Device"
  },
},

```

#### 4. Verwenden Sie die UUID-Domäne und die UUID des Geräts bzw. Containers:

```

# 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": "-----[ fpr2k-1 ]-----\nModel
: Cisco Firepower 2110 Threat Defense (77) Version 7.1.0 (Build 90)\nUUID
0b1a9c94-8ba8-11ec-b2fd-93263934908d\nLSP version
: lsp-rel-20220502-1613\nVDB
version
: 353\n-----\n\nCisco
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\"\n\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\n1:
Int: Internal-Data0/1 : address is 000f.b748.4801, irq 0\n3: Ext: Management1/1 :
address is 707d.b9e2.836d, irq 0\n4: Int: Internal-Datal/1 : address is 0000.0100.0001, irq
0\n5: Int: Internal-Datal/2 : address is 0000.0300.0001, irq 0\n6: Int: Internal-Controll1/1
: address is 0000.0001.0001, irq 0\n\nSerial Number: JAD213508B6\n\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-Benutzeroberfläche

Befolgen Sie die Schritte im Abschnitt.

## FDM REST-API

Befolgen Sie die Schritte im Abschnitt.

## FTD-Fehlerbehebungsdatei

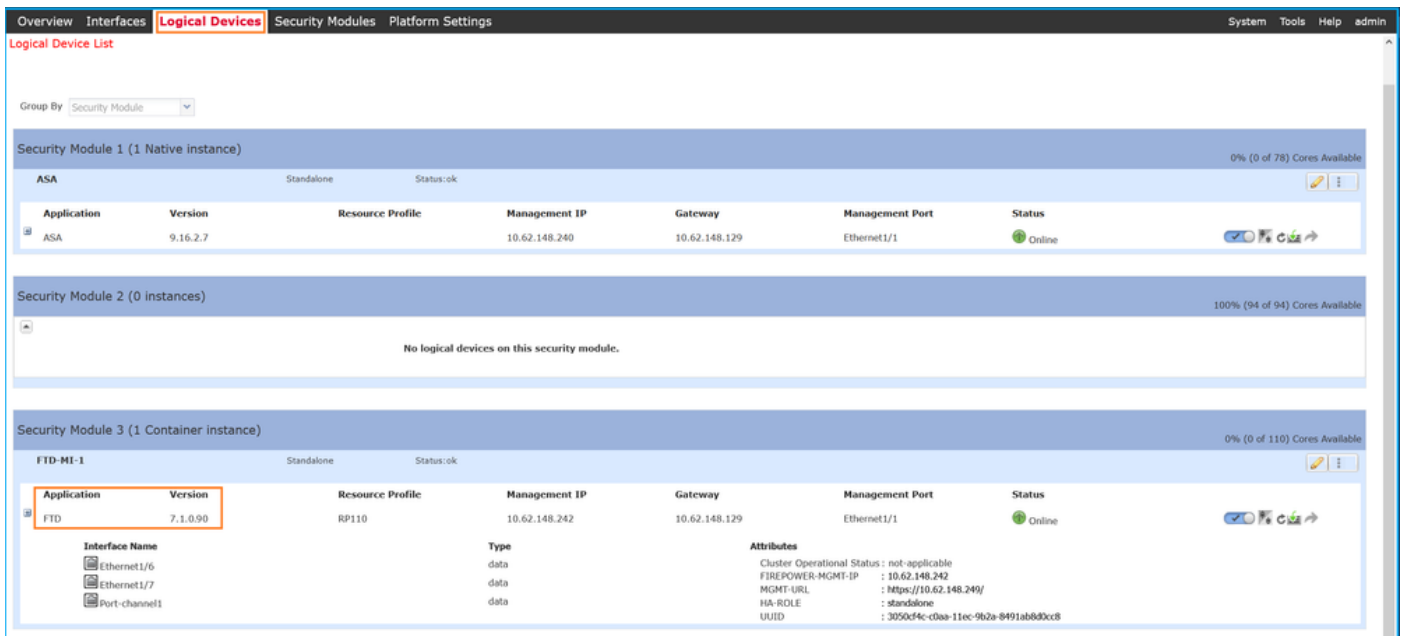
Befolgen Sie diese Schritte, um die FTD-Softwareversion in der FTD-Fehlerbehebungsdatei zu überprüfen:

1. Öffnen Sie die Fehlerbehebungsdatei, und navigieren Sie zum Ordner **<Dateiname>-Troubleshoot .tar/results-<date>—xxxxxx/command-output/**.
2. Öffnen Sie die Datei **usr-local-sf-bin-sfcli.pl show version.output**, und suchen Sie die Zeile mit **Model**:

```
# 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-Benutzeroberfläche

Verwenden Sie für FTD auf Firepower 4100/9300 den FCM, und prüfen Sie die **Version** auf der Registerkarte **Logical Devices (Logische Geräte)**:



## FXOS-CLI

### FTD für Firepower 4100/9300

Führen Sie die folgenden Schritte aus, um die FTD-Softwareversion auf der FXOS-CLI zu überprüfen:

1. Stellen Sie eine Konsolen- oder SSH-Verbindung zum Chassis her.
2. Wechseln Sie zum **Gültigkeitsbereich ssa** und führen Sie den Befehl **show app-instance** aus:

```
firepower# scope ssa
firepower /ssa # show app-instance
App Name   Identifier Slot ID   Admin State Oper State   Running Version Startup Version
Deploy Type Turbo Mode Profile Name Cluster State Cluster Role
-----
asa        ASA          1           Enabled   Online        9.16.2.7      9.16.2.7
Native    No           Not Applicable None
ftd       FTD-MI-1    3           Enabled   Online        7.1.0.90      7.1.0.90
Container No           RP110      Not Applicable None
```

### FTD für Firepower 1000/2100/3100

Führen Sie die folgenden Schritte aus, um die FTD-Softwareversion auf der FXOS-CLI zu überprüfen:

1. Herstellen einer Konsolenverbindung zum Chassis oder einer SSH-Verbindung zum FTD. Bei einer SSH-Verbindung mit der FTD führen Sie den Befehl **connect fxos** auf der FTD-CLISH aus:

```
> connect fxos
```

2. Wechseln Sie zum **Gültigkeitsbereich ssa** und führen Sie den Befehl **show app-instance** aus:

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

Application Name	Slot ID	Admin State	Operational State	Running Version	Startup
Version Deploy Type	Profile Name	Cluster Oper	State Cluster Role		
ftd	1	Enabled	Online	7.1.0.90	7.1.0.90
Native		Not Applicable	None		

## FXOS REST-API

Gehen Sie folgendermaßen vor, um die FTD-Softwareversion über eine FXOS-REST-API zu überprüfen:

### 1. Authentifizierungstoken anfordern:

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

2. Verwenden Sie das Token in dieser Abfrage, und stellen Sie sicher, dass Sie die Steckplatz-ID angeben, an der die FTD installiert ist:

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'token:
28821660bc74e418f3fadc443619df0387d69e7b150e035f688bed9d347b4838'
'https://192.0.2.100/api/slot/3/app-inst' | grep -Ei "identifizier|version"
  "identifizier": "FTD-MI-1",
  "runningVersion": "7.1.0.90",
    "hwCryptoVersion": "2",
  "startupVersion": "7.0.1.84",
  "versionIncompatibleErrorMgr": ""
```

## FXOS-Chassis-Show-Tech-Datei

Führen Sie die folgenden Schritte aus, um die FTD-Softwareversion in der Showtech-Datei des FXOS-Chassis zu überprüfen:

### FTD für Firepower 4100/9300

1. Öffnen Sie für FXOS-Versionen 2.7 und höher die Datei **sam\_techsupportinfo** in **<name>\_BC1\_all.tar/ FPRM\_A\_TechSupport.tar.gz/ FPRM\_A\_TechSupport.tar**

Für ältere Versionen öffnen Sie die Datei **sam\_techsupportinfo** in **FPRM\_A\_TechSupport.tar.gz/ FPRM\_A\_TechSupport.tar**.

2. Prüfen Sie den Abschnitt für jeden Steckplatz unter **"Ausblenden des Steckplatzes anzeigen"**:

```
# 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 für Firepower 1000/2100/3100

1. Öffnen Sie die Datei `tech_support_brief` in `<name>_FPRM.tar.gz/<name>_FPRM.tar`.
2. Überprüfen Sie die Abschnitte "SSA" und "Slot anzeigen":

```
# 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 Softwareversion

Die ASA-Softwareversion kann mithilfe der folgenden Optionen verifiziert werden:

- ASA-CLI
- ASA-SNMP-Umfrage
- ASA-Showtech-Datei
- FCM-Benutzeroberfläche
- FXOS-CLI
- FXOS REST-API
- FXOS-Chassis-Show-Tech-Datei

## ASA-CLI

Führen Sie die folgenden Schritte aus, um die ASA-Softwareversion auf der ASA CLI zu

überprüfen:

1. Verwenden Sie die folgenden Optionen für den Zugriff auf die ASA-CLI in Übereinstimmung mit dem Plattform- und Bereitstellungsmodus:

- Direkter Telnet-/SSH-Zugriff auf ASA mit Firepower 1000/3100 und Firepower 2100 im Appliance-Modus
- Zugriff von der FXOS-Konsolen-CLI auf der FirePOWER 2100 im Plattform-Modus und Verbindung mit ASA über den Befehl **connect as a**
- Zugriff von der FXOS-CLI über Befehle (Firepower 4100/9300):

**Verbinden Sie das Modul <x> [console|telnet], wobei x die Steckplatz-ID ist, und verbinden Sie sich dann als**

- Für virtuelle ASA direkter SSH-Zugriff auf ASA oder Konsolenzugriff über die Hypervisor- oder Cloud-Benutzeroberfläche

2. Führen Sie den Befehl **show version** aus:

```
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

Befolgen Sie diese Schritte, um die ASA-Softwareversion über SNMP zu überprüfen:

1. Stellen Sie sicher, dass SNMP konfiguriert und aktiviert ist.
2. Verwenden Sie den SNMP-Client zum Abfragen von OID **SNMPv2-MIB::sysDescr.0** oder **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-Showtech-Datei

Suchen Sie den Posten mit der Zeichenfolge **Cisco Adaptive Security Appliance Software Version**:

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

## FCM-Benutzeroberfläche

Befolgen Sie die Schritte im Abschnitt.

## FXOS-CLI

Befolgen Sie die Schritte im Abschnitt.

## FXOS REST-API

Befolgen Sie die Schritte im Abschnitt.

## FXOS-Chassis-Show-Tech-Datei

Befolgen Sie die Schritte im Abschnitt.

## Softwareversion des FirePOWER-Moduls

Das FirePOWER-Modul auf ASA ist der neue Name für die älteren Sourcefire-Module oder SFR.

Die Softwareversion kann mit den folgenden Optionen verifiziert werden:

- FMC-Benutzeroberfläche
- FMC REST-API
  
- Kommandozeile des FirePOWER-Moduls
- Fehlerbehebungsdatei für das FirePOWER-Modul
- ASA-CLI
- ASA-Showtech-Datei

## FMC-Benutzeroberfläche

Befolgen Sie die Schritte im Abschnitt.

## FMC REST-API

Befolgen Sie die Schritte im Abschnitt.

## FirePOWER-Modul-CLI

Gehen Sie folgendermaßen vor, um die Softwareversion des Firepower-Moduls auf der Modul-CLI zu überprüfen:

1. Stellen Sie über SSH oder die ASA-CLI eine Verbindung zum Modul über den Befehl **session sfr her**.
2. Führen Sie den Befehl **show version** aus:



```

> 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
-----

```

## Fehlerbehebungsdatei für das FirePOWER-Modul

Gehen Sie folgendermaßen vor, um die Softwareversion des Firepower-Moduls in der Fehlerbehebungsdatei zu überprüfen:

1. Öffnen Sie die Fehlerbehebungsdatei, und navigieren Sie zum Ordner **<Dateiname>-Troubleshoot .tar/results-<date>—xxxxxx/command-output/**.
2. Öffnen Sie die Datei **usr-local-sf-bin-sfcli.pl show version.output**, und suchen Sie die Zeile mit **Model**:

```

# 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

Führen Sie den Befehl **show module sfr details** auf der ASA CLI aus und überprüfen Sie die **Softwareversion**:

```

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-Showtech-Datei

Suchen Sie die Zeile mit der Zeichenfolge **show module sfr detail**:

```
----- 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
```

## Überprüfen der Versionen Snort, VDB und SRU

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

Die Snort-Version kann mithilfe der folgenden Optionen überprüft werden:

- FMC-Benutzeroberfläche
- FMC REST-API
- FDM-Benutzeroberfläche
- FDM REST-API
- FTD- oder FirePOWER-Modul-CLI
- FTD- oder FirePOWER-Modul zur Fehlerbehebung

### FMC-Benutzeroberfläche

Gehen Sie folgendermaßen vor, um die FTD Snort-Version auf der FMC-Benutzeroberfläche zu überprüfen:

1. Wählen Sie **Geräte > Gerätemanagement**:

The screenshot shows the Cisco Firepower Management Center interface. The 'Devices' menu is expanded, with 'Device Management' selected. The main dashboard area contains three widgets: 'Unique Applications over Time' (a line chart), 'Top Web Applications' (a table showing applications like Ubuntu and Internet Explorer), and 'Traffic by Application Risk' (a table showing risk levels like Medium and Very Low).

## 2. Überprüfen Sie die Beschriftung Snort:

The screenshot shows the 'Devices / Device Management' page in FMC. A table lists devices with columns for Name, Model, Version, Chassis, Licenses, Access Control Policy, and Group. Two devices are listed with 'Snort 3' in the 'Access Control Policy' column.

Name	Model	Version	Chassis	Licenses	Access Control Policy	Group
fpr2k-1(Primary, Active) 192.0.2.140 - Routed	Firepower 2110 with FTD	7.1.0	N/A	Base, Threat (2 more...)	Snort 3	LAB-FPR2K
ftp2k-2(Secondary, Standby) 192.0.2.149 - Routed	Firepower 2110 with FTD	7.1.0	N/A	Base, Threat (2 more...)	Snort 3	LAB-FPR2K

## FMC REST-API

Befolgen Sie diese Schritte, um die FTD Snort-Version über FMC REST-API zu überprüfen. Verwenden Sie einen REST-API-Client, um die Softwareversion zu überprüfen. In diesem Beispiel wird curl verwendet:

### 1. Authentifizierungstoken anfordern:

```
# 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
```

2. Identifizieren Sie die Domäne, die das Gerät enthält. Bei den meisten REST API-Abfragen ist der **Domänenparameter** obligatorisch. Verwenden Sie das **X-auth-access-Token** in dieser Abfrage, um die Liste der Domänen abzurufen:

```
# 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-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. Verwenden Sie die Domänen-UUID, um nach den **Geräterecords** zu suchen:

```

# curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-000000000001/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-000000000001/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-000000000001/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-000000000001/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-000000000001/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-000000000001/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-000000000001/devices/devicerecords/0b1a9c94-8ba8-11ec-b2fd-93263934908d"
    },
    "name": "fpr2k-1",
    "type": "Device"
  },
},

```

4. Verwenden Sie die UUID-Domäne und die UUID des Geräts bzw. Containers in dieser Anforderung:

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

Gehen Sie folgendermaßen vor, um die FTD Snort-Version auf der FDM-Benutzeroberfläche zu überprüfen:

1. Öffnen Sie die Seite **Updates**:





- FMC-Benutzeroberfläche
- FMC REST-API
- FMC-Fehlerbehebungsdatei
- FDM-Benutzeroberfläche
- FDM REST-API
- FTD-CLI
- FTD- oder FirePOWER-Modul zur Fehlerbehebung

## FMC-Benutzeroberfläche

Gehen Sie folgendermaßen vor, um die VDB-Version auf der FMC-Benutzeroberfläche zu überprüfen:

### 1. Wählen Sie Hilfe > Info:

The screenshot shows the Firepower Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. A dropdown menu is open under the 'admin' user profile, showing options like 'Page-level Help', 'How-Tos', 'Documentation on Cisco.com', 'What's New in This Release', 'Software Download', 'Secure Firewall YouTube', 'Secure Firewall on Cisco.com', 'Firepower Migration Tool', 'Partner Ecosystem', 'Ask a Question', and 'TAC Support Cases'. The 'About' option is highlighted with a red box and a '2' next to it.

### 2. VDB-Version überprüfen:

The screenshot shows the 'Help / About' page in the Firepower Management Center. The 'Model' section is expanded, displaying the following information:

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](mailto: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

Gehen Sie folgendermaßen vor, um die VDB-Version auf der FMC-CLI zu überprüfen:



1. Zugriff auf FMC über SSH oder Konsolenverbindung.
2. Führen Sie den Befehl **show version** aus:

```
> 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

Befolgen Sie diese Schritte, um die VDB-Version über eine FMC REST-API zu überprüfen. Verwenden Sie einen REST-API-Client, um die Softwareversion zu überprüfen. In diesem Beispiel wird curl verwendet:

1. Authentifizierungstoken anfordern:

```
# 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
```

2. Identifizieren Sie die Domäne, die das Gerät enthält. Bei den meisten REST API-Abfragen ist der **Domänenparameter** obligatorisch. Verwenden Sie das **X-auth-access-Token** in dieser Abfrage, um die Liste der Domänen abzurufen:

```
# 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-Fehlerbehebungsdatei

Gehen Sie folgendermaßen vor, um die VDB-Version in der FMC-Fehlerbehebungsdatei zu überprüfen:





2. Öffnen Sie die Datei `usr-local-sf-bin-sfcli.pl show version.output`, und suchen Sie die Zeile mit der **VDB-Version**:

```
# 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
-----

# 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
-----
```

## Aktualisierungsversionen für Angriffsregeln

Die Aktualisierungen der Angriffsregeln enthalten neue und aktualisierte Intrusion-Regeln und Präprozessorregeln, geänderte Zustände für installierte Regeln und geänderte Standardeinstellungen für Intrusion-Richtlinien.

Die sicheren Regelaktualisierungen (SRU) gelten für Snort Version 2, und die LSP-Updates (Lightweight Security Package) gelten für Snort Version 3.

Die Softwareversion der SRU/LSP kann mithilfe der folgenden Optionen überprüft werden:

- FMC-Benutzeroberfläche
- FMC REST-API
- FMC-Fehlerbehebungsdatei
- FDM-Benutzeroberfläche
- FDM REST-API
- FTD- oder FirePOWER-Modul-CLI
- FTD- oder FirePOWER-Modul zur Fehlerbehebung

## FMC-Benutzeroberfläche

Gehen Sie folgendermaßen vor, um die SRU/LSP-Versionen auf der FMC-Benutzeroberfläche zu überprüfen:

1. Wählen Sie **Hilfe > Info**:

## 2. Regelaktualisierungsversion und LSP-Version überprüfen:

## FMC-CLI

Führen Sie die folgenden Schritte aus, um die SRU/LSP-Versionen auf der FMC CLI zu überprüfen:

1. Zugriff auf FMC über SSH oder Konsolenverbindung.
2. Führen Sie den Befehl **show version** auf CLI aus:

```
> 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

Befolgen Sie diese Schritte, um die Softwareversion über eine REST-API-Anfrage zu überprüfen.

Verwenden Sie einen REST-API-Client, um die Softwareversion zu überprüfen. In diesem Beispiel wird **curl** verwendet:

### 1. Authentifizierungstoken anfordern:

```
# 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. Verwenden Sie das X-auth-access-Token in dieser Abfrage:

```
# 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-Fehlerbehebungsdatei

Gehen Sie folgendermaßen vor, um die SRU-Version in der FMC-Fehlerbehebungsdatei zu überprüfen:

1. Öffnen Sie die Fehlerbehebungsdatei, und wechseln Sie zu Ordner **<Dateiname>.tar/results-  
<date>—xxxxxx/dir-archives/etc/sf/**.
2. Öffnen Sie die Datei **sru\_versions.conf** und suchen Sie die Zeilen mit den Schlüsseln **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
```

Gehen Sie folgendermaßen vor, um die LSP-Version in der FMC-Fehlerbehebungsdatei zu überprüfen:

1. Öffnen Sie die Fehlerbehebungsdatei, und wechseln Sie zu Ordner **<Dateiname>.tar/results-<date>—xxxxxx/command-output**.
2. Datei **suchen var-sf-lsp-maxdeep 2-ls.output** und Zeile mit **/var/sf/lsp/active-lsp** überprüfen

```
# 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 -> /var/sf/lsp/lsp-rel-20220510-1044
19138299      4 drwxrwxr-x   5 www      root      4096 May 11 04:01 /var/sf/lsp/lsp-rel-
20220510-1044
19142266     600 -rwxrwxr-x   1 www      root     614400 May 10 14:55 /var/sf/lsp/lsp-rel-
20220510-1044/lsp.icdb.RELEASE.tar
19142234      4 drwxrwxr-x   5 www      root      4096 May 11 04:00 /var/sf/lsp/lsp-rel-
20220510-1044/ntd_metadata
19268898      4 drwxrwxr-x   2 www      root      4096 May 10 14:55 /var/sf/lsp/lsp-rel-
20220510-1044/icdb
19138303      4 drwxrwxr-x   6 www      root      4096 May 10 14:51 /var/sf/lsp/lsp-rel-
20220510-1044/talos_content
19142269   46640 -rw-r--r--   1 root     root    47759360 May 11 04:01 /var/sf/lsp/lsp-rel-
20220510-1044/lsp-rel-20220510-1044.tar.xz.REL.tar
19142267      4 -rwxrwxr-x   1 www      root      238 May 11 04:00 /var/sf/lsp/lsp-rel-
20220510-1044/.snort-versions
19142265      4 -rwxrwxr-x   1 www      root      26 May 10 14:51 /var/sf/lsp/lsp-rel-
20220510-1044/lspd_ver.properties
19139198     260 -rw-r--r--   1 root     root    264403 Feb 12 03:32 /var/sf/lsp/pigtail-
all-1644636642.log
19142270      0 lrwxrwxrwx   1 root     root      33 May 11 04:01 /var/sf/lsp/active-lsp
-> /var/sf/lsp/lsp-rel-20220510-1044
```

## FDM-Benutzeroberfläche

Aktivieren Sie auf der Hauptseite die Option **Intrusion Rule Update** (Regelaktualisierung für Sicherheitsrisiken):





```
"sruVersion" : "20211110-1348",
"lastSuccessSRUDate" : "2022-05-12 18:29:00Z",
"lspVersions" : [ "20211110-1348" ],
"type" : "sruversion"
```

## FTD- oder FirePOWER-Modul-CLI

Führen Sie die folgenden Schritte aus, um die SRU/LSP-Version auf der FTD-CLI oder der FirePOWER-Modul-CLI zu überprüfen:

1. Zugriff auf FTD über SSH oder Konsolenverbindung. Im Fall des FirePOWER-Moduls greifen Sie über SSH auf das Modul oder über den Befehl **session sfr** von der ASA CLI zu.
2. Führen Sie den Befehl **show version** auf CLI aus:

```
> 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
-----
```

```
> 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
-----
```

**Anmerkung:** Der Befehl **show version** zeigt die SRU-Update-Version an, wenn Snort 2 verwendet wird. Für Snort 3 LSP wird die Version angezeigt.

## FTD- oder FirePOWER-Modul Fehlerbehebungsdatei

Gehen Sie folgendermaßen vor, um die SRU/LSP-Versionen in der FTD- oder FirePOWER-Modul-Fehlerbehebungsdatei zu überprüfen:

1. Öffnen Sie die Fehlerbehebungsdatei, und wechseln Sie zum Ordner **<Dateiname>-troubleshoot.tar/results-<date>—xxxxxx/command-output/**.
2. Öffnen Sie die Datei **usr-local-sf-bin-sfcli.pl show version.output**, und suchen Sie die Zeile mit der **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 ]-----  
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  
-----
```

```
# 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  
-----
```

## Bekannte Probleme

Cisco Bug-ID [CSCwb34098](#) ENH: FMC-Version in Befehlsausgabe "show manager" anzeigen

Cisco Bug-ID [CSCve13470](#) ENH: Softwarebezogene OIDs für FirePOWER 6.x aktivieren

Cisco Bug-ID [CSCwb85969](#) ENH: Ausgabe des FMC CLISH-Befehls "show version" in Fehlerbehebungsdatei enthalten

Cisco Bug-ID [CSCvu15709](#) ENH: Unterstützung für SNMP-OIDs zum Abfragen von Standortversionen von SRU/VDB/GEO auf Firepower-Plattformen

## Zugehörige Informationen

- [Secure Firewall Management Center REST API Schnellstartanleitung, Version 7.1](#)
- [SNMP auf FirePOWER NGFW-Appliances konfigurieren](#)
- [REST API-Leitfaden für Cisco FirePOWER Threat Defense](#)
- [Referenz zur Cisco FXOS REST API](#)
- [Kompatibilität mit Cisco ASA](#)
- [Firepower 1000/2100 und Secure Firewall 3100 ASA- und FXOS-Paketversionen](#)
- [Paketkomponenten](#)

- [FirePOWER-Fehlerbehebung zur Dateigenerierung](#)