

# SNMP auf FirePOWER NGFW Appliances konfigurieren

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Chassis \(FXOS\) SNMP auf FPR4100/FPR9300](#)

[Konfigurieren von FXOS SNMPv1/v2c über GUI](#)

[Konfigurieren von FXOS SNMPv1/v2c über Befehlszeilenschnittstelle \(CLI\)](#)

[Konfigurieren von FXOS SNMPv3 über GUI](#)

[Konfigurieren von FXOS SNMPv3 über CLI](#)

[FTD \(LINA\) SNMP auf FPR4100/FPR9300](#)

[Konfigurieren von LINA SNMPv2c](#)

[Konfigurieren von LINA SNMPv3](#)

[SNMP in FPR2100](#)

[Chassis \(FXOS\) SNMP auf FPR2100](#)

[Konfigurieren von FXOS SNMPv1/v2c](#)

[Konfigurieren von FXOS SNMPv3](#)

[FTD \(LINA\) SNMP auf FPR2100](#)

[Überprüfung](#)

[Verifizieren von FXOS SNMP für FPR4100/FPR9300](#)

[FXOS SNMPv2c-Verifizierungen](#)

[FXOS SNMPv3-Verifizierungen](#)

[Verifizieren von FXOS SNMP für FPR2100](#)

[FXOS SNMPv2-Verifizierungen](#)

[FXOS SNMPv3-Verifizierungen](#)

[Verifizieren von FTD-SNMP](#)

[Zulassen von SNMP-Traffic zum FXOS auf FPR4100/FPR9300](#)

[Konfigurieren der globalen Zugriffsliste über die GUI](#)

[Konfigurieren der globalen Zugriffsliste über die CLI](#)

[Verifizierung](#)

[Verwendung des OID Object Navigator](#)

[Fehlerbehebung](#)

[Abfragen von FTD LINA SNMP nicht möglich](#)

[Abfragen von FXOS SNMP nicht möglich](#)

[Welche SNMP-OID-Werte sollten verwendet werden?](#)

[Abfragen von SNMP-Traps nicht möglich](#)

[Monitoring von FMC über SNMP nicht möglich](#)

[SNMP-Konfiguration im Firepower Device Manager \(FDM\)](#)

[SNMP-Cheat-Sheets zur Fehlerbehebung](#)

[So suchen Sie nach SNMP-Fehlern](#)

[Zugehörige Informationen](#)

## Einleitung

In diesem Dokument wird beschrieben, wie das Simple Network Management Protocol (SNMP) auf NGFW-FTD-Geräten der nächsten Generation konfiguriert wird und Fehler bei diesem Protokoll behoben werden.

## **Voraussetzungen**

### **Anforderungen**

Dieses Dokument erfordert grundlegende Kenntnisse des SNMP-Protokolls.

### **Verwendete Komponenten**

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

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 möglichen Auswirkungen aller Befehle kennen.

## **Hintergrundinformationen**

Firepower NGFW-Appliances können in 2 wichtige Subsysteme unterteilt werden:

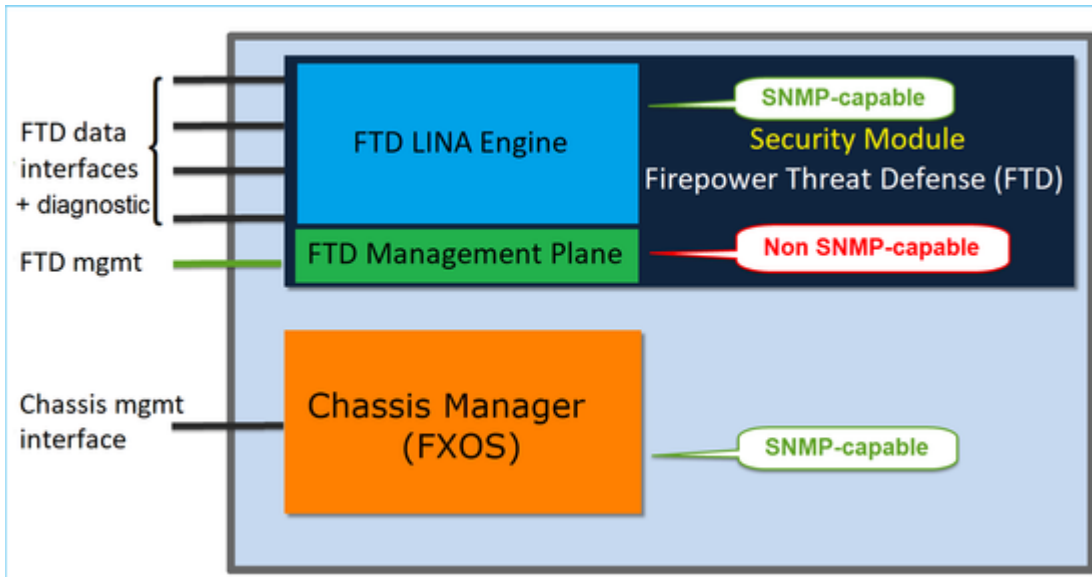
- Das Firepower Extensible Operative System (FX-OS) steuert die Chassis-Hardware.
- Firepower Threat Defense (FTD) wird im Modul ausgeführt.

FTD ist eine einheitliche Software, die aus zwei Haupt-Engines besteht, der Snort-Engine und der LINA-Engine. Die aktuelle SNMP-Engine der FTD leitet sich von der klassischen ASA ab und bietet Einblick in die LINA-bezogenen Funktionen.

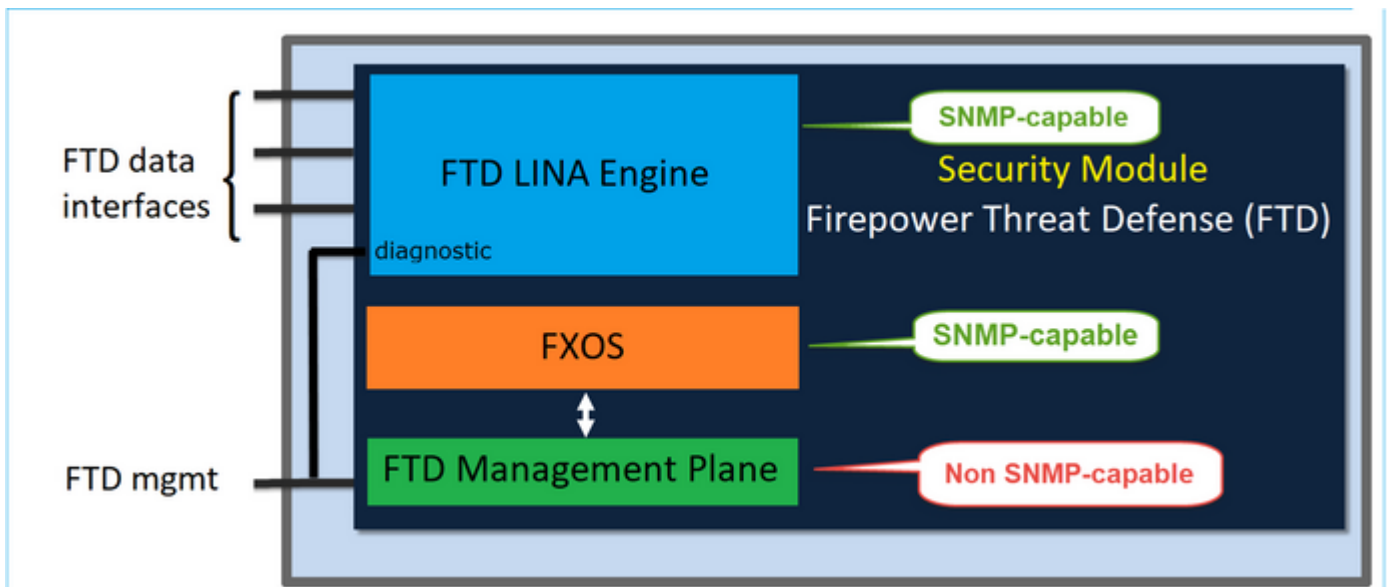
FX-OS und FTD verfügen über unabhängige Kontrollebenen und für Überwachungszwecke über unterschiedliche SNMP-Engines. Jedes der SNMP-Engines stellt unterschiedliche Informationen bereit und möchte möglicherweise beide überwachen, um eine umfassendere Ansicht des Gerätestatus zu erhalten.

Aus Hardwaresicht gibt es derzeit zwei Hauptarchitekturen für die Firepower NGFW-Appliances: die Firepower 2100-Serie und die Firepower 4100/9300-Serie.

Firepower 4100/9300-Geräte verfügen über eine dedizierte Schnittstelle für das Gerätemanagement. Dies ist die Quelle und das Ziel für den an das FXOS-Subsystem adressierten SNMP-Traffic. Auf der anderen Seite verwendet die FTD-Anwendung eine LINA-Schnittstelle (Daten und/oder Diagnose. In FTD-Versionen ab 6.6 kann auch die FTD-Managementschnittstelle verwendet werden) für die SNMP-Konfiguration.



Die SNMP-Engine auf Firepower 2100-Appliances verwendet die FTD-Managementschnittstelle und IP. Die Appliance selbst überbrückt den auf dieser Schnittstelle empfangenen SNMP-Traffic und leitet ihn an die FXOS-Software weiter.

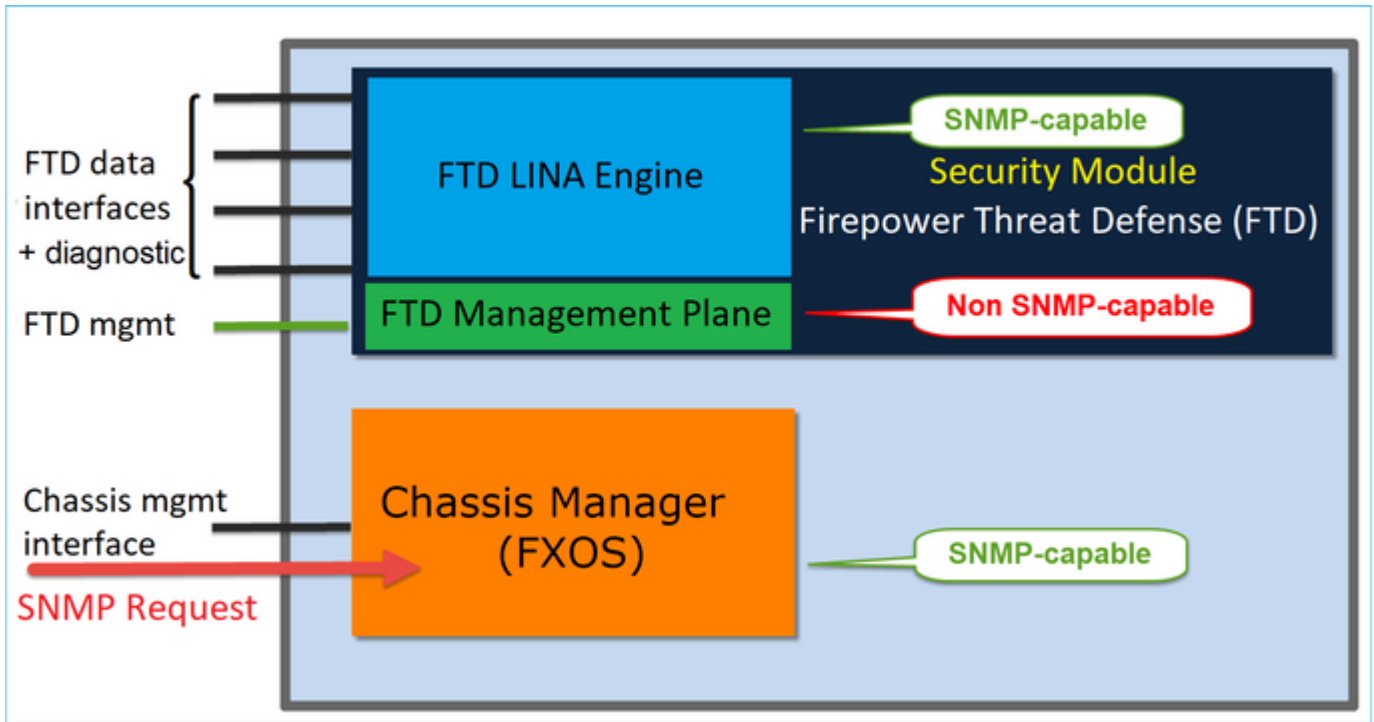


Bei FTDs mit Softwareversion 6.6+ wurden die folgenden Änderungen eingeführt:

- SNMP über die Managementschnittstelle.
- Auf den Plattformen der FPR1000- oder FPR2100-Serie vereint es sowohl LINA SNMP als auch FXOS SNMP über diese zentrale Managementschnittstelle. Darüber hinaus bietet es einen zentralen Konfigurationspunkt im FMC unter **Platform settings** > **SNMP** (Plattformeinstellungen > SNMP).

## Konfigurieren

### Chassis (FXOS) SNMP auf FPR4100/FPR9300



## Konfigurieren von FXOS SNMPv1/v2c über GUI

Schritt 1: Öffnen Sie die Firepower Chassis Manager (FCM)-UI und navigieren Sie zur Registerkarte **Platform Settings** > **SNMP** (Plattformeinstellungen > SNMP). Aktivieren Sie das Kontrollkästchen **SNMP enable** (SNMP aktivieren), geben Sie der **Community**-String an, die für SNMP-Anfragen verwendet werden soll, und klicken Sie auf **Save** (Speichern).

The screenshot shows the **Platform Settings** > **SNMP** configuration page. Key elements are highlighted with red boxes and numbered:

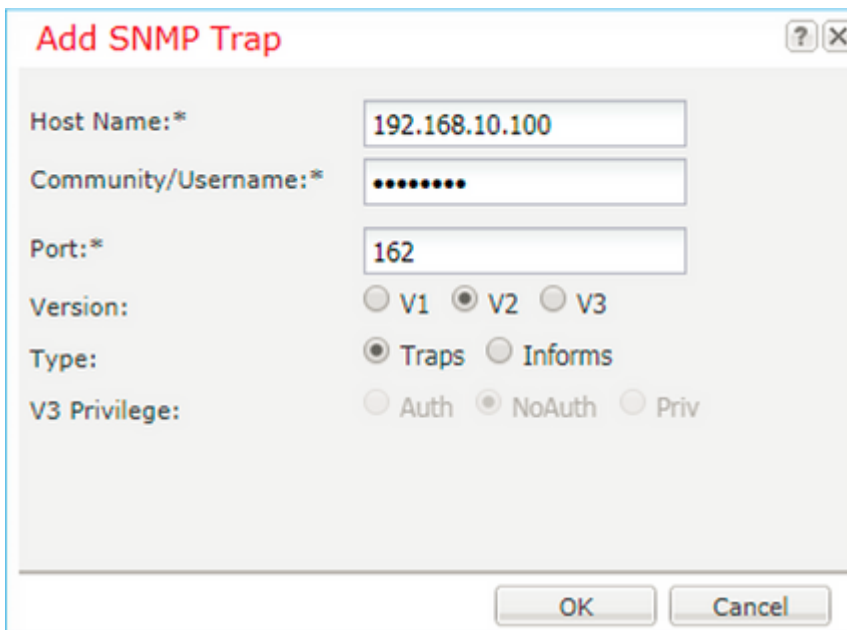
- Admin State:**  **Enable**
- Community/Username:**  **Set: No**
- Save** button
- SNMP Traps:**

Name	Port	Version	V3 Privilege	Type

Name	Auth Type	AES-128

**Hinweis:** Wenn das Feld Community/Benutzername bereits festgelegt ist, lautet der Text rechts neben dem leeren Feld **Festlegen: Yes (Festlegen)**. Wenn das Feld "Community/Benutzername" noch nicht mit einem Wert gefüllt ist, lautet der Text rechts neben dem leeren Feld **"Set: No" (Festlegen: Nein)**.

Schritt 2: Konfigurieren Sie den SNMP-Traps-Zielservers.



---

**Hinweis:** Die Community-Werte für Abfragen und Trap-Hosts sind unabhängig und können unterschiedlich sein.

---

Der Host kann als IP-Adresse oder mit einem Namen definiert werden. Wählen Sie **OK**, um die Konfiguration des SNMP-Trap-Servers automatisch zu speichern. Es ist nicht erforderlich, die Schaltfläche zum Speichern auf der SNMP-Hauptseite auszuwählen. Das gleiche geschieht, wenn Sie einen Host löschen.

### Konfigurieren von FXOS SNMPv1/v2c über Befehlszeilenschnittstelle (CLI)

```
<#root>
ksec-fpr9k-1-A#
scope monitoring
ksec-fpr9k-1-A /monitoring #
enable snmp
ksec-fpr9k-1-A /monitoring* #
set snmp community
Enter a snmp community:
ksec-fpr9k-1-A /monitoring* #
  enter snmp-trap 192.168.10.100
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set community
Community:
ksec-fpr9k-1-A /monitoring/snmp-trap* #
```

```
set version v2c
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set notificationtype traps
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set port 162
ksec-fpr9k-1-A /monitoring/snmp-trap* #
exit
ksec-fpr9k-1-A /monitoring* #
commit-buffer
```

## Konfigurieren von FXOS SNMPv3 über GUI

Schritt 1: Öffnen Sie FCM und navigieren Sie zur Registerkarte **Platform Settings > SNMP** (Plattformeinstellungen > SNMP).

Schritt 2: Für SNMP v3 ist es nicht erforderlich, im oberen Abschnitt einen Community-String festzulegen. Jeder erstellte Benutzer kann erfolgreich Abfragen an die FXOS-SNMP-Engine ausführen. Der erste Schritt ist die Aktivierung von SNMP in der Plattform. Anschließend können Sie die Benutzer und den Ziel-Trap-Host erstellen. Sowohl SNMP-Benutzer als auch SNMP-Trap-Hosts werden automatisch gespeichert.

Platform Settings > SNMP

Admin State:  Enable **1**

Port: 161

Community/Username:  Set:No

System Administrator Name:

Location:

**SNMP Traps**

**4**

Name	Port	Version	V3 Privilege	Type
------	------	---------	--------------	------

**SNMP Users**

**3**

Name	Auth Type	AES-128
------	-----------	---------

**2**

Schritt 3: Fügen Sie, wie in der Abbildung dargestellt, den SNMP-Benutzer hinzu. Der Authentifizierungstyp ist immer SHA, aber Sie können AES oder DES für die Verschlüsselung verwenden:

**Add SNMP User**

Name:\* user1

Auth Type: SHA

Use AES-128:

Password: .....

Confirm Password: .....

Privacy Password: .....

Confirm Privacy Password: .....

OK Cancel

Schritt 4: Fügen Sie den SNMP-Trap-Host hinzu, wie in der Abbildung dargestellt:

**Add SNMP Trap**

Host Name:\* 192.168.10.100

Community/Username:\* .....

Port:\* 162

Version:  V1  V2  V3

Type:  Traps  Informs

V3 Privilege:  Auth  NoAuth  Priv

OK Cancel

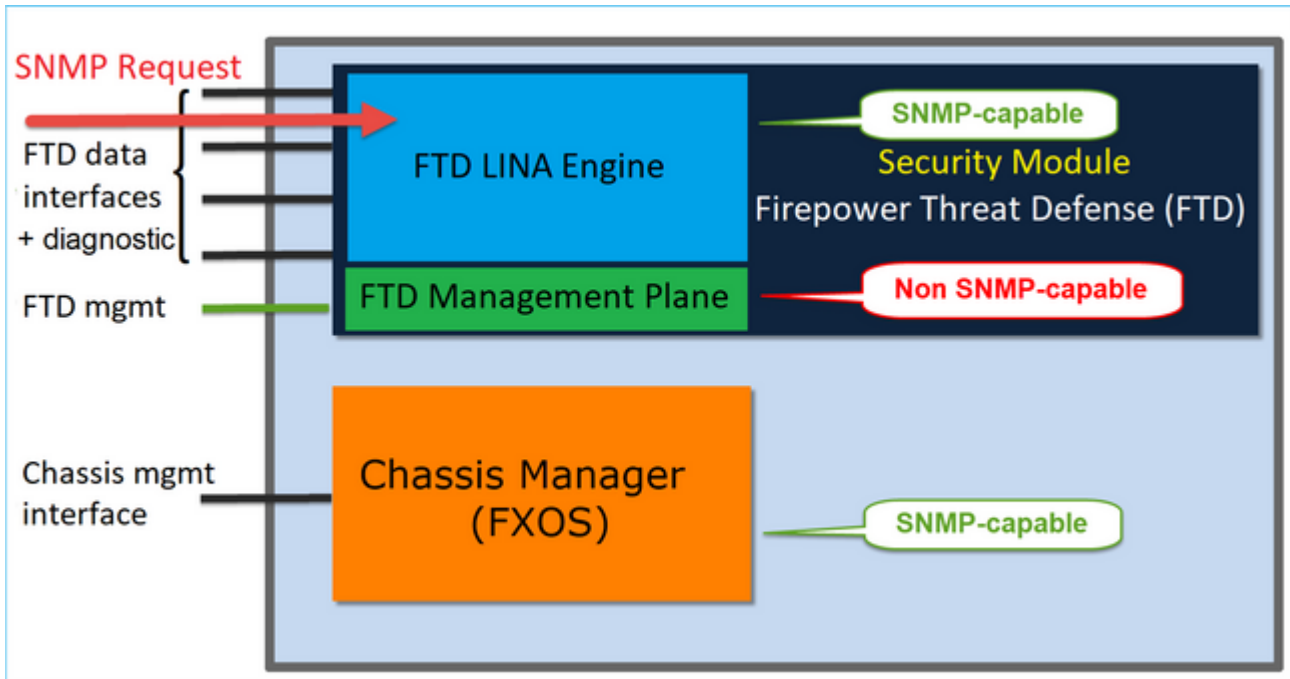
### Konfigurieren von FXOS SNMPv3 über CLI

```
<#root>
ksec-fpr9k-1-A#
scope monitoring
ksec-fpr9k-1-A /monitoring #
enable snmp
ksec-fpr9k-1-A /monitoring #
create snmp-user user1
```

```
Password:
ksec-fpr9k-1-A /monitoring/snmp-user* #
set auth sha
ksec-fpr9k-1-A /monitoring/snmp-user* #
set priv-password
Enter a password:
Confirm the password:
ksec-fpr9k-1-A /monitoring/snmp-user* #
set aes-128 yes
ksec-fpr9k-1-A /monitoring/snmp-user* #
exit
ksec-fpr9k-1-A /monitoring* #
enter snmp-trap 10.48.26.190
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set community
Community:
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set version v3
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set notificationtype traps
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set port 162
ksec-fpr9k-1-A /monitoring/snmp-trap* #
exit
ksec-fpr9k-1-A /monitoring* #
commit-buffer
```

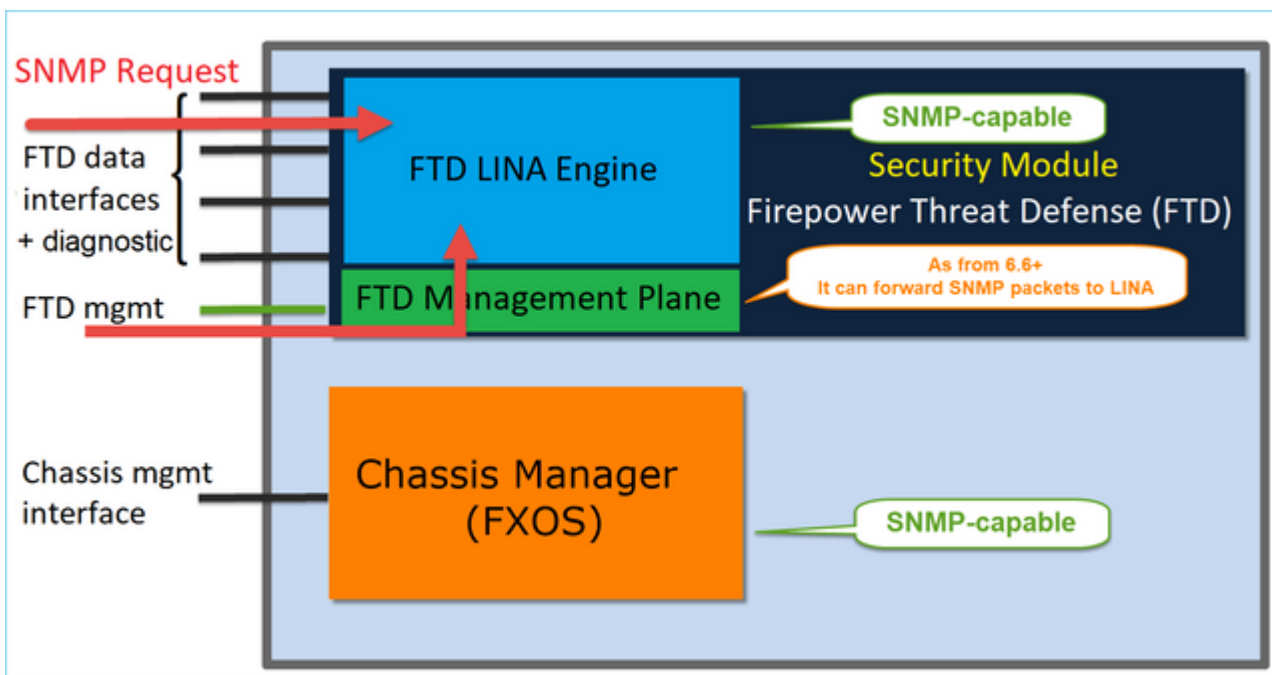
## **FTD (LINA) SNMP auf FPR4100/FPR9300**





### Änderungen in Versionen ab 6.6

- In Versionen ab 6.6 haben Sie auch die Möglichkeit, die FTD-Managementschnittstelle für Abfragen und Traps zu verwenden.



Die SNMP Single IP-Management-Funktion wird auf allen FTD-Plattformen ab Version 6.6 unterstützt:

- FPR2100
- FPR1000
- FPR4100
- FPR9300
- ASA5500, auf der FTD ausgeführt wird
- FTDv

### Konfigurieren von LINA SNMPv2c

Schritt 1: Navigieren Sie auf der FMC-UI zu **Devices > Platform Settings > SNMP (Geräte > Plattformeinstellungen > SNMP)**. Aktivieren Sie die Option Enable SNMP Servers (SNMP-Server aktivieren), und konfigurieren Sie die SNMPv2-Einstellungen wie folgt:

Schritt 2: Wählen Sie auf der Registerkarte **Hosts** die Schaltfläche **Add** (Hinzufügen) und geben Sie die SNMP-Servereinstellungen an:

**Edit SNMP Management Hosts** ? X

IP Address\* **SNMP-SERVER** +

SNMP Version **2c**

Username

Community String

Confirm

Poll

Trap

Port (1 - 65535)

**Available Zones** ↻

Search

- INSIDE\_FTD4110
- OUTSIDE1\_FTD4110
- OUTSIDE2\_FTD4110
- NET1\_4100-3
- NET2\_4100-3
- NET3\_4100-3

**Selected Zones/Interfaces**

**OUTSIDE3**

Add

Interface Name Add

OK Cancel

Sie können auch die **Diagnoseschnittstelle** als Quelle für die SNMP-Meldungen angeben. Die Diagnoseschnittstelle ist eine Datenschnittstelle, die nur "To-the-box" und "Out-of-the-box"-Traffic zulässt (nur Management).

**Add SNMP Management Hosts**

IP Address\*  
SNMP-SERVER +

SNMP Version  
2c

Username

Community String

Confirm

Poll  
 Trap

Trap Port  
162  
(1 - 65535)

Reachable By:

Device Management Interface (Applicable from v6.6.0 and above)  
 Security Zones or Named Interface

Available Zones ⌵

Q Search Add

- 2100\_inside
- 2100\_outside
- cluster\_dmz
- cluster\_inside
- cluster\_outside

Selected Zones/Interfaces

diagnostic 🗑

Interface Name Add

Cancel OK

Diese Abbildung stammt aus Version 6.6 und verwendet das helle Design.

Darüber hinaus können Sie in FTD-Versionen ab 6.6 auch die Managementschnittstelle auswählen:

### Add SNMP Management Hosts

IP Address\*  
 +

SNMP Version

Username

Community String

Confirm

Poll  
 Trap

Trap Port  
  
(1 - 65535)

Reachable By:

Device Management Interface *(Applicable from v6.6.0 and above)*

Security Zones or Named Interface

Available Zones

- 2100\_inside
- 2100\_outside
- cluster\_dmz
- cluster\_inside
- cluster\_outside

Selected Zones/Interfaces

diagnostic

Interface Name

Wenn die neue Managementschnittstelle ausgewählt ist, ist LINA SNMP über diese verfügbar.

Ergebnis:

- ARP Inspection
- Banner
- External Authentication
- Fragment Settings
- HTTP
- ICMP
- Secure Shell
- SMTP Server
- ▶ **SNMP**
- SSL
- Syslog
- Timeouts
- Time Synchronization
- UCAPL/CC Compliance

Enable SNMP Servers

Read Community String

Confirm\*

System Administrator Name

Location

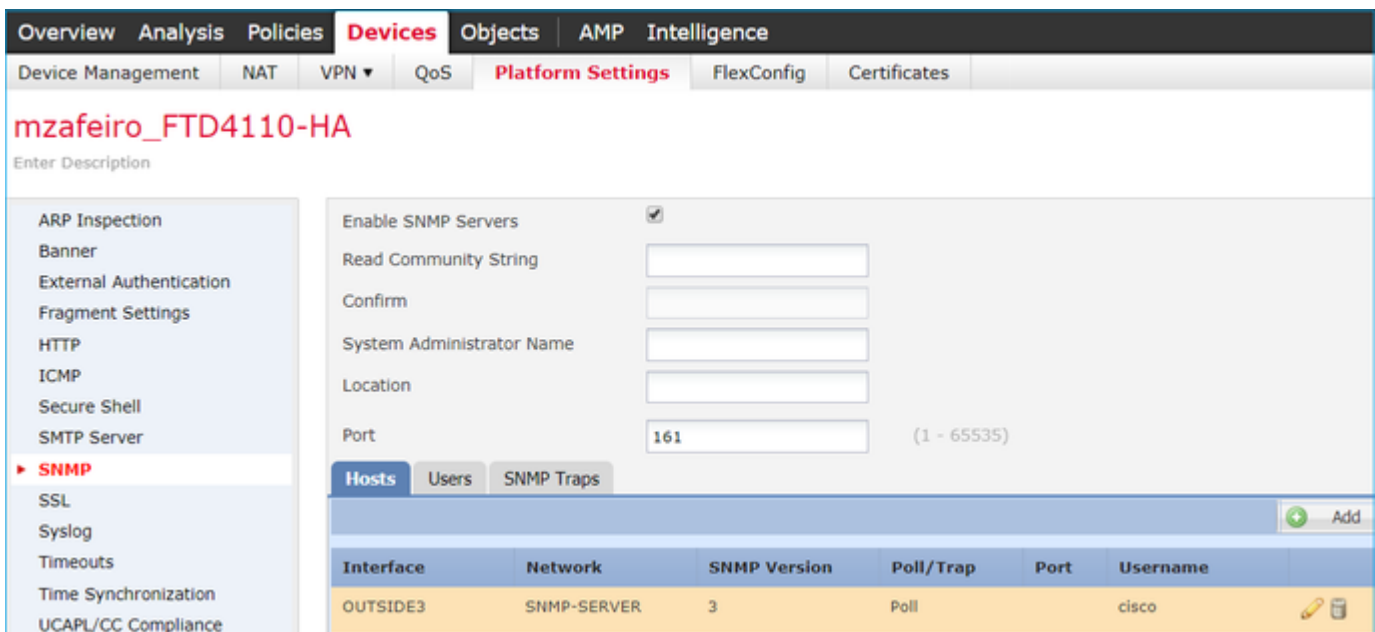
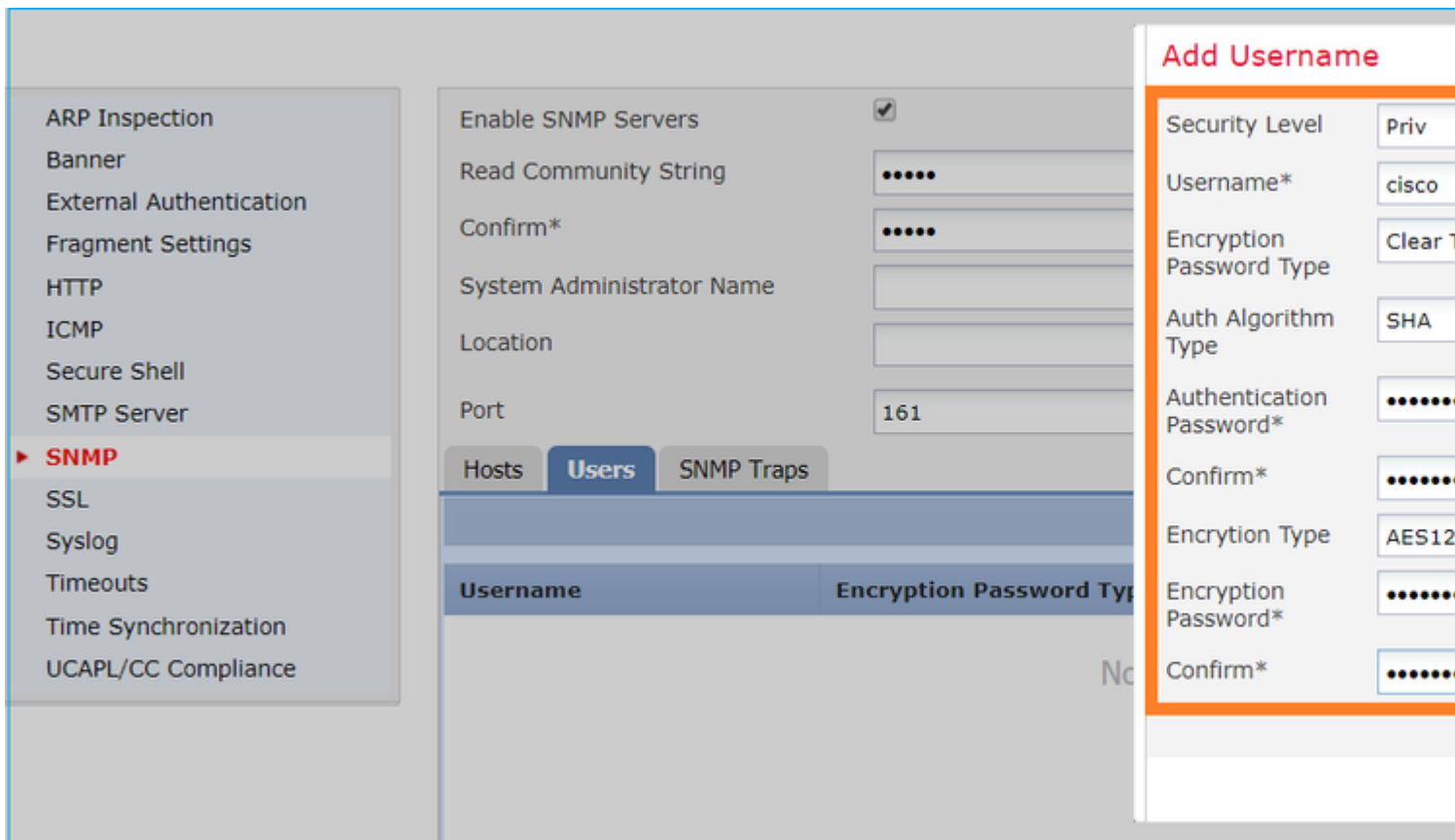
Port  (1 - 65535)

**Hosts** | Users | SNMP Traps

Interface	Network	SNMP Version	Poll/Trap	Port	Username
OUTSIDE3	SNMP-SERVER	2c	Poll		

### Konfigurieren von LINA SNMPv3

Schritt 1: Navigieren Sie auf der FMC-UI zu **Devices > Platform Settings > SNMP (Geräte > Plattformeinstellungen > SNMP)**. Aktivieren Sie die Option Enable SNMP Servers (SNMP-Server aktivieren) und konfigurieren Sie den SNMPv3-Benutzer und -Host:



Schritt 2: Konfigurieren Sie den Host auch für den Empfang von Traps:

### Edit SNMP Management Hosts

IP Address\*

SNMP Version

Username

Community String

Confirm

Poll

Trap

Port  (1 - 65535)

Available Zones

Selected Zones/Interfaces

Search

INSIDE\_FTD4110

OUTSIDE3

Schritt 3: Die Traps, die Sie empfangen möchten, können im Abschnitt **SNMP Traps** ausgewählt werden:

► **SNMP**

- SSL
- Syslog
- Timeouts
- Time Synchronization
- UCAPL/CC Compliance

Hosts Users **SNMP Traps**

Enable Traps  All SNMP  Syslog

**Standard**

Authentication:

Link up

Link Down

Cold Start

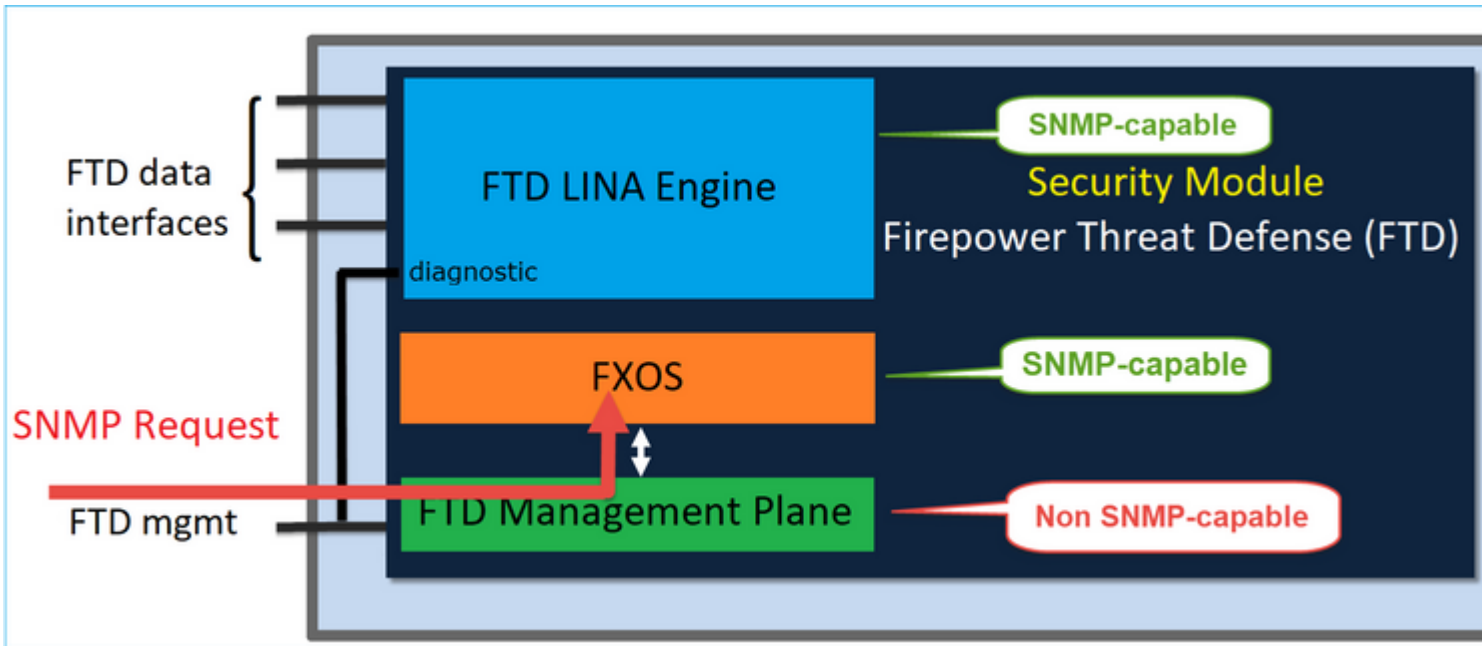
Warm Start

**Entity MIB**

## SNMP in FPR2100

Auf FPR2100-Systemen gibt es keinen FCM. Die einzige Möglichkeit, SNMP zu konfigurieren, ist über FMC.

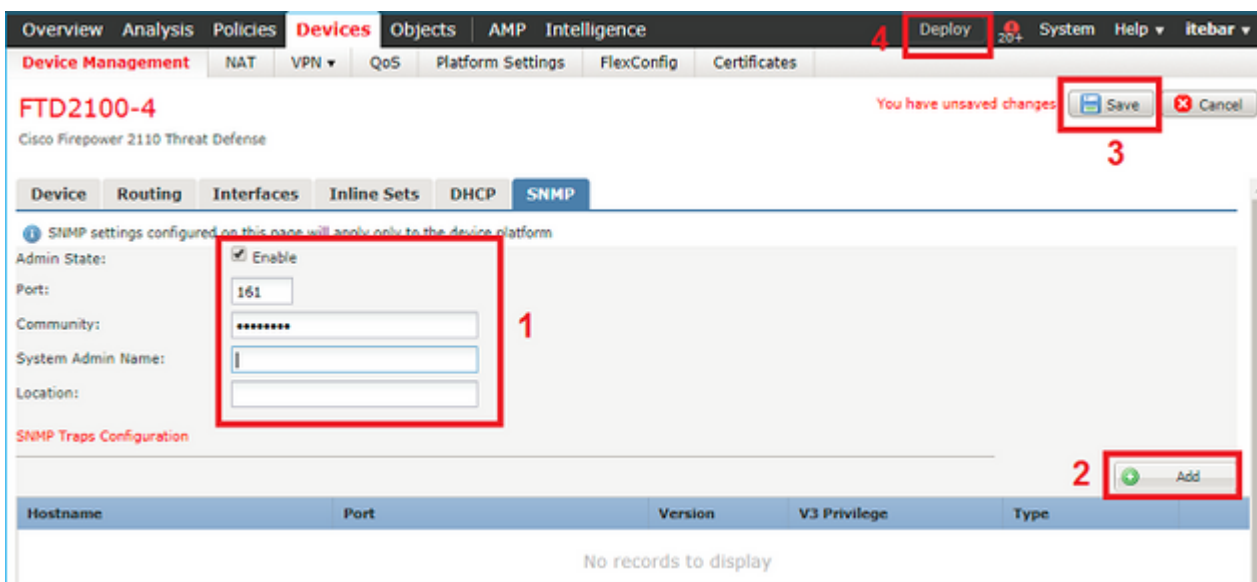
## Chassis (FXOS) SNMP auf FPR2100

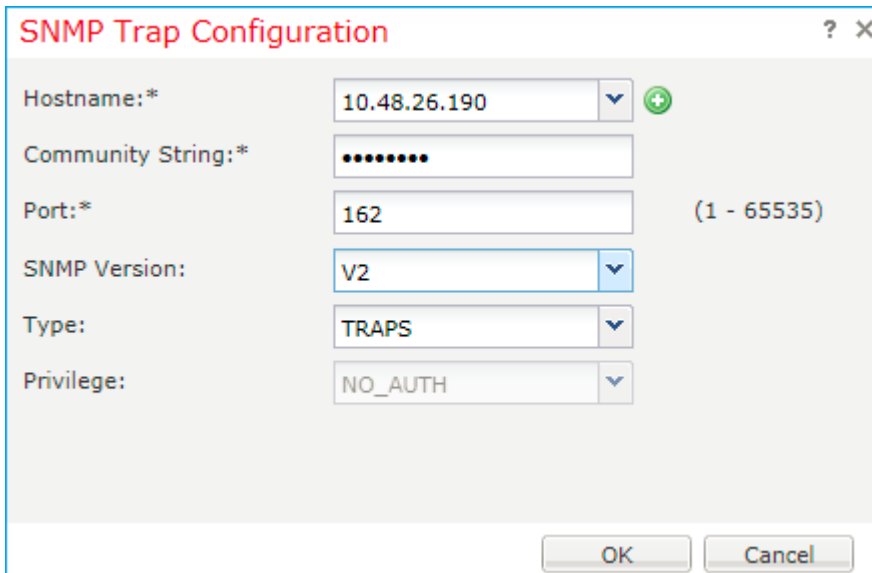


Ab FTD 6.6 haben Sie auch die Möglichkeit, die FTD-Managementschnittstelle für SNMP zu verwenden. In diesem Fall werden sowohl FXOS- als auch LINA-SNMP-Informationen über die FTD-Managementschnittstelle übertragen.

### Konfigurieren von FXOS SNMPv1/v2c

Öffnen Sie die FMC-Benutzeroberfläche und navigieren Sie zu **Devices > Device Management (Geräte > Gerätemanagement)**. Wählen Sie das Gerät und dann SNMP aus:





**SNMP Trap Configuration**

Hostname:\* 10.48.26.190

Community String:\* .....

Port:\* 162 (1 - 65535)

SNMP Version: V2

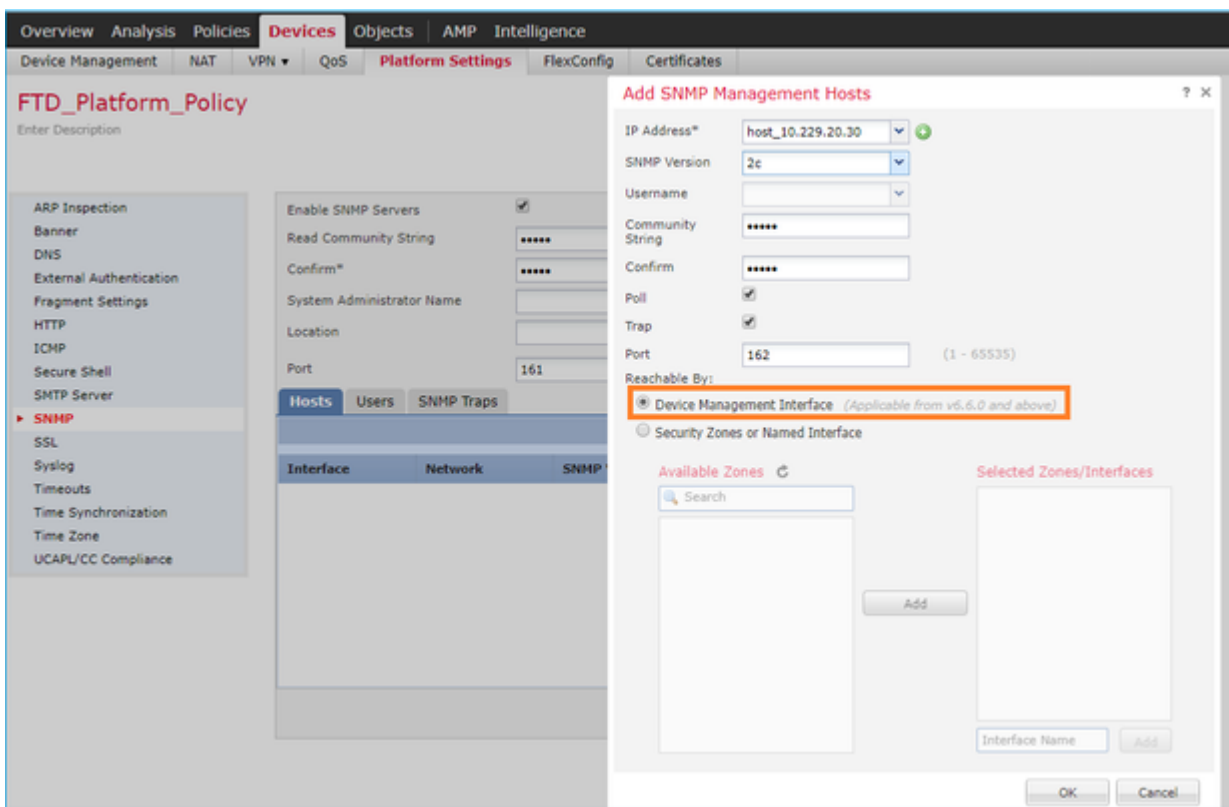
Type: TRAPS

Privilege: NO\_AUTH

OK Cancel

## Änderung ab FTD 6.6

Sie können die FTD-Managementschnittstelle angeben:



Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS **Platform Settings** FlexConfig Certificates

**FTD\_Platform\_Policy**

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP

ICMP

Secure Shell

SMTP Server

**SNMP**

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Enable SNMP Servers

Read Community String .....

Confirm\* .....

System Administrator Name

Location

Port 161

Hosts Users SNMP Traps

Interface Network SNMP

**Add SNMP Management Hosts**

IP Address\* host\_10.229.20.30

SNMP Version 2c

Username

Community String .....

Confirm .....

Poll

Trap

Port 162 (1 - 65535)

Reachable By:

Device Management Interface (Applicable from v6.6.0 and above)

Security Zones or Named Interface

Available Zones

Selected Zones/Interfaces

Add

Interface Name Add

OK Cancel

Da die Managementschnittstelle auch für SNMP konfiguriert werden kann, wird auf der Seite folgende Warnmeldung angezeigt:

Die SNMP-Konfiguration der Geräteplattform auf dieser Seite ist deaktiviert, wenn SNMP-Einstellungen, die mit der Gerätemanagement-Schnittstelle konfiguriert wurden, über **Geräte > Plattformeinstellungen (Schutz vor Bedrohungen) > SNMP > Hosts** erfolgen.

## Konfigurieren von FXOS SNMPv3



Öffnen Sie die FMC-UI und navigieren Sie zu **Choose Devices > Device Management (Geräte auswählen > Gerätemanagement)**. Wählen Sie das Gerät aus, und wählen Sie **SNMP** aus.

The screenshot shows the FMC-UI interface for device management. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Devices' tab is active, and the 'SNMP' sub-tab is selected. The device name is 'FTD2100-4' (Cisco Firepower 2110 Threat Defense). The 'Admin State' is set to 'Enable' (checkbox 1). The 'Port' is set to '161'. Below the main configuration, there are two sections: 'SNMP Traps Configuration' and 'SNMP Users Configuration'. Both sections have an 'Add' button (3 and 2 respectively). At the top right, there is a 'Deploy' button (5) and a 'Save' button (4). A notification 'You have unsaved changes' is visible.

The 'SNMP User Configuration' dialog box is shown. It contains the following fields and options:

- Username: \* user1
- Auth Algorithm Type: SHA
- Use AES:
- Password\*: [Redacted]
- Confirm: [Redacted]
- Privacy Password\*: [Redacted]
- Confirm: [Redacted]

Buttons: OK, Cancel

**SNMP Trap Configuration** ? X

Hostname:\* 10.48.26.190 +

Community String:\* .....

Port:\* 163 (1 - 65535)

SNMP Version: V3

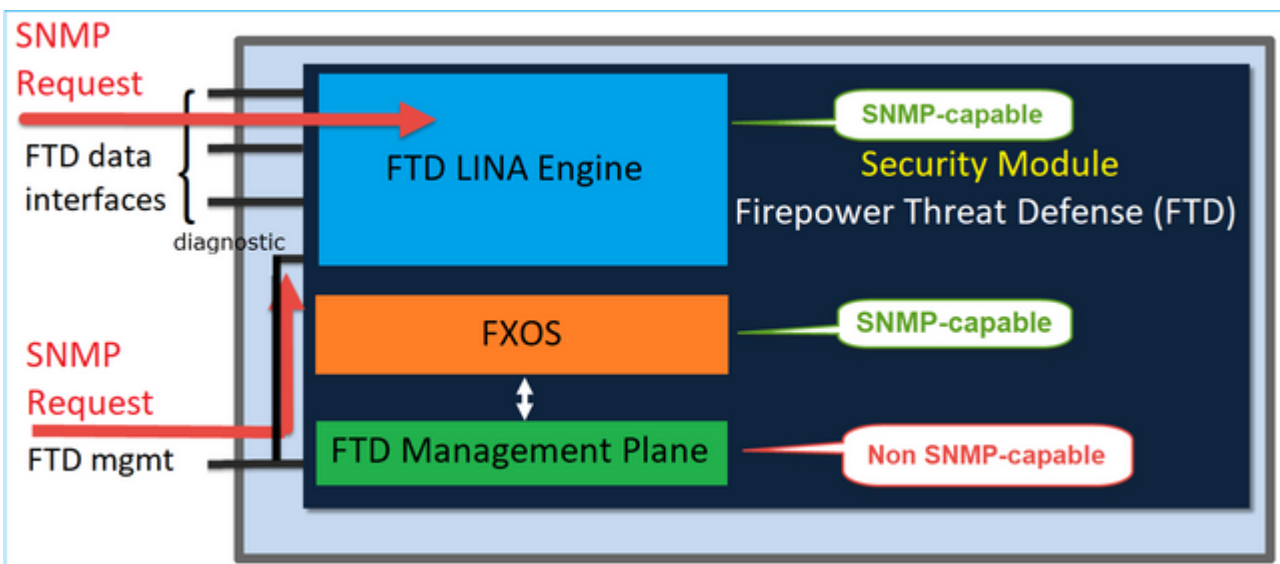
Type: TRAPS

Privilege: PRIV

OK Cancel

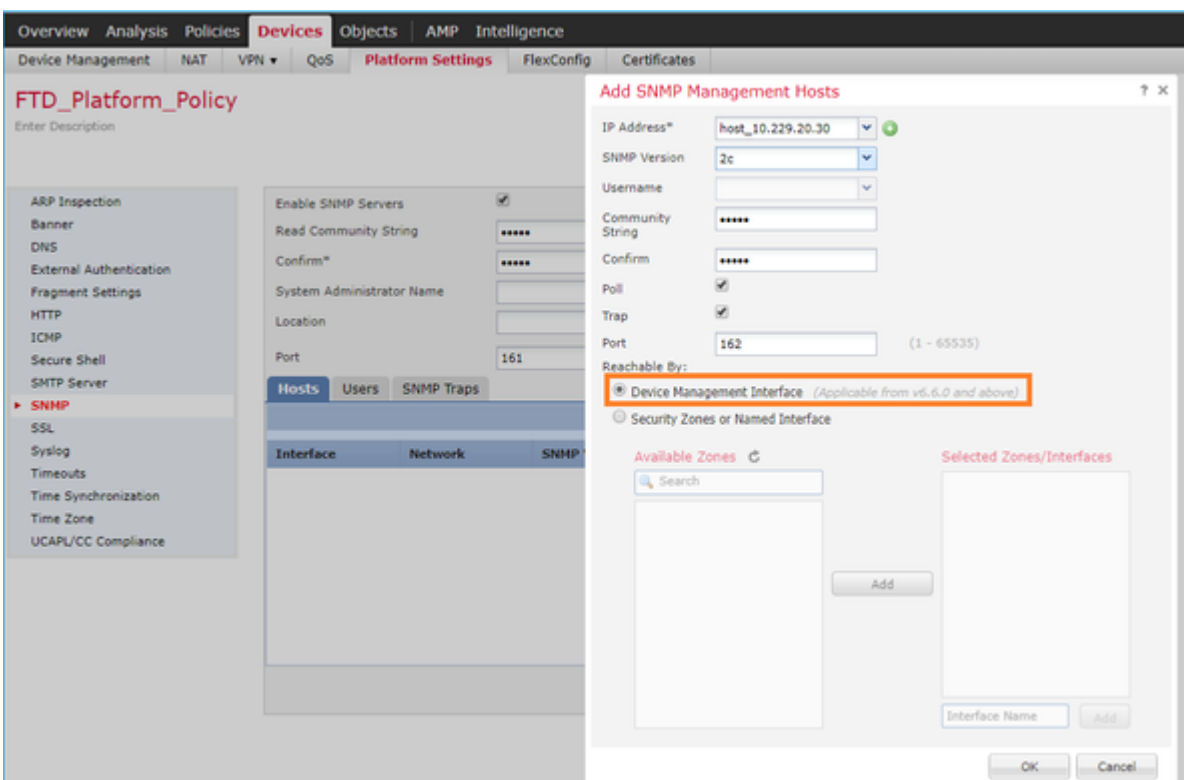
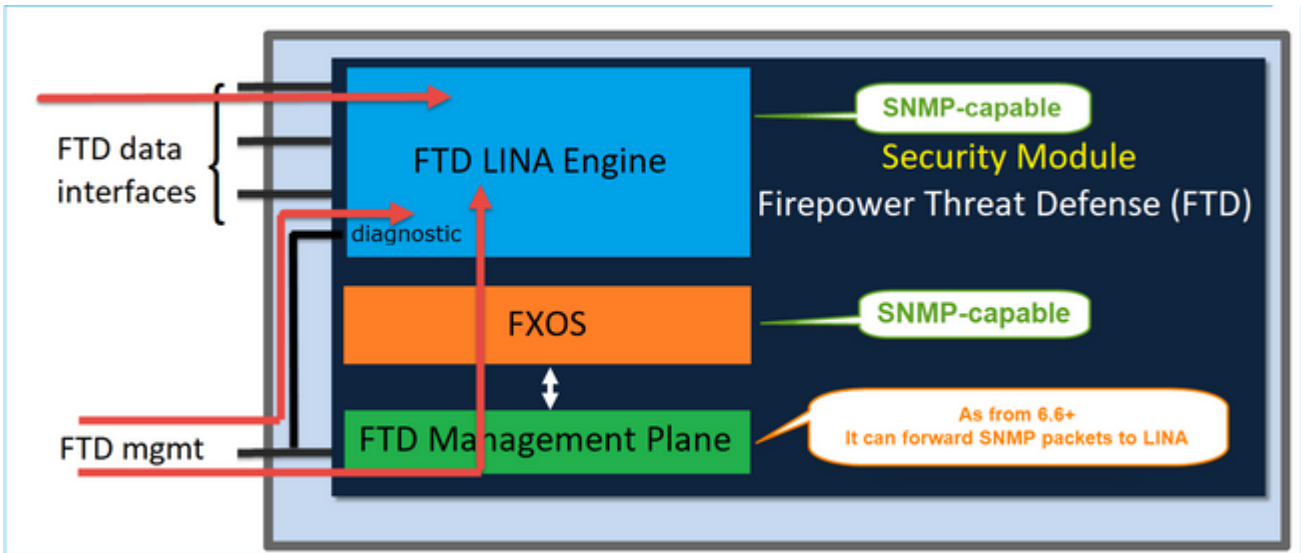
### FTD (LINA) SNMP auf FPR2100

- Für Versionen vor 6.6 ist die LINA-FTD-SNMP-Konfiguration auf FTD FP1xxx/FP21xx-Appliances identisch mit einer FTD auf Firepower 4100- oder 9300-Appliance.



### Versionen ab FTD 6.6

- In Versionen ab 6.6 haben Sie auch die Möglichkeit, die FTD-Managementschnittstelle für LINA-Abfragen und Traps zu verwenden.



Wenn die neue Managementschnittstelle ausgewählt ist:

- LINA SNMP ist über die Management-Schnittstelle verfügbar.
- Unter **Devices > Device Management** (Geräte > Gerätemanagement) ist die Registerkarte **SNMP** deaktiviert, da sie nicht mehr benötigt wird. Ein Benachrichtigungsbanner wird angezeigt. Die Registerkarte "SNMP Device" (SNMP-Gerät) wurde nur auf den Plattformen 2100/1100 angezeigt. Diese Seite ist auf den Plattformen FPR9300/FPR4100 und FTD55xx nicht vorhanden.

Nach der Konfiguration wird eine kombinierte LINA SNMP + FXOS SNMP-Abfrage/Trap (auf FP1xxx/FP2xxx) über die FTD-Managementschnittstelle angezeigt.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

**FTD2100-6**  
Cisco Firepower 2140 Threat Defense

Device Routing Interfaces Inline Sets DHCP **SNMP**

⚠ Device platform SNMP setting configuration on this page is deprecated and the same will be configurable through **Devices > Platform Settings (Threat Defense) > SNMP > Hosts with Device Management**

ℹ SNMP settings configured on this page will apply only to the device platform

Admin State:  Enable

Port:

Community:

System Admin Name:

Location:

SNMP Traps Configuration

Hostname	Port	Version	V3 Privilege	Type
No records to display				

Die SNMP Single IP-Management-Funktion wird auf allen FTD-Plattformen ab Version 6.6 unterstützt:

- FPR2100
- FPR1000
- FPR4100
- FPR9300
- ASA5500, auf der FTD ausgeführt wird
- FTDv

Weitere Informationen finden Sie unter Konfigurieren von SNMP für Threat Defense

## Überprüfung

### Verifizieren von FXOS SNMP für FPR4100/FPR9300

#### FXOS SNMPv2c-Verifizierungen

Verifizierung der CLI-Konfiguration:

```
<#root>
```

```
ksec-fpr9k-1-A /monitoring #
```

```
show snmp
```

```
Name: snmp
```

```
Admin State: Enabled
```

```
Port: 161
```

```
Is Community Set: Yes
```

```
Sys Contact:
```

```
Sys Location:
```

```
ksec-fpr9k-1-A /monitoring # show snmp-trap
```

SNMP Trap:

SNMP Trap	Port	Community	Version	V3 Privilege	Notification Type
192.168.10.100	162		V2c	Noauth	Traps

Im FXOS-Modus:

```
<#root>
```

```
ksec-fpr9k-1-A(fxos)#
```

```
show run snmp
```

```
!Command: show running-config snmp
```

```
!Time: Mon Oct 16 15:41:09 2017
```

```
version 5.0(3)N2(4.21)
snmp-server host 192.168.10.100 traps version 2c cisco456
snmp-server enable traps callhome event-notify
snmp-server enable traps callhome smtp-send-fail
â€¦! All traps will appear as enable â€¦!
snmp-server enable traps flexlink ifStatusChange
snmp-server context mgmt vrf management
snmp-server community cisco123 group network-operator
```

Zusätzliche Verifizierungen:

```
<#root>
```

```
ksec-fpr9k-1-A(fxos)#
```

```
show snmp host
```

Host	Port	Version	Level	Type	SecName
192.168.10.100	162	v2c	noauth	trap	cisco456

```
<#root>
```

```
ksec-fpr9k-1-A(fxos)#
```

```
show snmp
```

Community	Group / Access	context	acl_filter
cisco123	network-operator		

```
...
```

Testen von SNMP-Anfragen.

Durchführen einer SNMP-Anfrage von einem gültigen Host aus.

Trap-Generierung bestätigen.

Sie können "Flapping an interface with ethanalyzer enabled" (Flapping einer Schnittstelle mit aktiviertem EthAnalyzer) verwenden, um zu bestätigen, dass SNMP-Traps generiert und an die definierten Trap-Hosts gesendet werden:

```
<#root>
```

```
ksec-fpr9k-1-A(fxos)#
```

```
ethanalyzer local interface mgmt capture-filter "udp port 162"
```

```
Capturing on eth0
```

```
wireshark-broadcom-rcpu-dissector: ethertype=0xde08, devicetype=0x0
```

```
2017-11-17 09:01:35.954624 10.62.148.35 -> 192.168.10.100 SNMP sNMPv2-Trap
```

```
2017-11-17 09:01:36.054511 10.62.148.35 -> 192.168.10.100 SNMP sNMPv2-Trap
```

---

**Warnung:** Eine Schnittstellen-Klappe kann zu einem Ausfall des Datenverkehrs führen. Führen Sie diesen Test nur in einer Laborumgebung oder in einem Wartungsfenster durch.

---

## FXOS SNMPv3-Verifizierungen

Schritt 1: Öffnen Sie die FCM-UI. **Platform Settings > SNMP > User** (Plattformeinstellungen > SNMP > Benutzer) zeigt, ob ein Kennwort und ein Datenschutzkennwort konfiguriert sind:

The screenshot shows a dialog box titled "Edit user1" with the following fields and values:

- Name: user1
- Auth Type: SHA
- Use AES-128:
- Password: [Redacted] Set:Yes
- Confirm Password: [Redacted]
- Privacy Password: [Redacted] Set:Yes
- Confirm Privacy Password: [Redacted]

At the bottom of the dialog are "OK" and "Cancel" buttons.

Schritt 2: In der CLI können Sie die SNMP-Konfiguration unter **scope monitoring** (Bereichs-Monitoring) überprüfen:

```
<#root>
```

```
ksec-fpr9k-1-A /monitoring #
```

```
show snmp
```

```
Name: snmp
  Admin State: Enabled
  Port: 161
  Is Community Set: No
  Sys Contact:
  Sys Location:
```

```
ksec-fpr9k-1-A /monitoring # show snmp-user
```

```
SNMPv3 User:
  Name                Authentication type
  -----
  user1              Sha
```

```
ksec-fpr9k-1-A /monitoring #
```

```
show snmp-user detail
```

```
SNMPv3 User:
  Name: user1
  Authentication type: Sha
  Password: ****
  Privacy password: ****
  Use AES-128: Yes
```

```
ksec-fpr9k-1-A /monitoring #
```

```
show snmp-trap
```

```
SNMP Trap:
  SNMP Trap          Port      Community  Version V3 Privilege Notification Type
  -----
  192.168.10.100     162      V3         Priv     Traps
```

Schritt 3: Im FXOS-Modus können Sie die SNMP-Konfiguration und Details erweitern:

```
<#root>
```

```
ksec-fpr9k-1-A(fxos)#
```

```
show running-config snmp all
```

```
snmp-server user user1 network-operator auth sha 0x022957ee4690a01f910f1103433e4b7b07d4b5fc priv aes-128
snmp-server host 192.168.10.100 traps version 3 priv user1
```

```
ksec-fpr9k-1-A(fxos)#
```

```
show snmp user
```

---

SNMP USERS			
User	Auth	Priv(enforce)	Groups
user1	sha	aes-128(yes)	network-operator

---

NOTIFICATION TARGET USERS (configured for sending V3 Inform)

---

```
User          Auth Priv
-----
```

```
ksec-fpr9k-1-A(fxos)#
```

```
show snmp host
```

```
-----
Host          Port Version Level Type  SecName
-----
10.48.26.190  162  v3      priv  trap  user1
-----
```

Testen von SNMP-Anfragen.

Sie können die Konfiguration überprüfen und eine SNMP-Anfrage von jedem Gerät mit SNMP-Funktionen ausführen.

Um zu überprüfen, wie die SNMP-Anfrage verarbeitet wird, können Sie SNMP-Debugging verwenden:

```
<#root>
```

```
ksec-fpr9k-1-A(fxos)#
```

```
debug snmp pkt-dump
```

```
ksec-fpr9k-1-A(fxos)# 2017 Oct 16 17:11:54.681396 snmpd: 1281064976.000000:iso.10.10.1.1.10.10.10.1 =
2017 Oct 16 17:11:54.681833 snmpd:  SNMPPKTSTRT: 3.000000 161 1281064976.000000 1647446526.000000 0.000000
2017 Oct 16 17:11:54.683952 snmpd: 1281064976.000000:iso.10.10.1.2.10.10.10.2.83886080 = STRING: "mg
2017 Oct 16 17:11:54.684370 snmpd:  SNMPPKTSTRT: 3.000000 162 1281064976.000000 1647446526.000000 0.000000
```

---

Achtung: Ein Debugging kann die Geräteleistung beeinträchtigen.

---

## Verifizieren von FXOS SNMP für FPR2100

### FXOS SNMPv2-Verifizierungen

Überprüfen der Konfiguration über die CLI:

```
<#root>
```

```
FP2110-4 /monitoring #
```

```
show snmp
```

```
Name: snmp
  Admin State: Enabled
  Port: 161
  Is Community Set: Yes
  Sys Contact:
  Sys Location:
```



FP2110-4 /monitoring #

**show snmp-trap**

```
SNMP Trap:
  SNMP Trap          Port      Version V3 Privilege Notification Type
-----
  10.48.26.190      162      V2c      Noauth      Traps
```

Bestätigen des SNMP-Verhaltens.

Sie können überprüfen, ob Sie das FXOS abrufen und eine SNMP-Anfrage von einem Host oder einem beliebigen Gerät mit SNMP-Funktionen senden können.

Verwenden Sie den Befehl **capture-traffic**, um die SNMP-Anfrage und -Reaktion anzuzeigen:

<#root>

>

**capture-traffic**

Please choose domain to capture traffic from:

0 - management0

Selection?

0

Please specify tcpdump options desired.

(or enter '?' for a list of supported options)

Options:

**udp port 161**

HS\_PACKET\_BUFFER\_SIZE is set to 4.

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on management0, link-type EN10MB (Ethernet), capture size 96 bytes

13:50:50.521383 IP 10.48.26.190.42224 > FP2110-4.snmp: C=cisco123 GetNextRequest(29) interfaces.ifTable

13:50:50.521533 IP FP2110-4.snmp > 10.48.26.190.42224: C=cisco123 GetResponse(32) interfaces.ifTable

^C

Caught interrupt signal

Exiting.

2 packets captured

2 packets received by filter

0 packets dropped by kernel

## **FXOS SNMPv3-Verifizierungen**

Überprüfen der Konfiguration über die CLI:

<#root>

FP2110-4 /monitoring #

**show snmp**

Name: snmp  
Admin State: Enabled  
Port: 161  
Is Community Set: No  
Sys Contact:  
Sys Location:

FP2110-4 /monitoring #

**show snmp-user detail**

SNMPv3 User:

Name: user1  
Authentication type: Sha  
Password: \*\*\*\*  
Privacy password: \*\*\*\*  
Use AES-128: Yes

FP2110-4 /monitoring #

**show snmp-trap detail**

SNMP Trap:

SNMP Trap: 10.48.26.190  
Port: 163  
Version: V3  
V3 Privilege: Priv  
Notification Type: Traps

Bestätigen des SNMP-Verhaltens.

Senden Sie eine SNMP-Anfrage, um zu überprüfen, ob Sie das FXOS abrufen können.

Darüber hinaus können Sie die Anfrage erfassen:

<#root>

>

**capture-traffic**

Please choose domain to capture traffic from:

0 - management0

Selection?

0

Please specify tcpdump options desired.

(or enter '?' for a list of supported options)

Options:

**udp port 161**

HS\_PACKET\_BUFFER\_SIZE is set to 4.

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

```
listening on management0, link-type EN10MB (Ethernet), capture size 96 bytes
14:07:24.016590 IP 10.48.26.190.38790 > FP2110-4.snmp: F=r U= E= C= [|snmp]
14:07:24.016851 IP FP2110-4.snmp > 10.48.26.190.38790: F= [|snmp][|snmp]
14:07:24.076768 IP 10.48.26.190.38790 > FP2110-4.snmp: F=apr [|snmp][|snmp]
14:07:24.077035 IP FP2110-4.snmp > 10.48.26.190.38790: F=ap [|snmp][|snmp]
^C4 packets captured
Caught interrupt signal
```

Exiting.

```
4 packets received by filter
0 packets dropped by kernel
```

## Verifizieren von FTD-SNMP

So überprüfen Sie die FTD-LINA-SNMP-Konfiguration:

```
<#root>
```

```
Firepower-module1#
```

```
show run snmp-server
```

```
snmp-server host OUTSIDE3 10.62.148.75 community ***** version 2c
no snmp-server location
no snmp-server contact
snmp-server community *****
```

In FTD ab 6.6 können Sie die FTD-Managementschnittstelle für SNMP konfigurieren und verwenden:

```
<#root>
```

```
firepower#
```

```
show running-config snmp-server
```

```
snmp-server group Priv v3 priv
snmp-server group NoAuth v3 noauth
snmp-server user uspriv1 Priv v3 engineID
80000009fe99968c5f532fc1f1b0dbdc6d170bc82776f8b470 encrypted auth sha256
6d:cf:98:6d:4d:f8:bf:ee:ad:01:83:00:b9:e4:06:05:82:be:30:88:86:19:3c:96:42:3b
:98:a5:35:1b:da:db priv aes 128
6d:cf:98:6d:4d:f8:bf:ee:ad:01:83:00:b9:e4:06:05
snmp-server user usnoauth NoAuth v3 engineID
80000009fe99968c5f532fc1f1b0dbdc6d170bc82776f8b470
snmp-server host ngfw-management 10.225.126.168 community ***** version 2c
snmp-server host ngfw-management 10.225.126.167 community *****
snmp-server host ngfw-management 10.225.126.186 version 3 uspriv1
no snmp-server location
no snmp-server contact
```

Zusätzliche Verifizierung:

```
<#root>
```

```
Firepower-module1#
```

```
show snmp-server host
```

```
host ip = 10.62.148.75, interface = OUTSIDE3 poll community ***** version 2c
```

Führen Sie über die SNMP-Server-CLI einen snmpwalk aus:

```
<#root>
```

```
root@host:/Volume/home/admin#
```

```
snmpwalk -v2c -c cisco -OS 10.62.148.48
```

```
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Firepower Threat Defense, Version 10.2.3.1 (Build 43), ASA Versio
```

```
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.2313
```

```
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (8350600) 23:11:46.00
```

```
SNMPv2-MIB::sysContact.0 = STRING:
```

```
SNMPv2-MIB::sysName.0 = STRING: Firepower-module1
```

```
SNMPv2-MIB::sysLocation.0 = STRING:
```

```
SNMPv2-MIB::sysServices.0 = INTEGER: 4
```

```
IF-MIB::ifNumber.0 = INTEGER: 10
```

```
IF-MIB::ifIndex.5 = INTEGER: 5
```

```
IF-MIB::ifIndex.6 = INTEGER: 6
```

```
IF-MIB::ifIndex.7 = INTEGER: 7
```

```
IF-MIB::ifIndex.8 = INTEGER: 8
```

```
IF-MIB::ifIndex.9 = INTEGER: 9
```

```
IF-MIB::ifIndex.10 = INTEGER: 10
```

```
IF-MIB::ifIndex.11 = INTEGER: 11
```

```
...
```

Verifizierung der SNMP-Traffic-Statistik.

```
<#root>
```

```
Firepower-module1#
```

```
show snmp-server statistics
```

```
1899 SNMP packets input
```

```
0 Bad SNMP version errors
```

```
0 Unknown community name
```

```
0 Illegal operation for community name supplied
```

```
0 Encoding errors
```

```
1899 Number of requested variables
```

```
0 Number of altered variables
```

```
0 Get-request PDUs
```

```
1899 Get-next PDUs
```

```
0 Get-bulk PDUs
```

```
0 Set-request PDUs (Not supported)
```

```
1904 SNMP packets output
```

```
0 Too big errors (Maximum packet size 1500)
```

```
0 No such name errors
```

```
0 Bad values errors
```

```
0 General errors
```

```
1899 Response PDUs
```

## Zulassen von SNMP-Traffic zum FXOS auf FPR4100/FPR9300

Die FXOS-Konfiguration auf FPR4100/9300 kann den SNMP-Zugriff pro Quell-IP-Adresse einschränken. Im Abschnitt "Access List Configuration" (Zugriffslistenkonfiguration) wird festgelegt, welche Netzwerke/Hosts das Gerät über SSH, HTTPS oder SNMP erreichen können. Sie müssen sicherstellen, dass SNMP-Abfragen von Ihrem SNMP-Server zulässig sind.

### Konfigurieren der globalen Zugriffsliste über die GUI

The screenshot shows the 'Platform Settings' page in the GUI. The left sidebar has 'Access List' selected. The main content area shows the 'IPv4 Access List' configuration. The table below is a summary of the entries shown in the screenshot:

IP Address	Prefix Length	Protocol
0.0.0.0	0	https
0.0.0.0	0	snmp
0.0.0.0	0	ssh

Below the IPv4 table, the 'IPv6 Access List' section is visible, containing three entries:

IP Address	Prefix Length	Protocol
::	0	https
::	0	snmp
::	0	ssh

### Konfigurieren der globalen Zugriffsliste über die CLI

```
<#root>
ksec-fpr9k-1-A#
scope system
ksec-fpr9k-1-A /system #
  scope services
ksec-fpr9k-1-A /system/services #
  enter ip-block 0.0.0.0 0 snmp
ksec-fpr9k-1-A /system/services/ip-block* #
commit-buffer
```

## Verifizierung

<#root>

```
ksec-fpr9k-1-A /system/services #
```

```
show ip-block
```

Permitted IP Block:

IP Address	Prefix Length	Protocol
0.0.0.0	0	https
0.0.0.0	0	snmp
0.0.0.0	0	ssh

## Verwendung des OID Object Navigator

[Cisco SNMP Object Navigator](#) ist ein Online-Tool, mit dem Sie die verschiedenen OIDs übersetzen und eine kurze Beschreibung abrufen können.

The screenshot shows the Cisco SNMP Object Navigator interface. The main heading is "SNMP Object Navigator". Below the heading, there are navigation tabs: "HOME", "SUPPORT", and "TOOLS & RESOURCES". Under "TOOLS & RESOURCES", the "SNMP Object Navigator" tab is selected. The main content area has a "TRANSLATE/BROWSE" tab selected, with "SEARCH", "DOWNLOAD MIBS", and "MIB SUPPORT - SW" tabs also visible. Below the tabs, there are two options: "Translate" and "Browse The Object Tree". The "Translate" option is active. The instruction reads: "Translate OID into object name or object name into OID to receive object details". The input field "Enter OID or object name:" contains the value "1.3.6.1.4.1.9.9.109.1.1.1". To the right of the input field, there are "examples -" with "OID: 1.3.6.1.4.1.9.9.27" and "Object Name: ifIndex". A "Translate" button is located below the input field. Below the input field, the "Object Information" section is displayed. The "Specific Object Information" section is highlighted with a green background. The information is as follows:

Object	cpmCPUTotalTable
OID	1.3.6.1.4.1.9.9.109.1.1.1
Type	SEQUENCE
Permission	not-accessible
Status	current
MIB	<a href="#">CISCO-PROCESS-MIB</a> ; - <a href="#">View Supporting Images</a>
Description	A table of overall CPU statistics.

Verwenden Sie den Befehl **show snmp-server oid** von der FTD-LINA-CLI aus, um die gesamte Liste der abfragbaren LINA-OIDs abzurufen.

<#root>

>

```
system support diagnostic-cli
```

```
firepower#
```

```
show snmp-server oid
```

```
-----  
[0]      10.10.1.10.10.10.1.1.      sysDescr  
[1]      10.10.1.10.10.10.1.2.      sysObjectID  
[2]      10.10.1.10.10.10.1.3.      sysUpTime  
[3]      10.10.1.1.10.1.1.4.        sysContact  
[4]      10.10.1.1.10.1.1.5.        sysName  
[5]      10.10.1.1.10.1.1.6.        sysLocation  
[6]      10.10.1.1.10.1.1.7.        sysServices  
[7]      10.10.1.1.10.1.1.8.        sysORLastChange  
...  
[1081]   10.3.1.1.10.0.10.1.10.1.9. vacmAccessStatus  
[1082]   10.3.1.1.10.0.10.1.10.1.   vacmViewSpinLock  
[1083]   10.3.1.1.10.0.10.1.10.2.1.3. vacmViewTreeFamilyMask  
[1084]   10.3.1.1.10.0.10.1.10.2.1.4. vacmViewTreeFamilyType  
[1085]   10.3.1.1.10.0.10.1.10.2.1.5. vacmViewTreeFamilyStorageType  
[1086]   10.3.1.1.10.0.10.1.10.2.1.6. vacmViewTreeFamilyStatus  
-----  
firepower#
```

---

**Hinweis:** Der Befehl ist ausgeblendet.

---

## Fehlerbehebung

Die gängigsten SNMP-Case-Generierungen, die von Cisco TAC erkannt werden, sind:

1. Abfragen von FTD LINA SNMP nicht möglich
2. Abfragen von FXOS SNMP nicht möglich
3. Welche SNMP-OID-Werte sollten verwendet werden?
4. Abfragen von SNMP-Traps nicht möglich
5. Monitoring von FMC über SNMP nicht möglich
6. SNMP kann nicht konfiguriert werden
7. SNMP-Konfiguration im Firepower Device Manager

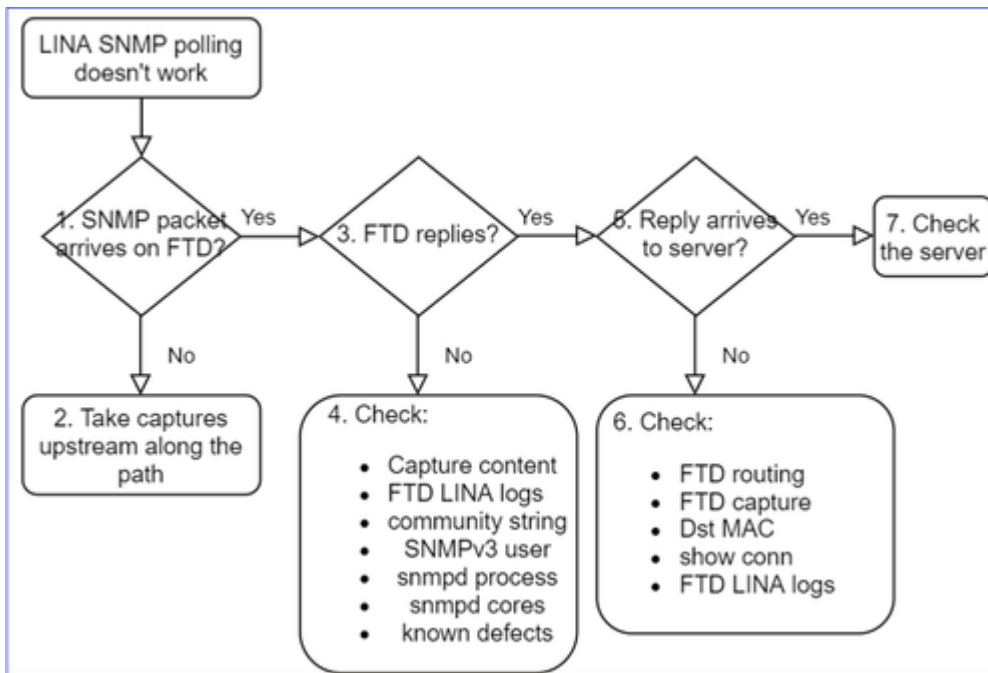
### Abfragen von FTD LINA SNMP nicht möglich

Problembeschreibungen (Beispiele aus echten Cisco TAC-Cases):

- "Daten können nicht über SNMP abgerufen werden"
- "Gerät kann nicht über SNMPv2 abgefragt werden"
- "SNMP funktioniert nicht. Wir möchten die Firewall mit SNMP überwachen, aber nach der Konfiguration treten Probleme auf."
- "Wir haben zwei Monitoring-Systeme, welche die FTD nicht über SNMP v2c oder 3 überwachen können."
- "SNMP-Walk funktioniert nicht auf der Firewall."

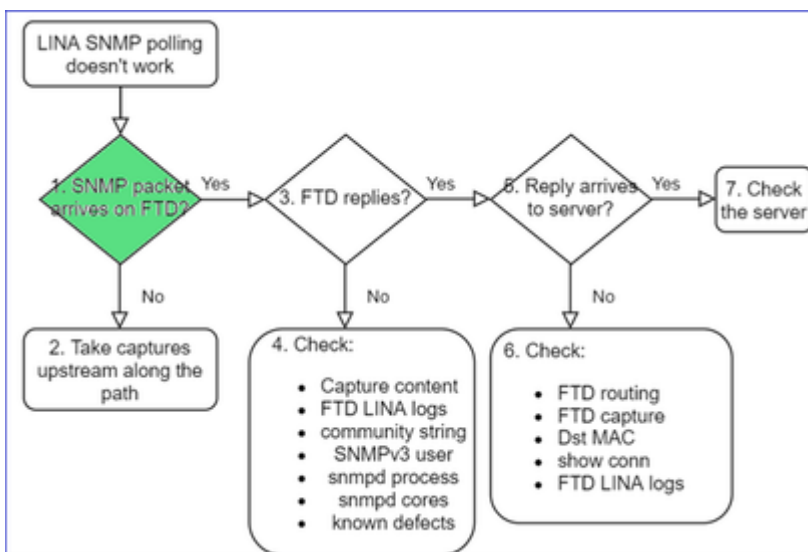
### Empfehlung zur Fehlerbehebung

Es wird empfohlen, das Flussdiagramm bei LINA SNMP-Polling-Problemen mit dem folgenden Prozess zu beheben:



## Details

### 1. Kommt das SNMP-Paket auf FTD an?



- Erfassungen aktivieren, um die Ankunft von SNMP-Paketen zu überprüfen.

SNMP auf der FTD-Verwaltungsschnittstelle (nach Version 6.6) verwendet das Schlüsselwort "management":

```
<#root>
```

```
firepower#
```

```
show run snmp-server
```

```
snmp-server host management 192.168.2.100 community ***** version 2c
```



SNMP auf FTD-Datenschnittstellen verwendet den Namen der Schnittstelle:

```
<#root>
```

```
firepower#
```

```
show run snmp-server
```

```
snmp-server host net201 192.168.2.100 community ***** version 2c
```

Erfassung auf der FTD-Managementschnittstelle:

```
<#root>
```

```
>
```

```
capture-traffic
```

```
Please choose domain to capture traffic from:
```

```
0 - management1
```

```
1 - management0
```

```
2 - Global
```

```
Selection?
```

```
1
```

Erfassung auf der FTD-Datenschnittstelle:

```
<#root>
```

```
firepower#
```

```
capture SNMP interface net201 trace match udp any any eq 161
```

FTD-Paketverfolgung auf der Datenschnittstelle (Funktionsszenario " vor 6.6/9.14.1):

```

FP1150-1# show capture SNMP packet-number 3 trace

1450 packets captured

  3: 21:10:58.642331      802.1Q vlan#208 P0 192.0.2.100.38478 > 192.0.2.30.161:  udp 39
...
Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.0.2.30 using egress ifc identity
...
Result:
input-interface: net208
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow

```

The SNMP packet is terminated on identity interface (ASA or LINA)

FTD-Paketverfolgung auf der Datenschnittstelle (nicht funktionales Szenario – nach 6.6/9.14.1):

```

firepower# show capture SNMP packet-number 1 trace

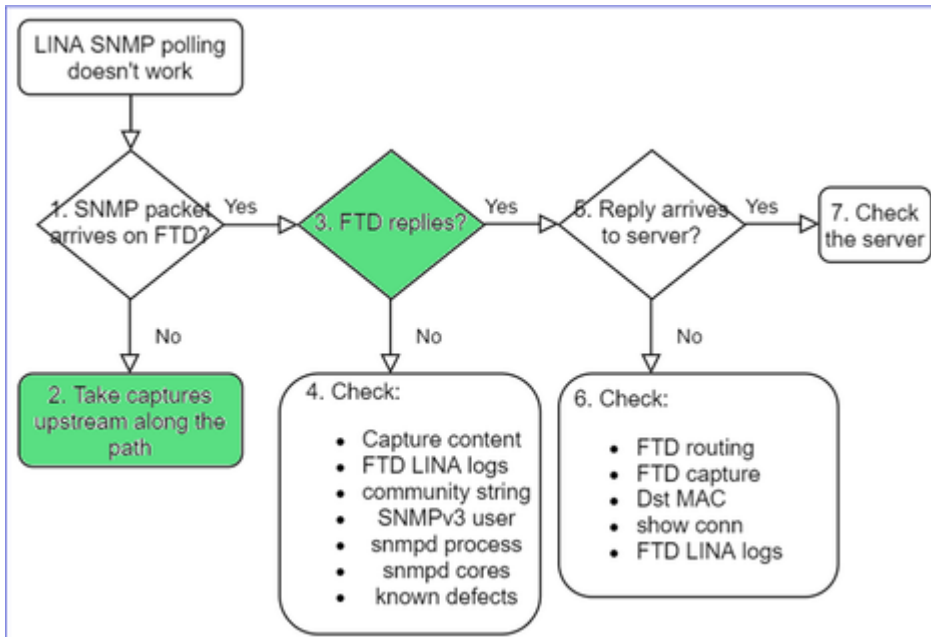
  1: 22:43:39.568101      802.1Q vlan#201 P0 192.168.21.100.58255 > 192.168.21.50.161:  udp 39
...
Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Elapsed time: 9
Config:
nat (nlp_int_tap,net201) source static nlp_server__snmp_192.168.21.100_intf4 interface destination static
0_192.168.21.100_4 0_192.168.21.100_4
Additional Information:
NAT divert to egress interface nlp_int_tap(vrfid:0)
Untranslate 192.168.21.50/161 to 169.254.1.2/161

```

NAT diverts the packet to Snort engine (NLP – Non-Lina Process tap interface)

**2. Falls SNMP-Pakete in der FTD-Eingangserfassung nicht angezeigt werden:**

- Erfassungen upstream entlang des Pfades vornehmen.
- Stellen Sie sicher, dass der SNMP-Server die korrekte FTD-IP verwendet.
- Starten Sie vom Switch-Port zur FTD-Schnittstelle, und bewegen Sie sich stromaufwärts.



### 3. Werden FTD SNMP-Antworten angezeigt?

So überprüfen Sie, ob FTD antwortet:

1. FTD-Ausgangserfassung (LINA- oder MGMT-Schnittstelle)

Suchen Sie nach SNMP-Paketen mit Quellport 161:

```
<#root>
```

```
firepower#
```

```
show capture SNMP
```

```
75 packets captured
```

```

1: 22:43:39.568101      802.1Q vlan#201 P0 192.168.2.100.58255 > 192.168.2.50.161:  udp 39
2: 22:43:39.568329      802.1Q vlan#201 P0 192.168.2.100.58255 > 192.168.2.50.161:  udp 39
3: 22:43:39.569611      802.1Q vlan#201 P0 192.168.2.50.161 > 192.168.2.100.58255:  udp 119

```

In Versionen nach 6.6/9.14.1 gibt es einen weiteren Erfassungspunkt: Erfassung über die NLP-Tipp-Schnittstelle. Die NAT-IP-Adresse gehört zum Bereich 162.254.x.x:

```
<#root>
```

```
admin@firepower:~$
```

```
sudo tcpdump -i tap_nlp
```

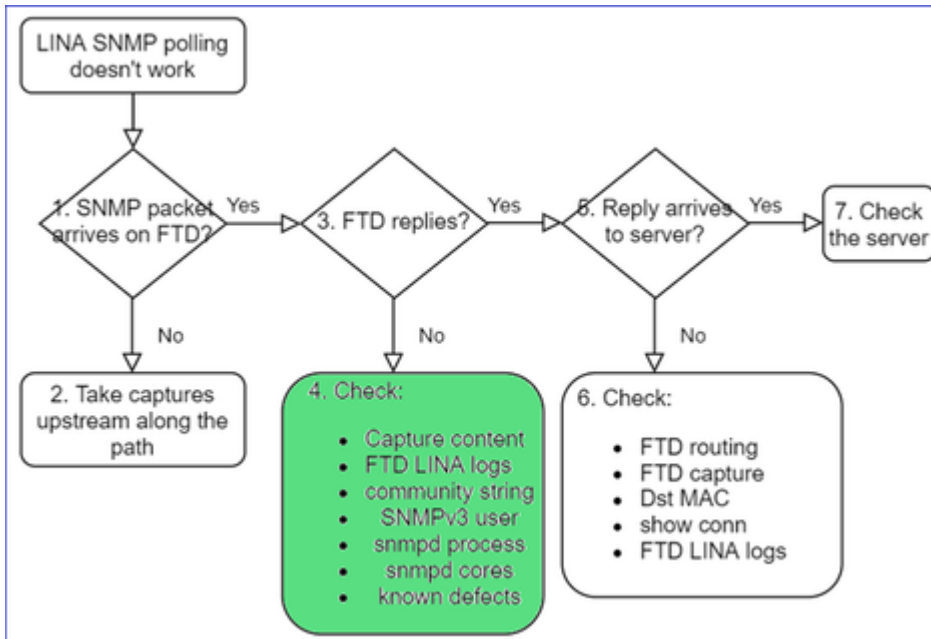
```
listening on tap_nlp, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```

16:46:28.372018 IP 192.168.2.100.49008 > 169.254.1.2.snmp: C="Cisc0123" GetNextRequest(28) E:cisco.9.1
16:46:28.372498 IP 192.168.1.2.snmp > 192.168.2.100.49008: C="Cisc0123" GetResponse(35) E:cisco.9.109

```

### 4. Zusätzliche Kontrollen



antwort: Überprüfen Sie für Firepower 4100/9300-Geräte die [FXOS-Kompatibilitätstabelle](#).

#### Firepower 4100/9300 Compatibility with ASA and Threat Defense

The following table lists compatibility between the ASA or threat defense applications with the Firepower 4100/9300.

The FXOS versions with (EoL) appended have reached their end of life (EoL), or end of support.

**Note** The **bold** versions listed below are specially-qualified companion releases. You should use these software combinations whenever possible because Cisco performs enhanced testing for these combinations.

**Note** Firepower 1000/2100 appliances utilize FXOS only as an underlying operating system that is included in the ASA and threat defense unified image bundles.

**Note** FXOS 2.12/ASA 9.18/Threat Defense 7.2 was the final version for the Firepower 4110, 4120, 4140, 4150, and Security Modules SM-24, SM-36, and SM-44 for the Firepower 9300.

Table 2. ASA or Threat Defense, and Firepower 4100/9300 Compatibility

FXOS Version	Model	ASA Version
2.13(0.198)+ <b>Note</b> FXOS 2.13(0.198)+ does not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use 9.14(1.15)+. Other releases that are paired with 2.12(0.31)+, such as 9.13 or 9.12, are not affected.	Firepower 4112	<b>9.19(x)</b> (recommended) 9.18(x) 9.17(x) 9.16(x) 9.15(1) 9.14(x)
	Firepower 4145 Firepower 4125 Firepower 4115	<b>9.19(x)</b> (recommended) 9.18(x) 9.17(x) 9.16(x) 9.15(1) 9.14(x)
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	9.15(1) 9.14(x) 9.13(1) 9.12(x)
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	<b>9.18(x)</b> (recommended) 9.17(x) 9.16(x) 9.15(1) 9.14(x) 9.13(x)
2.12(0.31)+ <b>Note</b> FXOS 2.12(0.31)+ does not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use 9.14(1.15)+. Other releases that are paired with 2.12(0.31)+, such as 9.13 or 9.12, are not affected.	Firepower 4112	<b>9.18(x)</b> (recommended) 9.17(x) 9.16(x) 9.15(1) 9.14(x)
	Firepower 4145 Firepower 4125 Firepower 4115	<b>9.18(x)</b> (recommended) 9.17(x) 9.16(x) 9.15(1) 9.14(x)
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	9.13(1) 9.12(x)
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	9.12(x) 9.10(x) 9.9(x) 9.8(x)
2.11(1.154)+ <b>Note</b> FXOS 2.11(1.154)+ does not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use	Firepower 4112	<b>9.17(x)</b> (recommended) 9.16(x) 9.15(1) 9.14(x)

b. Überprüfen Sie die FTD-LINA-SNMP-Server-Statistiken:

```
<#root>
firepower#
clear snmp-server statistics

firepower#
show snmp-server statistics

379 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  351 Number of requested variables    <- SNMP requests in
&€|
360 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  351 Response PDUs                    <- SNMP replies out
  9 Trap PDUs
```

c. FTD LINA-Verbindungstabelle

Diese Prüfung ist sehr nützlich, falls Sie Pakete in der Erfassung auf der FTD-Eingangsschnittstelle nicht sehen. Beachten Sie, dass dies nur eine gültige Verifizierung für SNMP auf der Datenschnittstelle ist. Wenn SNMP auf der Verwaltungsschnittstelle (nach 6.6/9.14.1) ausgeführt wird, wird keine Verbindung erstellt.

```
<#root>
firepower#
show conn all protocol udp port 161

13 in use, 16 most used
...
UDP nlp_int_tap 192.168.1.2:161 net201 192.168.2.100:55048, idle 0:00:21, bytes 70277, flags -c
```

d. FTD-LINA-Syslogs

Dies ist ebenfalls eine gültige Verifizierung nur für SNMP auf der Datenschnittstelle! Wenn SNMP auf der Managementschnittstelle ausgeführt wird, wird kein Protokoll erstellt:

```
<#root>
firepower#
show log | i 302015.*161
```

Jul 13 2021 21:24:45: %FTD-6-302015: Built inbound UDP connection 5292 for net201:192.0.2.100/42909 (192.0.2.100)

e. Überprüfen, ob FTD die SNMP-Pakete aufgrund einer falschen Host-Quell-IP verwirft

```
firepower# show capture SNMP packet-number 1 trace
 1: 22:33:00.183248      802.1Q vlan#201 P0 192.168.21.100.43860 > 192.168.21.50.161: udp 39
Phase: 1
Type: CAPTURE
...
Phase: 6
Type: ACCESS-LIST
Result: DROP
...
Result:
input-interface: net201(vrfid:0)
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
flow (NA)/NA

firepower# show run snmp-server
snmp-server host net201 192.168.22.100

firepower# show asp table classify interface net201 dom
Input Table
in id=0x14f65b193b30, priority=501, domain=permit, den
hits=8, user_data=0x0, cs_id=0x0, use_real_addr
src ip/id=192.168.22.100, mask=255.255.255.255,
dst ip/id=169.254.1.2, mask=255.255.255.255, po
input_ifc=net201(vrfid:0), output_ifc=any
```

f. Falsche Anmeldeinformationen (SNMP-Community)

In den Erfassungsinhalten sehen Sie die Community-Werte (SNMP v1 und 2c):

```
snmp
-----
Delta      Source      Destination  Protocol  Length
-----
0.000000  192.168.21.100  192.168.21.50  SNMP
-----
<
> Frame 3: 88 bytes on wire (704 bits), 88 bytes captured (704 bits)
> Ethernet II, Src: VMware_85:3e:d2 (00:50:56:85:3e:d2), Dst: a2:b8:dc
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 201
> Internet Protocol Version 4, Src: 192.168.21.100, Dst: 192.168.21.50
> User Datagram Protocol, Src Port: 45230, Dst Port: 161
v Simple Network Management Protocol
  version: v2c (1)
  community: cisco123
  data: get-next-request (1)
```

g. Falsche Konfiguration (z. B. SNMP-Version oder Community-String)

Es gibt mehrere Möglichkeiten, die SNMP-Konfiguration des Geräts und die Community-Strings zu überprüfen:

<#root>

firepower#

more system:running-config | i community

snmp-server host net201 192.168.2.100 community cISC0123 version 2c

Eine andere Möglichkeit:

<#root>

```
firepower#  
debug menu netsnmp 4
```

#### h. FTD LINA/ASA ASP verwirft Pakete

Dies ist eine nützliche Überprüfung, um zu verifizieren, ob die SNMP-Pakete von der FTD verworfen werden. Löschen Sie zuerst die Zähler (clear asp drop) und testen Sie dann:

```
<#root>
```

```
firepower#  
clear asp drop  
  
firepower#  
show asp drop
```

```
Frame drop:  
  No valid adjacency (no-adjacency)                6  
  No route to host (no-route)                      204  
  Flow is denied by configured rule (acl-drop)      502  
  FP L2 rule drop (l2_acl)                          1
```

```
Last clearing: 19:25:03 UTC Aug 6 2021 by enable_15
```

```
Flow drop:  
Last clearing: 19:25:03 UTC Aug 6 2021 by enable_15
```

#### i. ASP-Erfassungen

ASP-Erfassungen bieten Einblick in die verworfenen Pakete (z. B. ACL oder Adjacency):

```
<#root>  
firepower#  
capture ASP type asp-drop all
```

Testen Sie und überprüfen Sie dann den Inhalt der Erfassung:

```
<#root>  
firepower#  
show capture  
  
capture ASP type asp-drop all [Capturing - 196278 bytes]
```

## j) SNMP-Core (Traceback) – Verifizierungsmethode 1

Diese Überprüfung ist nützlich, wenn Sie Probleme mit der Systemstabilität vermuten:

```
<#root>
```

```
firepower#
```

```
show disk0: | i core
```

```
13 52286547 Jun 11 2021 12:25:16 coredumpfsys/core.snmpd.6208.1626214134.gz
```

## SNMP-Core (Traceback) – Verifizierungsmethode 2

```
<#root>
```

```
admin@firepower:~$
```

```
ls -l /var/data/cores
```

```
-rw-r--r-- 1 root root 685287 Jul 14 00:08 core.snmpd.6208.1626214134.gz
```

Wenn eine SNMP-Core-Datei angezeigt wird, sammeln Sie diese Elemente und wenden Sie sich an Cisco TAC:

- FTD TS-Datei (oder ASA Show Tech)
- snmpd-Core-Dateien

SNMP-Debugs (dies sind versteckte Befehle und nur bei neueren Versionen verfügbar):

```
<#root>
```

```
firepower#
```

```
debug snmp trace [255]
```

```
firepower#
```

```
debug snmp verbose [255]
```

```
firepower#
```

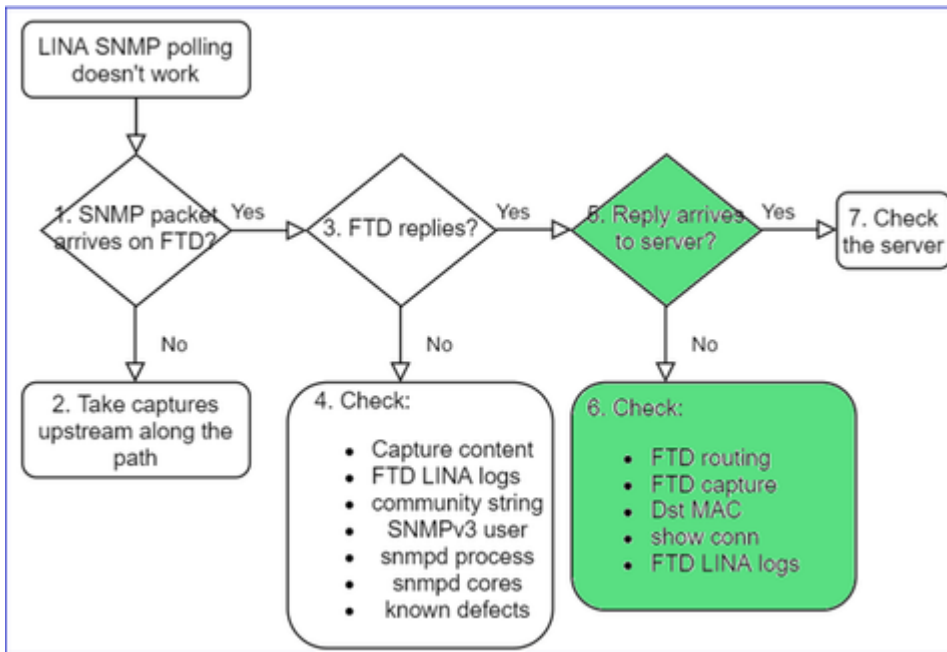
```
debug snmp error [255]
```

```
firepower#
```

```
debug snmp packet [255]
```

**Kommt die SNMP-Antwort der Firewall beim Server an?**





Wenn FTD antwortet, aber die Antwort den Server nicht erreicht, überprüfen Sie Folgendes:

antwort: FTD-Routing

Für das Routing über die FTD-Managementschnittstelle:

```

<#root>
>
show network
  
```

Für das Routing über die FTD-LINA-Datenschnittstelle:

```

<#root>
firepower#
show route
  
```

### b. Verifizierung der Ziel-MAC-Adresse

Verifizierung der Ziel-MAC-Adresse auf der FTD-Managementschnittstelle:

```

<#root>
>
capture-traffic
  
```

Please choose domain to capture traffic from:  
0 - management1

1 - management0  
2 - Global  
Selection?

1

Please specify tcpdump options desired.  
(or enter '?' for a list of supported options)  
Options:

-n -e udp port 161

01:00:59.553385 a2:b8:dc:00:00:02 > 5c:fc:66:36:50:ce, ethertype IPv4 (0x0800), length 161: 10.62.148.19

Verifizierung der Ziel-MAC-Adresse auf der FTD-LINA-Datenschnittstelle:

<#root>

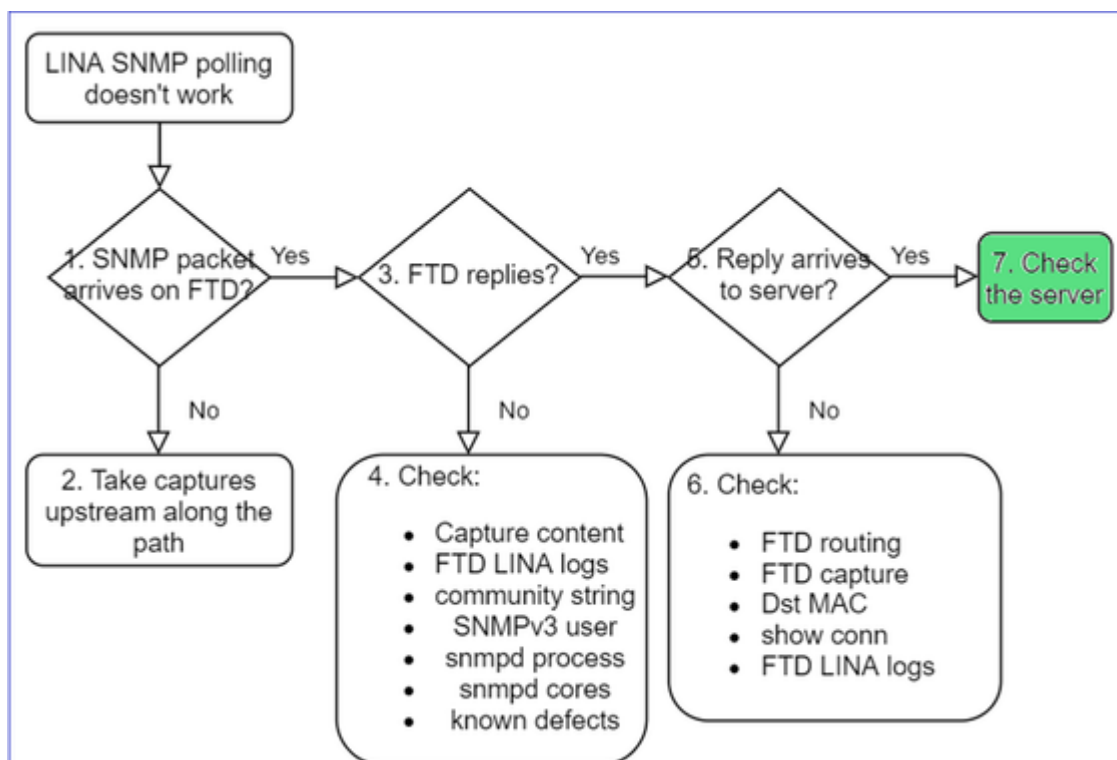
firepower#

show capture SNMP detail

...  
6: 01:03:01.391886 a2b8.dc00.0003 0050.5685.3ed2 0x8100 Length: 165  
802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.40687: [udp sum ok] udp 119 (DF) (ttl 64, i

c. Überprüfen Sie Geräte entlang des Pfads, die SNMP-Pakete verwerfen oder blockieren können.

### Überprüfen des SNMP-Servers



antwort: Überprüfen Sie den Erfassungsinhalt, um die Einstellungen zu überprüfen.

b. Serverkonfiguration überprüfen.

c. Versuchen Sie, den SNMP-Community-Namen zu ändern (z. B. ohne Sonderzeichen).

Sie können einen Endhost oder sogar FMC verwenden, um die Abfrage zu testen, solange die beiden folgenden Bedingungen erfüllt sind:

1. SNMP-Konnektivität ist vorhanden.
2. Die Quell-IP darf das Gerät abfragen.

```
<#root>
```

```
admin@FS2600-2:~$
```

```
snmpwalk -c cisco -v2c 192.0.2.197
```

```
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Firepower Threat Defense, Version 7.0.0 (Build 3), ASA Version 9
```

## Überlegungen zu SNMPv3-Abfragen

- Lizenz: SNMPv3 erfordert eine Strong Encryption-Lizenz. Stellen Sie sicher, dass die Funktion "Export Controlled" (Exportkontrolle) im Smart Licensing-Portal aktiviert ist
- Sie können die Fehlerbehebung mit einem neuen Benutzer/neuen Anmeldeinformationen versuchen.
- Wenn eine Verschlüsselung verwendet wird, können Sie den SNMPv3-Datenverkehr entschlüsseln und die Nutzlast überprüfen, wie in beschrieben:  
<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215092-analyze-firepower-firewall-captures-to-e.html#anc59>
- Ziehen Sie AES128 für die Verschlüsselung in Betracht, falls Ihre Software von Fehlern wie den folgenden betroffen ist:
- Cisco Bug-ID [CSCvy27283](#)

ASA/FTD SNMPv3-Abfragen können mit den Datenschutzalgorithmen AES192/AES256 fehlschlagen.

Cisco Bug-ID [CSCvx45604](#) SNMPv3-Walk schlägt auf Benutzer mit auth sha und priv aes 192 fehl

---

**Hinweis:** Wenn SNMPv3 aufgrund einer nicht übereinstimmenden Algorithmen fehlschlägt, werden die Ausgaben für "show" angezeigt, und die Protokolle enthalten keine offensichtlichen Informationen.

---

```

firepower# show snmp-server statistics
6 SNMP packets input
 0 Bad SNMP version errors
 0 Unknown community name
 0 Illegal operation for community name supplied
 0 Encoding errors
 0 Number of requested variables
 0 Number of altered variables
 0 Get-request PDUs
 0 Get-next PDUs
 0 Get-bulk PDUs
 0 Set-request PDUs (Not supported)
0 SNMP packets output
 0 Too big errors (Maximum packet size 1500)
 0 No such name errors
 0 Bad values errors
 0 General errors
 0 Response PDUs
 0 Trap PDUs

```

Input packets increase, but no replies!

First recommended action:  
Verify your configuration 'show run snmp-server'

Überlegungen zu SNMPv3-Abfragen – Kundenreferenzen

### 1. SNMPv3-SNMP-Walk – Funktionsszenario

<#root>

admin@FS2600-2:~\$

```
snmpwalk -v 3 -u Cisco123 -l authPriv -a SHA -A Cisco123 -x AES -X Cisco123 192.168.21.50
```

```
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Firepower Threat Defense, Version 7.0.0 (Build 3), ASA Version 9.
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.2315
```

In der Erfassung (snmpwalk) sehen Sie eine Antwort für jedes Paket:

```

firepower# show capture SNMP
...
14: 23:44:44.156714      802.1Q vlan#201 P0 192.168.21.100.54240 > 192.168.21.50.161: udp 64
15: 23:44:44.157325      802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.54240: udp 132
16: 23:44:44.160819      802.1Q vlan#201 P0 192.168.21.100.54240 > 192.168.21.50.161: udp 157
17: 23:44:44.162039      802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.54240: udp 238
18: 23:44:44.162375      802.1Q vlan#201 P0 192.168.21.100.54240 > 192.168.21.50.161: udp 160
19: 23:44:44.197850      802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.54240: udp 168
20: 23:44:44.198262      802.1Q vlan#201 P0 192.168.21.100.54240 > 192.168.21.50.161: udp 160
21: 23:44:44.237826      802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.54240: udp 162
22: 23:44:44.238268      802.1Q vlan#201 P0 192.168.21.100.54240 > 192.168.21.50.161: udp 160
23: 23:44:44.277909      802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.54240: udp 159
24: 23:44:44.278260      802.1Q vlan#201 P0 192.168.21.100.54240 > 192.168.21.50.161: udp 160
25: 23:44:44.317869      802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.54240: udp 168

```

Die Erfassungsdatei zeigt nichts Ungewöhnliches:

```

Simple Network Management Protocol
  msgVersion: snmpv3 (3)
  > msgGlobalData
  > msgAuthoritativeEngineID: 80000009feca41e36a96147f184553b777
    1... .... = Engine ID Conformance: RFC3411 (SNMPv3)
    Engine Enterprise ID: ciscoSystems (9)
    Engine ID Format: Reserved/Enterprise-specific (254)
    Engine ID Data: ca41e36a96147f184553b777a7127ccb3710888f
  msgAuthoritativeEngineBoots: 6
  msgAuthoritativeEngineTime: 5089
  msgUserName: Cisco123
  > msgAuthenticationParameters: 79ee0d463313558f4529954f
    > [Authentication: OK]
      > [Expert Info (Chat/Checksum): SNMP Authentication OK]
        [SNMP Authentication OK]
        [Severity level: Chat]
        [Group: Checksum]
      msgPrivacyParameters: 714e78d6bc292c88

```

## 2. SNMPv3-SNMP-Walk â€œ Verschlüsselungsfehler

Tipp #1: Es gibt ein Timeout:

```
<#root>
```

```
admin@FS2600-2:~$
```

```
snmpwalk -v 3 -u Cisco123 -l authPriv -a SHA -A Cisco123 -x DES -X Cisco123 192.168.21.50
```

Timeout: No Response from 192.168.2.1

Hinweis #2: Es gibt viele Anfragen und 1 Antwort:

```

firepower# show capture SNMP
7 packets captured

```

1:	23:25:06.248446	802.1Q vlan#201 P0	192.168.21.100.55137	>	192.168.21.50.161:	udp 64
2:	23:25:06.248613	802.1Q vlan#201 P0	192.168.21.100.55137	>	192.168.21.50.161:	udp 64
3:	23:25:06.249224	802.1Q vlan#201 P0	192.168.21.50.161	>	192.168.21.100.55137:	udp 132
4:	23:25:06.252992	802.1Q vlan#201 P0	192.168.21.100.55137	>	192.168.21.50.161:	udp 163
5:	23:25:07.254183	802.1Q vlan#201 P0	192.168.21.100.55137	>	192.168.21.50.161:	udp 163
6:	23:25:08.255388	802.1Q vlan#201 P0	192.168.21.100.55137	>	192.168.21.50.161:	udp 163
7:	23:25:09.256624	802.1Q vlan#201 P0	192.168.21.100.55137	>	192.168.21.50.161:	udp 163

Hinweis #3: Wireshark-Entschlüsselungsfehler:

```
> User Datagram Protocol, Src Port: 35446, Dst Port: 161
  Simple Network Management Protocol
    msgVersion: snmpv3 (3)
  > msgGlobalData
  > msgAuthoritativeEngineID: 80000009fec41e36a96147f184553b777a7127ccb3710888f
    msgAuthoritativeEngineBoots: 6
    msgAuthoritativeEngineTime: 4359
    msgUserName: Cisco123
  > msgAuthenticationParameters: 1bc9daaa366647cbbb70c5d5
    msgPrivacyParameters: 0000000197eaef1a
  > msgData: encryptedPDU (1)
    encryptedPDU: 452ee7ef0b13594f8b0f6031213217477ecb2422d353581311cade539a27951af821524c...
      Decrypted data not formatted as expected, wrong key?
        [Expert Info (Warning/Malformed): Decrypted data not formatted as expected, wrong key?]
          [Decrypted data not formatted as expected, wrong key?]
          [Severity level: Warning]
          [Group: Malformed]
```

Hinweis 4: Überprüfen Sie die Datei `ma_ctx2000.log` auf die Meldung `error parsing ScopedPDU` (Fehler bei der Analyse von ScopedPDU):

```
<#root>
```

```
> expert
```

```
admin@firepower:~$
```

```
tail -f /mnt/disk0/log/ma_ctx2000.log
```

```
security service 3 error parsing ScopedPDU
security service 3 error parsing ScopedPDU
security service 3 error parsing ScopedPDU
```

Der Fehler beim Parsen von ScopedPDU ist ein starker Hinweis auf einen Verschlüsselungsfehler. In der Datei `ma_ctx2000.log` werden nur Ereignisse für SNMPv3 angezeigt.

### 3. SNMPv3-SNMP-Walk "Authentifizierungsfehler"

Hinweis #1: Authentifizierungsfehler

```
<#root>
```

```
admin@FS2600-2:~$
```

```
snmpwalk -v 3 -u Cisco123 -l authPriv -a MD5 -A Cisco123 -x AES -X Cisco123 192.168.21.50
```

```
snmpwalk: Authentication failure (incorrect password, community or key)
```

Hinweis #2: Es gibt viele Anfragen und Antworten

```
firepower# show capture SNMP
```

```
4 packets captured
```

```
1: 23:25:28.468847 802.1Q vlan#201 P0 192.168.21.100.34348 > 192.168.21.50.161: udp 64
2: 23:25:28.469412 802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.34348: udp 132
3: 23:25:28.474386 802.1Q vlan#201 P0 192.168.21.100.34348 > 192.168.21.50.161: udp 157
4: 23:25:28.475561 802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.34348: udp 137
```

Hinweis #3: Wireshark: Falsch geformtes Paket

```
> Internet Protocol Version 4, Src: 192.168.21.100, Dst: 192.168.21.50
> User Datagram Protocol, Src Port: 47752, Dst Port: 161
> Simple Network Management Protocol
✓ [Malformed Packet: SNMP]
  ▾ [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
    [Malformed Packet (Exception occurred)]
    [Severity level: Error]
    [Group: Malformed]
```

Hinweis 4: Überprüfen Sie die Datei `ma_ctx2000.log` auf die Meldung `Authentication failed` (Authentifizierung fehlgeschlagen):

```
<#root>
```

```
>
```

```
expert
```

```
admin@firepower:~$
```

```
tail -f /mnt/disk0/log/ma_ctx2000.log
```

```
Authentication failed for Cisco123
```

```
Authentication failed for Cisco123
```

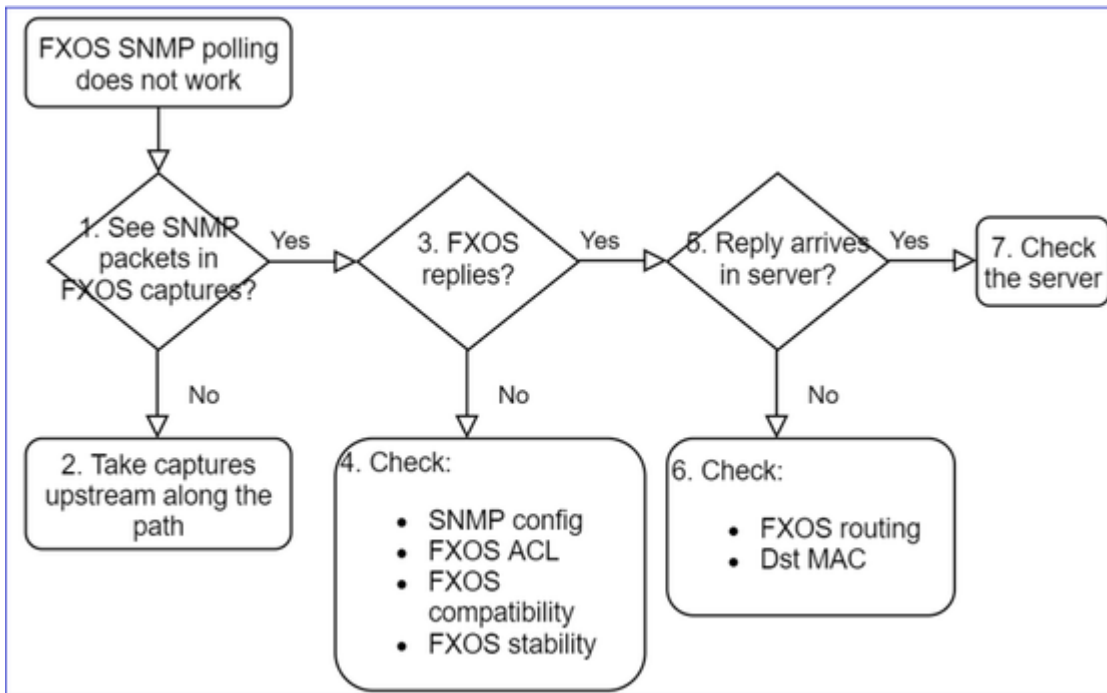
## Abfragen von FXOS SNMP nicht möglich

Problembeschreibungen (Beispiele aus echten Cisco TAC-Cases):

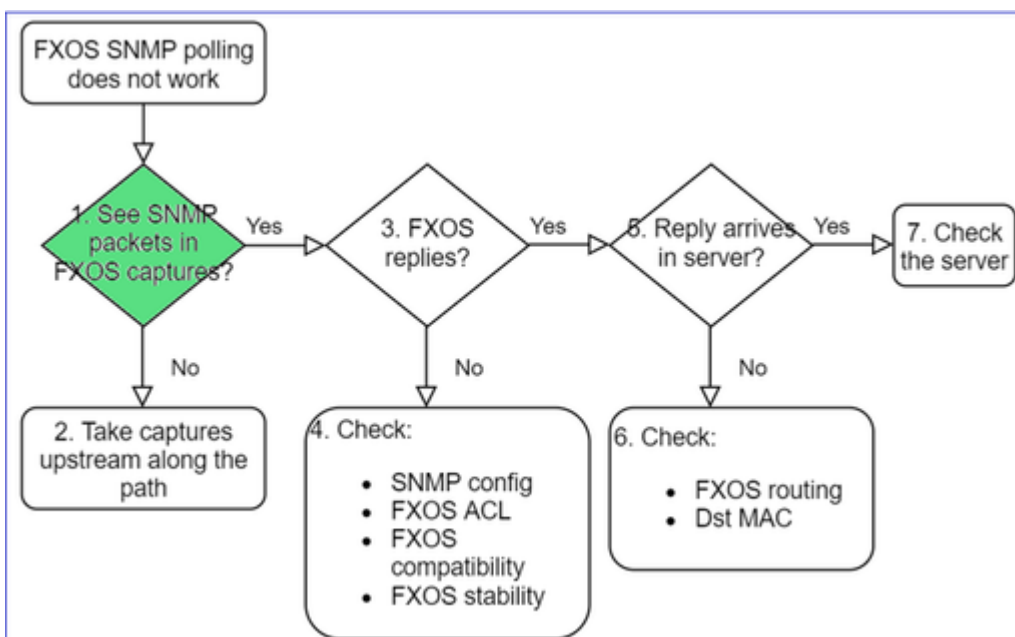
- `SNMP` gibt eine falsche Version für FXOS zurück. Beim Abfragen der Version des FXOS mit `SNMP` ist die Ausgabe schwer zu verstehen.
- Die `SNMP-Community` konnte nicht auf FXOS FTD4115 eingerichtet werden.
- Nach einem FXOS-Upgrade von 2.8 auf 2.9 in der Standby-Firewall erhalten wir ein Timeout, wenn wir versuchen, Informationen über `SNMP` zu erhalten.
- `SNMP-Walk` schlägt in FXOS auf 9300 fehl, funktioniert aber in FXOS auf 4140 in derselben Version. Erreichbarkeit und `Community` sind nicht das Problem.
- Wir möchten 25 `SNMP-Server` auf FPR4K FXOS hinzufügen, aber dies ist nicht möglich.

## Empfohlene Fehlerbehebung

Auf diese Weise werden Fehler im Flussdiagramm bei FXOS `SNMP-Polling-Problemen` behoben:



### 1. Werden SNMP-Pakete in FXOS-Erfassungen angezeigt?



### FPR1xxx/21xx

- Auf FPR1xxx/21xx gibt es keinen Chassis-Manager (Appliance-Modus).
- Sie können die FXOS-Software über die Verwaltungsschnittstelle abfragen.

<#root>

>

capture-traffic

Please choose domain to capture traffic from:

- 0 - management0
- 1 - Global



Selection?

0

Please specify tcpdump options desired.  
(or enter '?' for a list of supported options)  
Options:

```
-n host 192.0.2.100 and udp port 161
```

## 41xx/9300

- Verwenden Sie auf Firepower 41xx/93xx das CLI-Tool Ethalyzer, um eine Chassis-Erfassung zu erstellen:

```
<#root>
```

```
firepower#
```

```
connect fxos
```

```
firepower(fxos)#
```

```
ethalyzer local interface mgmt capture-filter "udp port 161" limit-captured-frames 50 write workspace
```

```
firepower(fxos)#
```

```
exit
```

```
firepower#
```

```
connect local-mgmt
```

```
firepower(local-mgmt)#
```

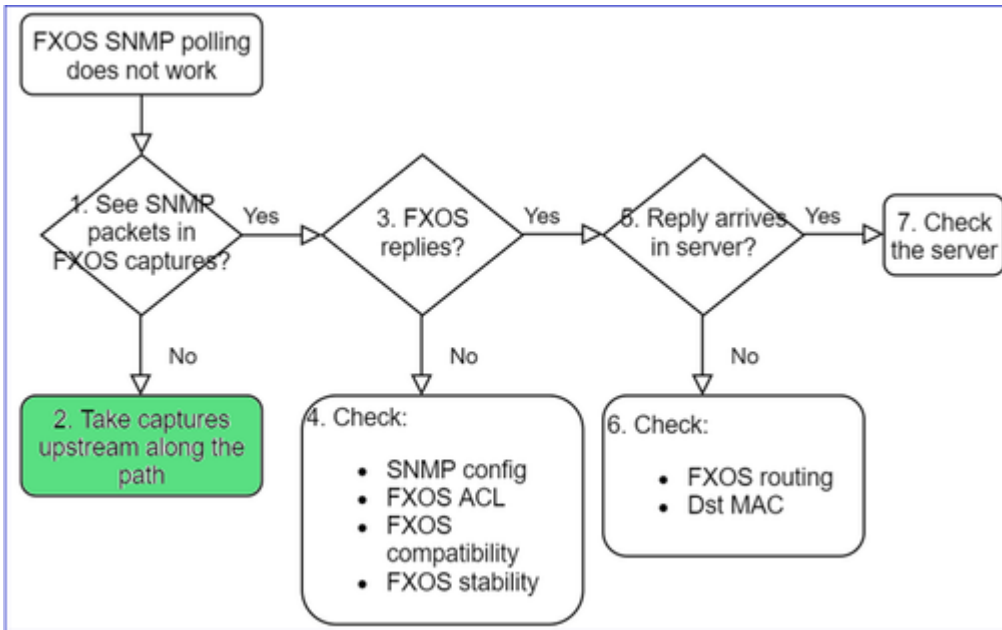
```
dir
```

```
1
```

```
11152 Jul 26 09:42:12 2021 SNMP.pcap  
firepower(local-mgmt)#
```

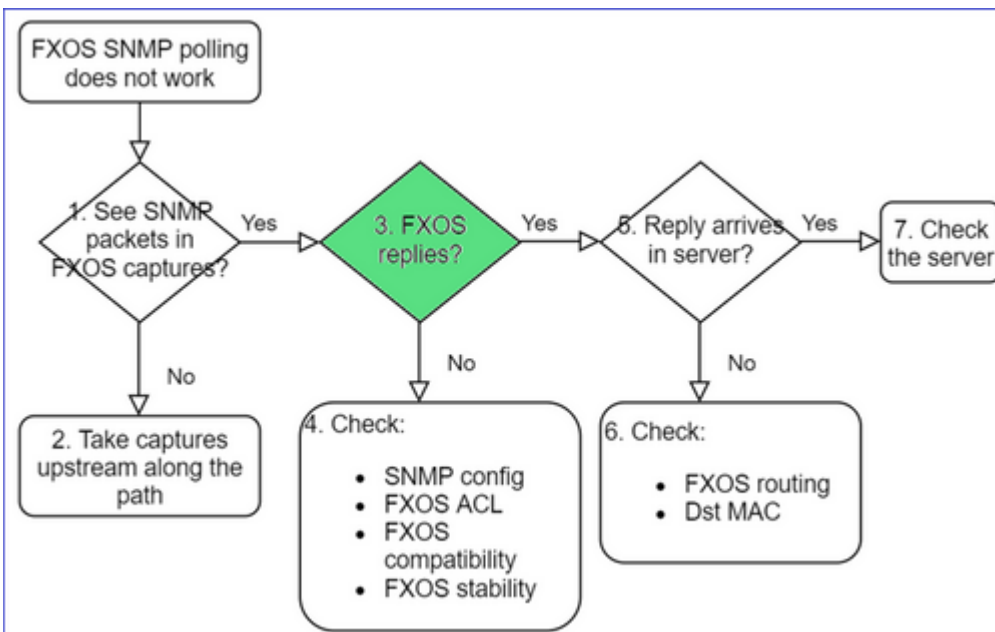
```
copy workspace:///SNMP.pcap ftp://ftp@192.0.2.100/SNMP.pcap
```

## 2. Keine Pakete in FXOS erfasst?



- Erfassungen upstream entlang des Pfades vornehmen

### 3. FXOS-Antworten?



- Funktionsszenario:

<#root>

>

capture-traffic

...

Options:

-n host 192.0.2.23 and udp port 161

HS\_PACKET\_BUFFER\_SIZE is set to 4.

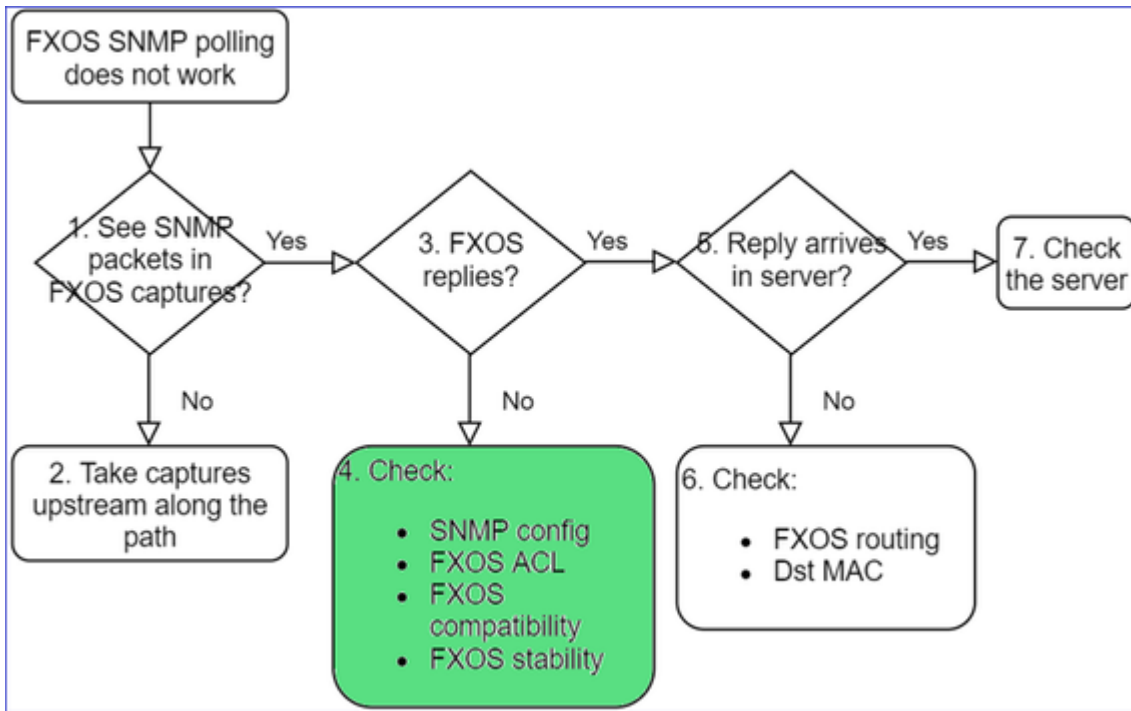
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on management0, link-type EN10MB (Ethernet), capture size 262144 bytes

08:17:25.952457 IP 192.168.2.23.36501 > 192.168.2.28.161: C="Cisco123" GetNextRequest(25) .10.3.1.1.2

08:17:25.952651 IP 192.168.2.28.161 > 192.168.2.23.36501: C="Cisco123" GetResponse(97) .1.10.1.1.1.1

#### 4. FXOS antwortet nicht



#### Zusätzliche Prüfungen

- Überprüfen Sie die SNMP-Konfiguration (über UI oder CLI):

```
<#root>
```

```
firepower#
```

```
scope monitoring
```

```
firepower /monitoring #
```

```
show snmp
```

```
Name: snmp
```

```
Admin State: Enabled
```

```
Port: 161
```

```
Is Community Set: Yes
```

- Seien Sie vorsichtig mit den Sonderzeichen (z. B. `&#x2011;`):

```
<#root>
```

```
FP4145-1#
```

```
connect fxos
```

```
FP4145-1(fxos)#
```

```
show running-config snmp all
```

```
FP4145-1(fxos)#
```

```
show snmp community
```

Community	Group / Access	context	acl_filter
-----	-----	-----	-----
Cisco123	network-operator		

- Verwenden Sie für SNMP v3 `show snmp-user [detail]`.
- Überprüfen der FXOS-Kompatibilität

[https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html#id\\_59069](https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html#id_59069)

#### 4. Falls FXOS nicht antwortet

Überprüfen Sie die FXOS-SNMP-Zähler:

```
FP4145-1# connect fxos
FP4145-1(fxos)# show snmp
...
2243 SNMP packets input
  0 Bad SNMP versions
  28 Unknown community name
  0 Illegal operation for community name
supplied
  28 Encoding errors
  2214 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  2214 Get-next PDUs
  0 Set-request PDUs
3483 SNMP packets output
  0 Too big errors
  1296 Out Traps PDU
```

Diagram illustrating the mapping of SNMP statistics to their respective categories:

- 2243 SNMP packets input → Total requests (polling)
- 28 Unknown community name → Bad community requests (v2c)
- 3483 SNMP packets output → Total replies
- 1296 Out Traps PDU → Traps generated

- Überprüfen Sie die FXOS Access Control List (ACL). Dies gilt nur für FPR41xx/9300-Plattformen.

Wenn der Datenverkehr durch die FXOS-ACL blockiert wird, werden Anforderungen angezeigt, aber keine Antworten:

```
<#root>
```

```
firepower(fxos)#
```

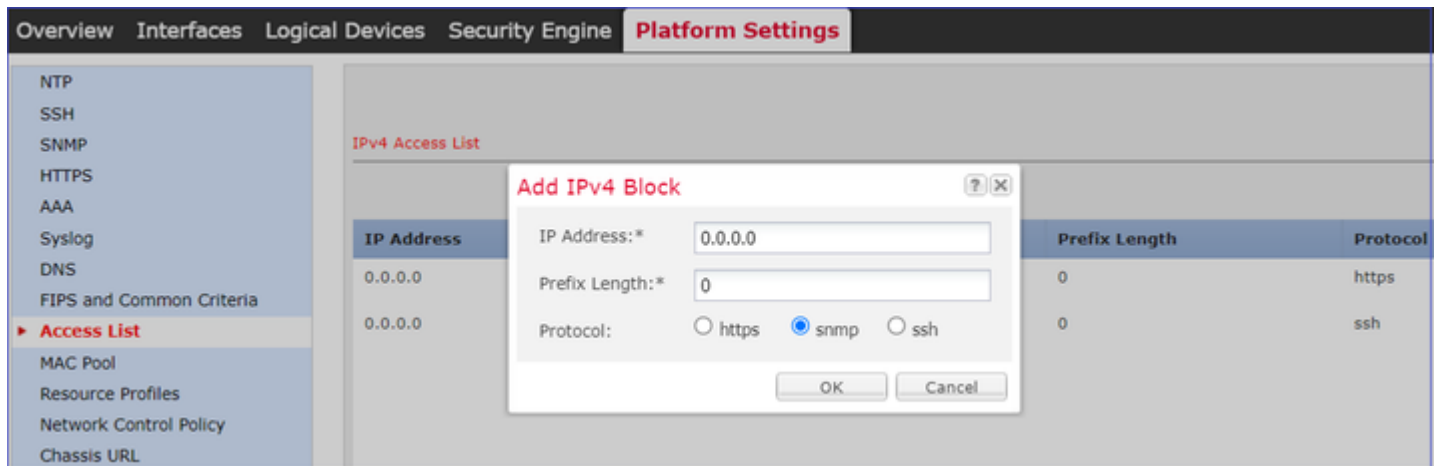
```
ethalyzer local interface mgmt capture-filter
```

```
"udp port 161" limit-captured-frames 50 write workspace:///SNMP.pcap
```

```
Capturing on 'eth0'
```

```
1 2021-07-26 11:56:53.376536964 192.0.2.23 â†’ 192.168.2.37 SNMP 84 get-next-request 10.3.1.10.2.1
2 2021-07-26 11:56:54.377572596 192.0.2.23 â†’ 192.168.2.37 SNMP 84 get-next-request 10.10.1.10.1.1
3 2021-07-26 11:56:55.378602241 192.0.2.23 â†’ 192.168.2.37 SNMP 84 get-next-request 10.3.1.10.2.1
```

Sie können die FXOS-ACL über die Benutzeroberfläche (UI) überprüfen:



Sie können die FXOS-ACL auch über die CLI überprüfen:

```
<#root>
```

```
firepower#
```

```
scope system
```

```
firepower /system #
```

```
scope services
```

```
firepower /system/services #
```

```
show ip-block detail
```

```
Permitted IP Block:
```

```
IP Address: 0.0.0.0
```

```
Prefix Length: 0
```

```
Protocol: snmp
```

- Debuggen von SNMP (nur Pakete). Gilt nur für FPR41xx/9300:

```
<#root>
```

```
FP4145-1#
```

```
connect fxos
```

```
FP4145-1(fxos)#
terminal monitor
```

```
FP4145-1(fxos)#
debug snmp pkt-dump
```

```
2021 Aug 4 09:51:24.963619 snmpd: SNMPPKTSTRT: 1.000000 161 495192988.000000 0.000000 0.000000 0.000000
```

- Debug SNMP (all) â€“ Diese Debug-Ausgabe ist sehr ausfhrlich.

```
<#root>
```

```
FP4145-1(fxos)#
debug snmp all
```

```
2021 Aug 4 09:52:19.909032 snmpd: SDWRAP message Successfully processed
2021 Aug 4 09:52:21.741747 snmpd: Sending it to SDB-Dispatch
2021 Aug 4 09:52:21.741756 snmpd: Sdb-dispatch did not process
```

- berprfen Sie, ob SNMP-bezogene FXOS-Fehler vorliegen:

```
<#root>
```

```
FXOS#
show fault
```

```
Severity Code Last Transition Time ID Description
-----
Warning F78672 2020-04-01T21:48:55.182 1451792 [FSM:STAGE:REMOTE-ERROR]: Result: resource-unavailable C
```

- berprfen Sie, ob snmpd-Cores vorhanden sind:

Auf FPR41xx/FPR9300:

```
<#root>
firepower#
connect local-mgmt

firepower(local-mgmt)#
dir cores
```

```
1 1983847 Apr 01 17:26:40 2021 core.snmpd.10012.1585762000.gz
```

Auf FPR1xxx/21xx:

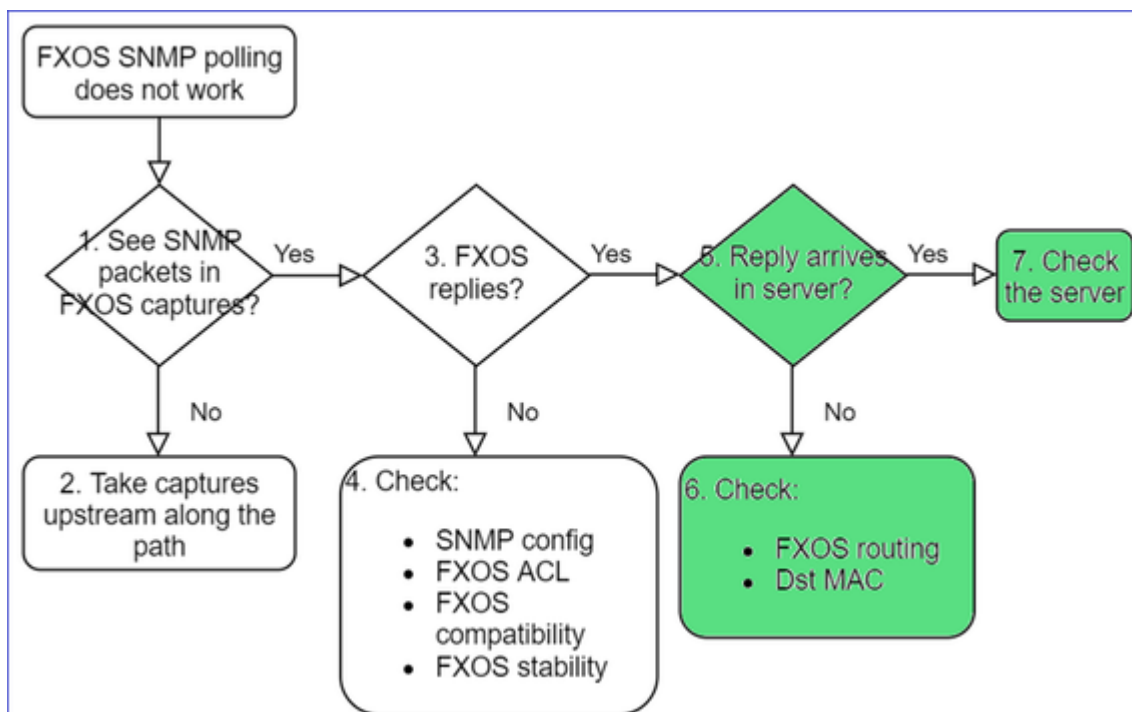
<#root>

```
firepower(local-mgmt)#
```

```
dir cores_fxos
```

Wenn Sie snmpd-Cores sehen, erfassen Sie die Cores zusammen mit dem FXOS-Bundle zur Fehlerbehebung und wenden Sie sich an Cisco TAC.

### 5. Kommt die SNMP-Antwort im SNMP-Server an?



- Überprüfen des FXOS-Routings

Diese Ausgabe stammt von FPR41xx/9300:

<#root>

```
firepower#
```

```
show fabric-interconnect
```

Fabric Interconnect:

	ID	00B IP Addr	00B Gateway	00B Netmask	00B IPv6 Address	00B IPv6 Gateway	Prefix	Operab
A	192.168.2.37	192.168.2.1	10.255.255.128	::	::	64		Operable

- Führen Sie eine Paketerfassung durch, exportieren sie die PCAP (Packet Capture) und überprüfen Sie die Ziel-MAC-Adresse der Antwort.
- Überprüfen Sie zuletzt den SNMP-Server (Erfassung, Konfiguration, Anwendung usw.)

## Welche SNMP-OID-Werte sollten verwendet werden?

Problembeschreibungen (Beispiele aus echten Cisco TAC-Cases):

- "Wir möchten die Cisco Firepower-Geräte überwachen. Bitte geben Sie uns SNMP-OIDs für jede Core-CPU, jeden Arbeitsspeicher und jede Festplatte."
- "Gibt es eine OID, die verwendet werden kann, um den Status der Stromversorgung auf dem ASA 5555-Gerät zu überwachen?"
- "Wir möchten die SNMP-OID des Chassis auf FPR 2K und FPR 4K abrufen."
- "Wir möchten den ASA-ARP-Cache abfragen."
- "Wir benötigen die SNMP-OID für BGP-Peer-Down."

## So finden Sie die SNMP-OID-Werte

Folgende Dokumente enthalten Informationen zu SNMP-OIDs auf Firepower-Geräten:

- Whitepaper zum SNMP-Monitoring mit Cisco Firepower Threat Defense (FTD):

<https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw/white-paper-c11-741739.html>

- Cisco Firepower 4100/9300 FXOS MIB Referenzleitfaden:

[https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/mib/b\\_FXOS\\_4100\\_9300\\_MIBRef.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/mib/b_FXOS_4100_9300_MIBRef.html)

- So suchen Sie auf FXOS-Plattformen nach einer bestimmten OID:

<https://www.cisco.com/c/en/us/support/docs/security/firepower-9000-series/214337-how-to-look-for-an-specific-oid-on-fxos.html>

- Überprüfen der SNMP-OIDs über die CLI (ASA/LINA)

```
<#root>
```

```
firepower#
```

```
show snmp-server ?
```

```
engineID    Show snmp engineID
group       Show snmp groups
host        Show snmp host's
statistics  Show snmp-server statistics
user        Show snmp users
```

```
firepower#
```

```
show snmp-server oid
```

```
<- hidden option!
[1] .1.10.1.1.10.1.2.1  IF-MIB::ifNumber
[2] .1.10.1.1.10.2.2.1.1  IF-MIB::ifIndex
[3] .1.10.1.1.10.2.2.1.2  IF-MIB::ifDescr
[4] .1.10.1.1.10.2.2.1.3  IF-MIB::ifType
```



- Weitere Informationen zu OIDs finden Sie im SNMP Object Navigator

<https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en>

- Führen Sie auf FXOS (41xx/9300) die folgenden beiden Befehle über die FXOS-CLI aus:

```
<#root>
```

```
FP4145-1#
```

```
connect fxos
```

```
FP4145-1(fxos)#
```

```
show snmp internal oids supported create
```

```
FP4145-1(fxos)#
```

```
show snmp internal oids supported
```

```
- SNMP All supported MIB OIDs -0x11a72920
Subtrees for Context:
ccitt
1
1.0.88010.1.1.1.1.1.1.1 ieee8021paeMIB
1.0.88010.1.1.1.1.1.1.2
...
```

### Kurzübersicht zu gängigen OIDs

Anforderung	OID
CPU (LINA)	10.3.1.1.4.1.9.9.109
CPU (Snort)	10.3.1.1.4.1.9.9.109.1.1.1.1.7, 10.3.1.1.4.1.9.9.109.1.1.1.1.10 (FV >= 6.7)
Arbeitsspeicher (LINA)	10.3.1.1.4.1.9.9.48, 10.3.1.1.4.1.9.9.221
Arbeitsspeicher (Linux/FMC)	10.3.1.1.4.1.2021.4
Für FXOS genutzter/freier Speicherplatz (41xx/93xx)	10.3.1.1.4.1.9.9.109.1.1.1.1.12.1, 10.3.1.1.4.1.9.9.109.1.1.1.1.13.1

Schnittstellen	1.10.1.1.1.2
Informationen bzgl. Hochverfügbarkeit	10.3.1.1.4.1.9.9.147.1.10.1.1.1
Cluster-Informationen	10.3.1.1.4.1.9.9.491.1.8.1
VPN-Informationen	10.3.1.1.4.1.9.9.171.1 - Tipp: firepower# show snmp-server oid   i ike
BGP-Status	ENH Cisco Bug-ID <a href="#">CSCux13512</a> :BGP-MIB für SNMP-Abfragen hinzufügen
FPR1K/2K ASA/ASA v Smart Licensing	ENH Cisco Bug-ID <a href="#">CSCvv83590</a> : ASA v/ASA auf der FPR1k/2k: SNMP OID zum Verfolgen des Status von Smart Licensing erforderlich
LINA-SNMP-OIDs für Port-Channel auf FXOS-Ebene	ENH Cisco Bug-ID <a href="#">CSCvu91544</a> :Unterstützung für Lina-SNMP-OIDs für Port-Channel-Schnittstellenstatistiken auf FXOS-Ebene

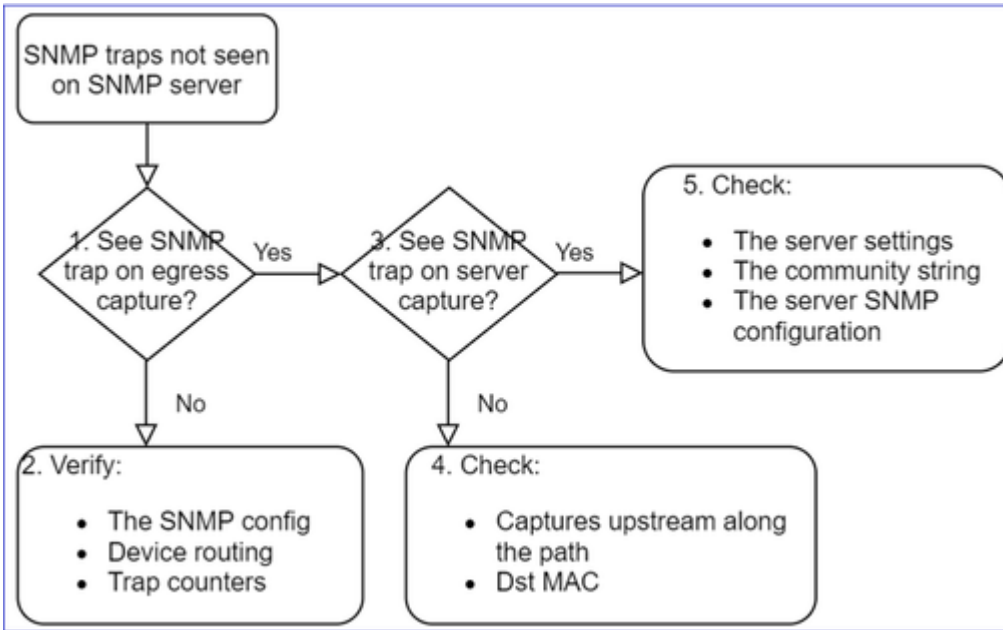
## Abfragen von SNMP-Traps nicht möglich

Problembeschreibungen (Beispiele aus echten Cisco TAC-Cases):

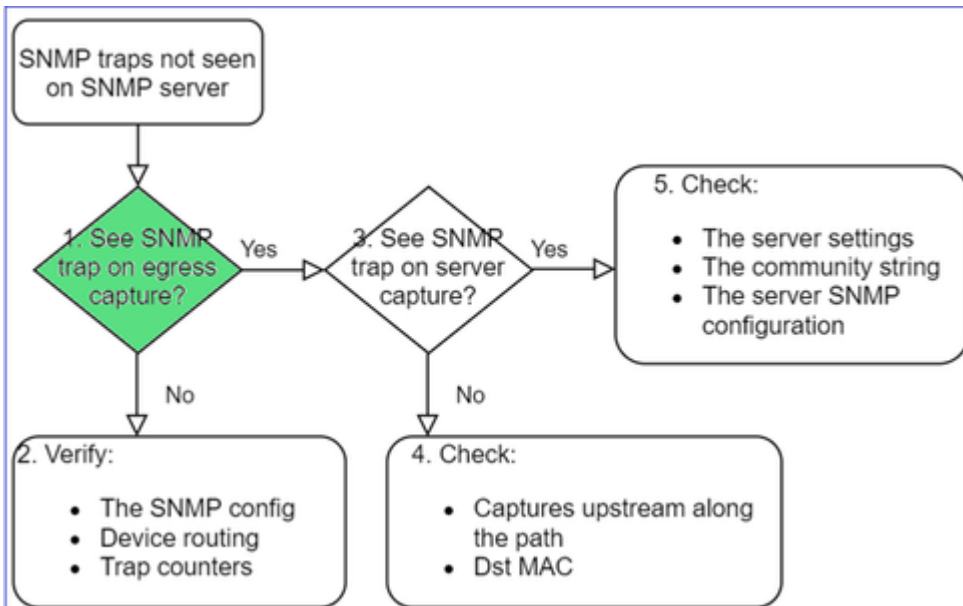
- â€žSNMPv3 von FTD sendet keine Trap an den SNMP-Server.â€œ
- â€žFMC und FTD senden keine SNMP-Trap-Nachrichten.â€œ
- â€žWir haben SNMP auf unserem FTD 4100 für FXOS konfiguriert und SNMPv3 und SNMPv2 ausprobiert, aber beide können keine Traps senden.â€œ
- â€žFirepower SNMP sendet keine Traps an das Monitoring-Tool.â€œ
- â€žFirewall FTD sendet keinen SNMP-Trap an NMS.â€œ
- â€žSNMP-Server-Traps funktionieren nicht.â€œ
- â€žWir haben SNMP auf unserem FTD 4100 für FXOS konfiguriert und SNMPv3 und SNMPv2 ausprobiert, aber beide können keine Traps senden.â€œ

## Empfohlene Fehlerbehebung

Mit diesem Verfahren können Sie das Flussdiagramm für FirePOWER SNMP-Trap-Probleme beheben:



### 1. Werden SNMP-Traps bei der Egress-Erfassung angezeigt?



So erfassen Sie LINA/ASA-Traps auf der Managementschnittstelle:

```
<#root>
```

```
>
```

```
capture-traffic
```

Please choose domain to capture traffic from:

0 - management0

1 - Global

Selection?

```
0
```

Options:

```
-n host 192.168.2.100 and udp port 162
```

So erfassen Sie LINA/ASA-Traps auf der Datenschnittstelle:

```
<#root>
firepower#
  capture SNMP interface net208 match udp any any eq 162
```

So erfassen Sie FXOS-Traps (41xx/9300):

```
<#root>
firepower#
connect fxos

firepower(fxos)#
ethalyzer local interface mgmt capture-filter "udp port 162" limit-captured-frames 500 write workspace

1 2021-08-02 11:22:23.661436002 10.62.184.9 â†’ 10.62.184.23 SNMP 160 snmpV2-trap 10.3.1.1.2.1.1.3.0 1
firepower(fxos)#

exit

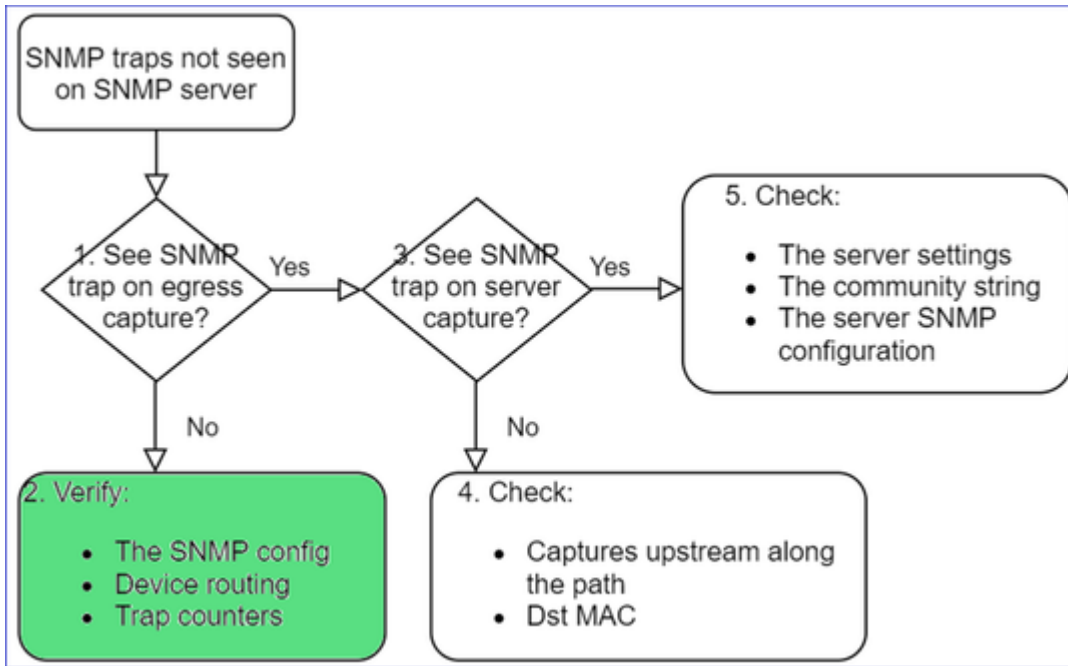
firepower#
connect local-mgmt

firepower(local-mgmt)#
dir

1 11134 Aug 2 11:25:15 2021 SNMP.pcap
firepower(local-mgmt)#

copy workspace:///SNMP.pcap ftp://ftp@192.0.2.100/SNMP.pcap
```

## 2. Wenn Pakete an der Ausgangsschnittstelle nicht angezeigt werden



<#root>

firepower#

show run all snmp-server

```

snmp-server host ngfw-management 10.62.184.23 version 3 Cisco123 udp-port 162
snmp-server host net208 192.168.208.100 community ***** version 2c udp-port 162
snmp-server enable traps failover-state
  
```

### FXOS-SNMP-Traps-Konfiguration:

<#root>

FP4145-1#

scope monitoring

FP4145-1 /monitoring #

show snmp-trap

SNMP Trap:

SNMP Trap	Port	Community	Version	V3 Privilege	Notification	Type
192.168.2.100	162	****	V2c	Noauth	Traps	

Hinweis: Unter 1xxx/21xx werden diese Einstellungen nur bei "**Devices**" (**Geräte**) > "**Device Management**" (**Geräteverwaltung**) > "**SNMP config**" angezeigt.

- LINA/ASA-Routing für Traps über die Managementschnittstelle:

```
<#root>
```

```
>
```

```
show network
```

- LINA/ASA-Routing für Traps über die Datenschnittstelle:

```
<#root>
```

```
firepower#
```

```
show route
```

- FXOS-Routing (41xx/9300):

```
<#root>
```

```
FP4145-1#
```

```
show fabric-interconnect
```

- Trap-Zähler (LINA/ASA):

```
<#root>
```

```
firepower#
```

```
show snmp-server statistics | i Trap
```

```
20 Trap PDUs
```

Und FXOS:

```
<#root>
```

```
FP4145-1#
```

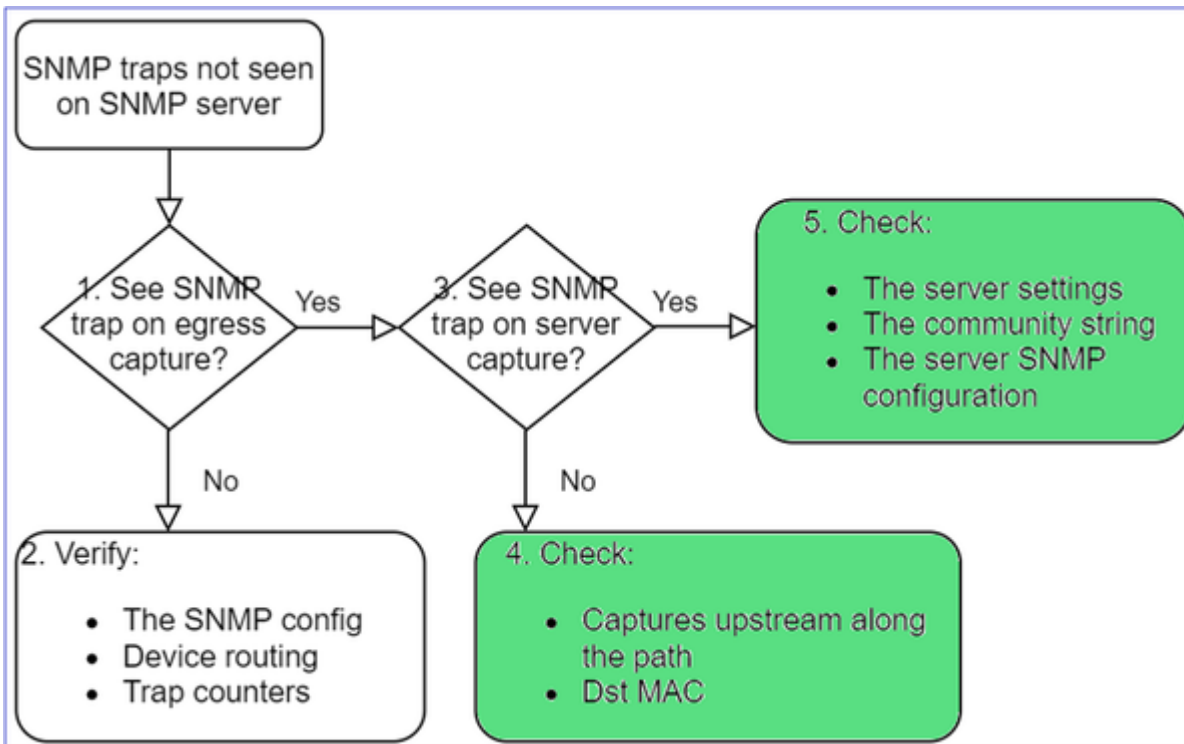
```
connect fxos
```

```
FP4145-1(fxos)#
```

```
show snmp | grep Trap
```

```
1296 Out Traps PDU
```

## Zusätzliche Prüfungen



- Nehmen Sie eine Erfassung auf dem Ziel-SNMP-Server auf.

Weitere zu überprüfende Punkte:

- Erfassungen entlang des Pfads.
- Ziel-MAC-Adresse von SNMP-Trap-Paketen.
- SNMP-Servereinstellungen und -status (z. B. Firewall, offene Ports usw.)
- SNMP-Community-String.
- SNMP-Serverkonfiguration.

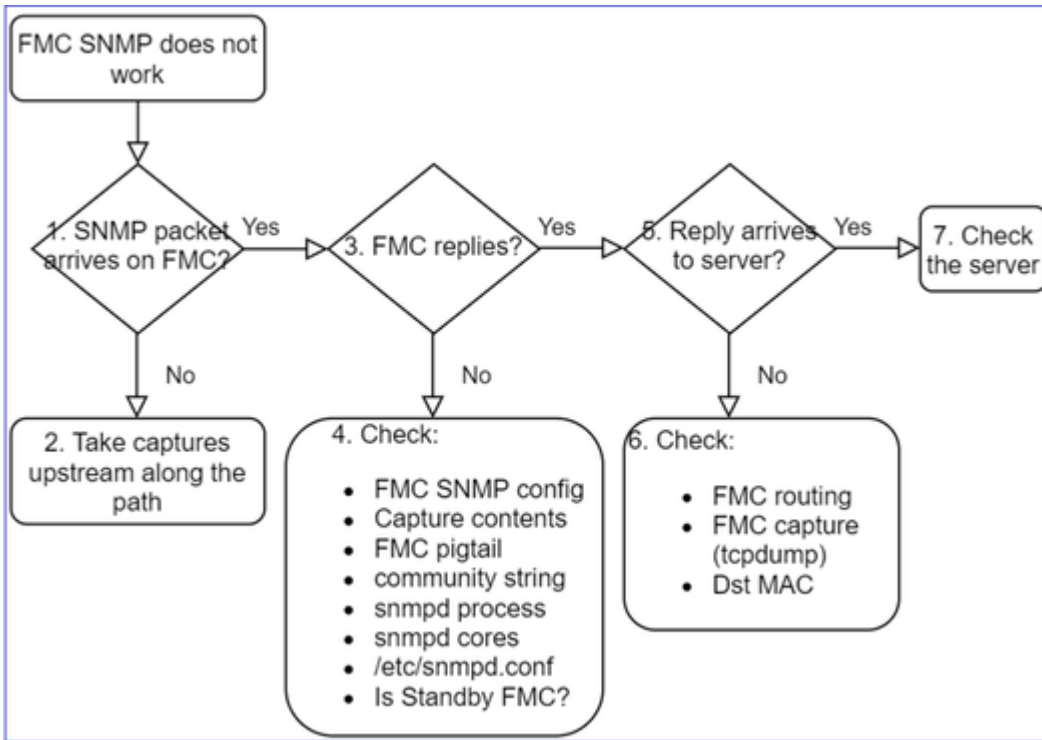
## Monitoring von FMC über SNMP nicht möglich

Problembeschreibungen (Beispiele aus echten Cisco TAC-Cases):

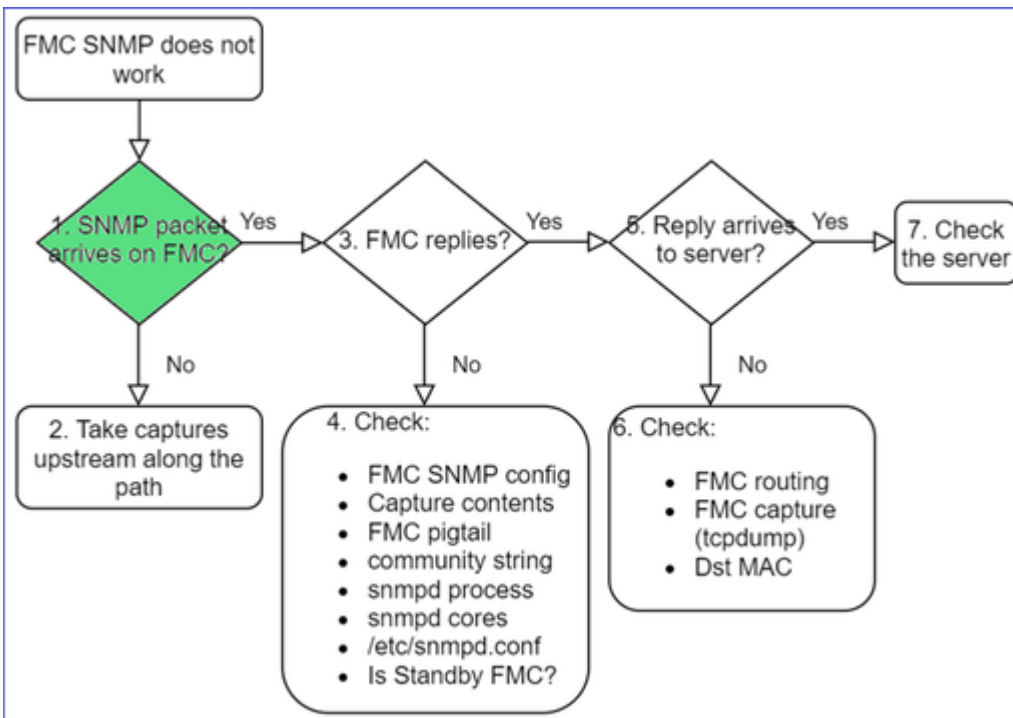
- "SNMP funktioniert auf Standby-FMC nicht."
- "Wir müssen den FMC-Speicher überwachen."
- "Sollte SNMP unter Standby 192.168.4.0.8 FMC funktionieren?"
- "Wir müssen die FMCs so konfigurieren, dass ihre Ressourcen wie CPU, Speicher usw. überwacht werden."

## Fehlerbehebung

Auf diese Weise werden Fehlerbehebungen für das Flussdiagramm bei FMC-SNMP-Problemen durchgeführt:



### 1. SNMP-Paket kommt auf FMC an?



- Erfassung auf der FMC-Managementschnittstelle:

<#root>

```
admin@FS2600-2:~$
```

```
sudo tcpdump -i eth0 udp port 161 -n
```

HS\_PACKET\_BUFFER\_SIZE is set to 4.

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode



```
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
10:58:45.961836 IP 192.168.2.10.57076 > 192.168.2.23.161: C="Cisco123" GetNextRequest(28) .10.3.1.1.4.
```

---

**Tipp:** Speichern Sie die Aufzeichnung im FMC /var/common/-Verzeichnis und laden Sie sie von der FMC-Benutzeroberfläche herunter.

---

```
<#root>
```

```
admin@FS2600-2:~$
```

```
sudo tcpdump -i eth0 udp port 161 -n -w /var/common/FMC_SNMP.pcap
```

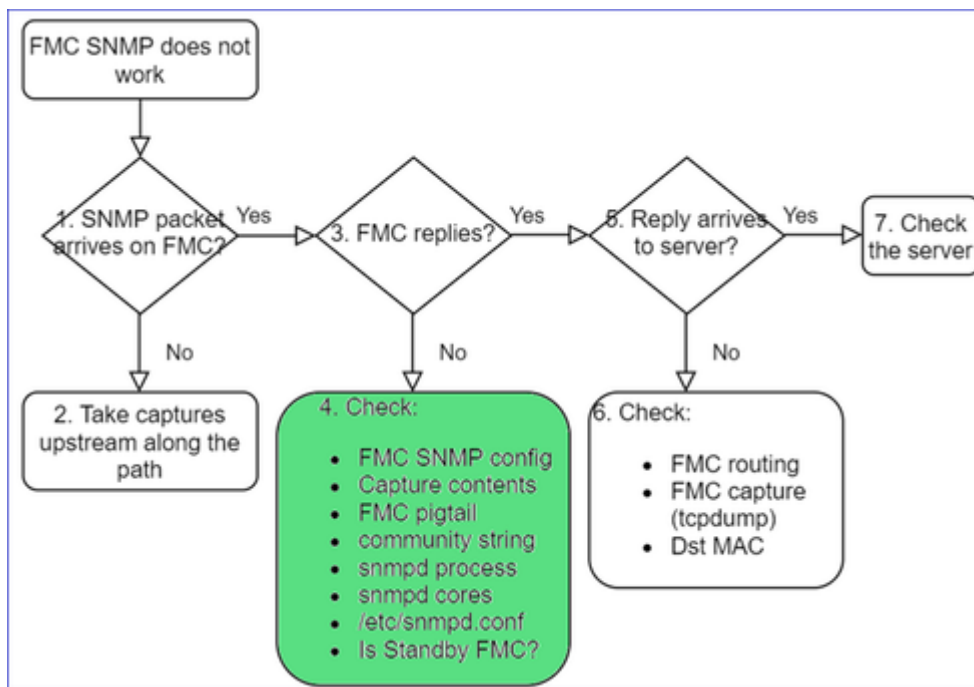
```
HS_PACKET_BUFFER_SIZE is set to 4.
```

```
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
^C46 packets captured
```

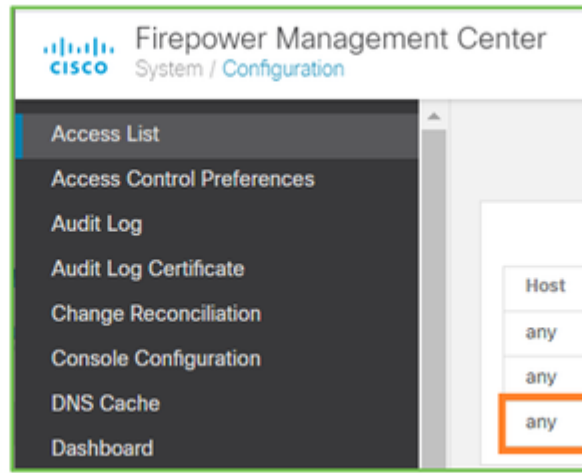
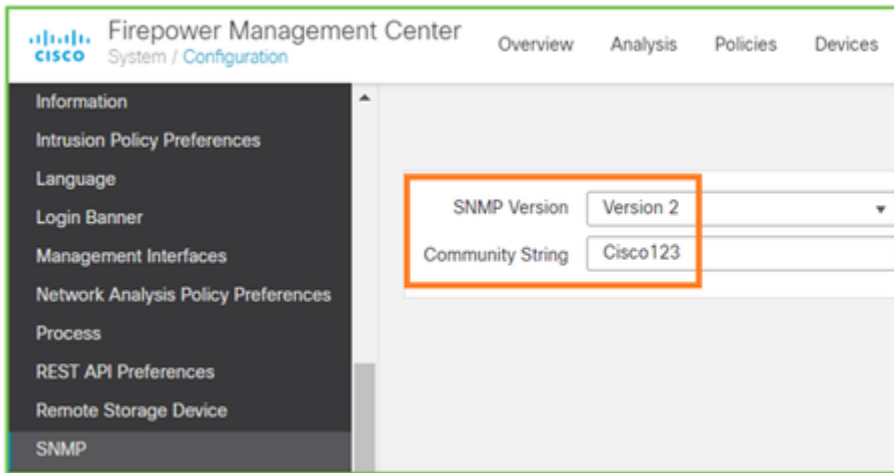
```
46 packets received by filter
```

### Antwortet FMC?



Wenn FMC nicht antwortet, überprüfen Sie Folgendes:

- FMC-SNMP-Konfiguration (System > Configuration)
  1. SNMP-Abschnitt
  2. Abschnitt "Access List" (Zugriffsliste)



Wenn FMC nicht antwortet, überprüfen Sie Folgendes:

- Erfassen (PCAP) von Inhalten
- Community-String (in den Erfassungen zu sehen)
- FMC-Pigtail-Ausgabe (Suchen nach Fehlern, Ausfällen, Nachverfolgungen) und Inhalt von /var/log/snmpd.log
- snmpd-Prozess

<#root>

admin@FS2600-2:~\$

`sudo pmtool status | grep snmpd`

```
snmpd (normal) - Running 12948
Command: /usr/sbin/snmpd -c /etc/snmpd.conf -Ls daemon -f -p /var/run/snmpd.pid
PID File: /var/run/snmpd.pid
Enable File: /etc/snmpd.conf
```

- snmpd-Cores

<#root>

admin@FS2600-2:~\$

`ls -al /var/common | grep snmpd`

```
-rw----- 1 root root          5840896 Aug  3 11:28 core_1627990129_FS2600-2_snmpd_3.12948
```

- Backend-Konfigurationsdatei in /etc/snmpd.conf:

<#root>

admin@FS2600-2:~\$

`sudo cat /etc/snmpd.conf`

```
# additional user/custom config can be defined in *.conf files in this folder
includeDir /etc/snmp/config.d
engineIDType 3
agentaddress udp:161,udp6:161
rocommunity Cisco123
rocommunity6 Cisco123
```

---

**Hinweis:** Wenn SNMP deaktiviert ist, ist die Datei snmpd.conf nicht vorhanden.

---

- Handelt es sich um ein Standby-FMC?

In Versionen vor 6.4.0-9 und vor 6.6.0 sendet das Standby-FMC keine SNMP-Daten (snmpd befindet sich im Status "Waiting"). Dies ist ein erwartungsgemäßes Verhalten. Siehe Erweiterung zu Cisco Bug-ID [CSCvs32303](#)

### SNMP kann nicht konfiguriert werden

Problembeschreibungen (Beispiele aus echten Cisco TAC-Cases):

- "Wir möchten SNMP für Cisco Firepower Management Center und Firepower 4115 Threat Defense konfigurieren."
- "Unterstützung mit SNMP-Konfiguration auf FTD".
- "Wir möchten das SNMP-Monitoring auf meiner FTD-Appliance aktivieren."
- "Wir versuchen, den SNMP-Service in FXOS zu konfigurieren, aber das System lässt uns zum Schluss keinen Puffer zuweisen. Es heißt: Fehler: Änderungen nicht zulässig. Verwenden Sie 'Connect ftd', um Änderungen vorzunehmen."
- "Wir möchten das SNMP-Monitoring auf unserer FTD-Appliance aktivieren."
- "SNMP kann nicht auf FTD konfiguriert werden und das Gerät wird nicht überwacht."

### Vorgehensweise bei Problemen mit der SNMP-Konfiguration

Erste Schritte: Dokumentation!

- Lesen Sie das aktuelle Dokument!
- FMC-Konfigurationsleitfaden:

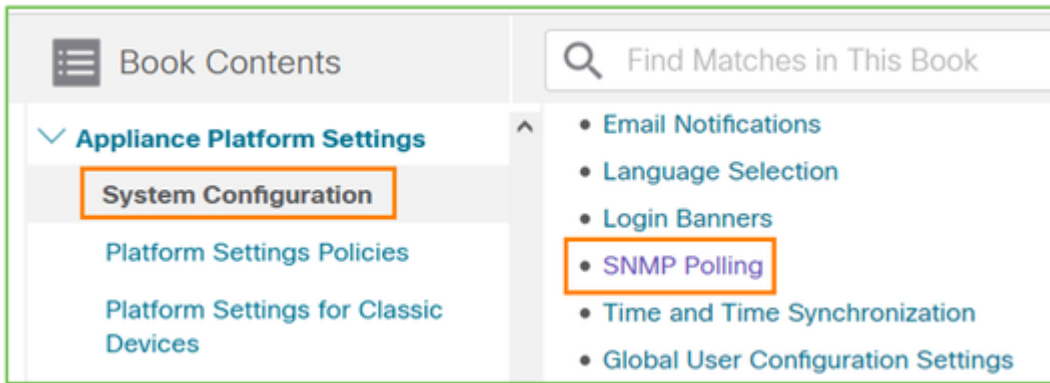
<https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70.html>

- FXOS-Konfigurationsleitfaden:

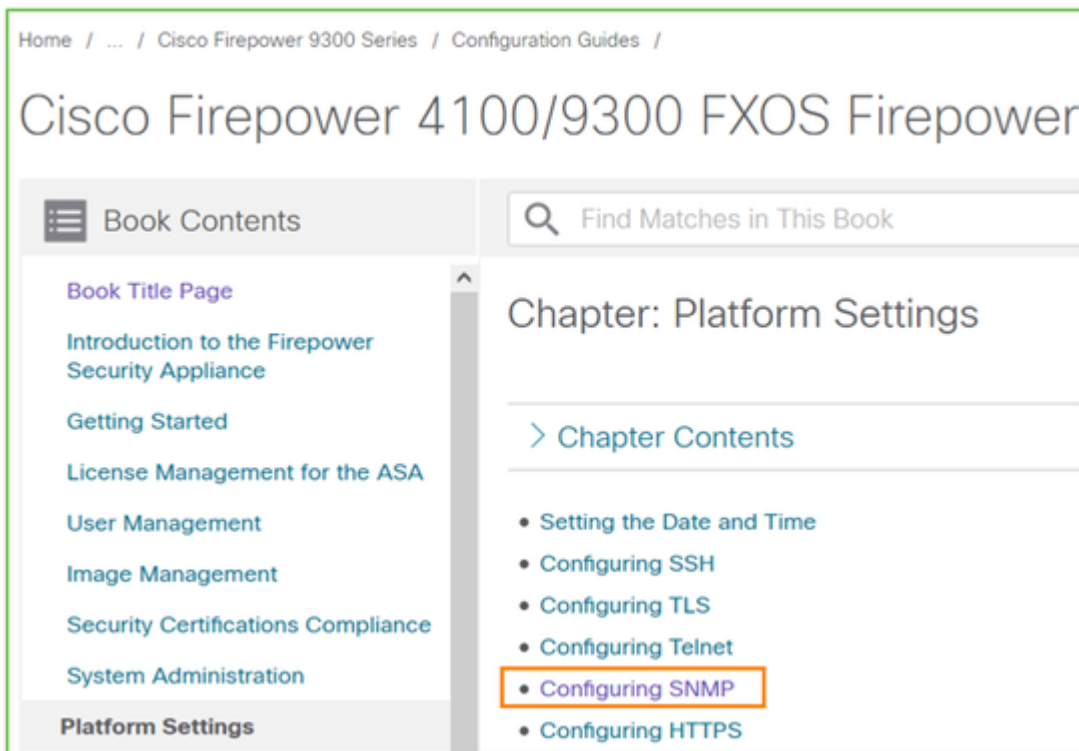
[https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos2101/web-guide/b\\_GUI\\_FXOS\\_ConfigGuide\\_2101/platform\\_settings.html#topic\\_6C6725BBF4BC4333BA207BE9DB115F5](https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos2101/web-guide/b_GUI_FXOS_ConfigGuide_2101/platform_settings.html#topic_6C6725BBF4BC4333BA207BE9DB115F5)

Beachten Sie die verschiedenen SNMP-Dokumente!

FMC SNMP:



FXOS SNMP:



SNMP-Konfiguration der Firepower 41xx/9300:



SNMP-Konfiguration für Firepower 1xxx/21xx:

<ul style="list-style-type: none"> <li>▼ Firepower Threat Defense Interfaces and Device Settings <ul style="list-style-type: none"> <li>Interface Overview for Firepower Threat Defense</li> <li>Regular Firewall Interfaces for Firepower Threat Defense</li> <li>Inline Sets and Passive Interfaces for Firepower Threat Defense</li> <li>DHCP and DDNS Services for Threat Defense</li> <li><b>SNMP for the Firepower 1000/2100</b></li> </ul> </li> </ul>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## SNMP-Konfiguration im Firepower Device Manager (FDM)

Problembeschreibungen (Beispiele aus echten Cisco TAC-Cases):

- â€žWir benötigen Anleitungen zu SNMPv3 auf dem Gerät Firepower mit FDM.â€œ
- â€žDie SNMP-Konfiguration funktioniert auf FPR 2100-Geräten über FDM nicht.â€œ
- â€žDie SNMP v3-Konfiguration kann nicht auf dem FDM funktionieren.â€œ
- â€žFDM 6.7 SNMP-Konfigurationsunterstützung.â€œ
- â€žAktivieren von SNMP v3 in Firepower FDM.â€œ

### Vorgehensweise bei Problemen mit der SNMP-FDM-Konfiguration

- Für Versionen vor 6.7 können Sie die SNMP-Konfiguration mit FlexConfig durchführen:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd-fdm-advanced.html>

- Ab Firepower Version 6.7 wird die SNMP-Konfiguration nicht mehr mit FlexConfig, sondern mit der REST-API durchgeführt:

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/216551-configure-and-troubleshoot-snmp-on-firep.html>

### SNMP-Cheat-Sheets zur Fehlerbehebung

1xxx/21xx/41xx/9300 (LINA/ASA) â€œ Was Sie erfassen müssen, bevor Sie einen Case beim Cisco TAC erstellen

Command	Beschreibung
firepower# show run snmp-server	Überprüfen der ASA/FTD LINA SNMP-Konfiguration.
firepower# show snmp-server statistics	Überprüfen Sie die SNMP-Statistiken für ASA/FTD LINA. Konzentrieren Sie sich auf die Zähler für die Ein- und die Ausgabe von SNMP-Paketen.
> capture-traffic	Erfassen von Traffic auf der Managementschnittstelle.

firepower# capture SNMP-POLL interface net201 trace match udp any any eq 161	Erfassen Sie Datenverkehr an der Datenschnittstelle (name eif "net201") für UDP 161 (SNMP-Abfrage).
firepower# capture SNMP-TRAP interface net208 match udp any any eq 162	Erfassen Sie Datenverkehr über die Datenschnittstelle (name eif "net208") für UDP 162. (SNMP-Traps).
firepower# show capture SNMP-POLL packet-number 1 trace	Verfolgen Sie ein eingehendes SNMP-Paket, das an der ASA/FTD LINA-Datenschnittstelle eingeht.
admin@firepower:~\$ sudo tcpdump -i tap_nlp	Erfassung über die interne Tapp-Schnittstelle von NLP (Non-Lina Process).
firepower# show conn all protocol udp port 161	Überprüfen Sie alle ASA-/FTD-LINA-Verbindungen im UDP 161 (SNMP-Abfrage).
firepower# show log   i 302015.*161	Überprüfen des ASA/FTD-LINA-Protokolls 302015 auf SNMP-Abfragen.
firepower# more system:running-config   i community	Überprüfen des SNMP-Community-Strings.
firepower# debug menu netsnmp 4	Überprüfen der SNMP-Konfiguration und der Prozess-ID.
firepower# show asp table classify interface net201 domain permit match port=161	Überprüfen Sie die Anzahl der Zugriffe auf die SNMP-Zugriffskontrollliste für die Schnittstelle mit dem Namen "net201".
firepower# show disk0:   i core	Überprüfen, ob SNMP-Cores vorhanden sind
admin@firepower:~\$ ls -l /var/data/cores	Überprüfen, ob SNMP-Cores vorhanden sind " gilt nur für FTD.
firepower# show route	Überprüfen der ASA/FTD-LINA-Routing-Tabelle.
> show network	Überprüfen der Routing-Tabelle der FTD-Managementebene.

admin@firepower:~\$ tail -f /mnt/disk0/log/ma_ctx2000.log	Überprüfen/Fehlerbehebung von SNMPv3 auf FTD.
firepower# debug snmp trace [255] firepower# debug snmp verbose [255] firepower# debug snmp error [255] firepower# debug snmp packet [255]	Versteckte Befehle in neueren Versionen. Interne Debugs, nützlich bei der Fehlerbehebung bei SNMP mit Cisco TAC.

41xx/9300 (FXOS) – Was Sie erfassen müssen, bevor Sie einen Case beim Cisco TAC erstellen

Command	Beschreibung
firepower# connect fxos  firepower(fxos)# ethalyzer local interface mgmt capture-filter "udp port 161" limit-captured-frames 50 write workspace:///SNMP-POLL.pcap  firepower(fxos)# exit  firepower# connect local-mgmt  firepower(local-mgmt)# dir  1 11152 Jul 26 09:42:12 2021 SNMP.pcap  firepower(local-mgmt)# copy workspace:///SNMP.pcap <a href="ftp://ftp@192.0.2.100/SNMP.pcap">ftp://ftp@192.0.2.100/SNMP.pcap</a>	FXOS-Erfassung für SNMP-Abfrage (UDP 161)  Upload auf einen Remote-FTP-Server  FTP-IP: 192.0.2.100  FTP-Benutzername: ftp
firepower# connect fxos  firepower(fxos)# ethalyzer local interface mgmt capture-filter "udp port 162" limit-captured-frames 50 write workspace:///SNMP-TRAP.pcap	FXOS-Erfassung für SNMP-Traps (UDP 162)
firepower# scope system  firepower /system # scope services  firepower /system/services # show ip-block detail	Überprüfen der FXOS-ACL
firepower# show fault	Überprüfen auf FXOS-Fehler

firepower# show fabric-interconnect	Überprüfen der Konfiguration der FXOS-Schnittstelle und der Standard-Gateway-Einstellungen
firepower# connect fxos firepower(fxos)# show running-config snmp all	Überprüfen der FXOS-SNMP-Konfiguration
firepower# connect fxos firepower(fxos)# show snmp internal oids supported create firepower(fxos)# show snmp internal oids supported	Überprüfen der FXOS-SNMP-OIDs
firepower# connect fxos firepower(fxos)# show snmp	Überprüfen der FXOS-SNMP-Einstellungen und -Zähler
firepower# connect fxos firepower(fxos)# terminal monitor firepower(fxos)# debug snmp pkt-dump firepower(fxos)# debug snmp all	Debuggen von FXOS SNMP (Pakete oder alle)  Verwenden Sie <code>terminal no monitor</code> und <code>undebug all</code> , um den Vorgang zu stoppen

1xxx/21xx (FXOS) – Was Sie erfassen müssen, bevor Sie einen Case beim Cisco TAC erstellen

Command	Beschreibung
> capture-traffic	Erfassen von Traffic auf der Managementschnittstelle
> show network	Überprüfen der Routing-Tabelle der FTD-Managementebene
firepower# scope monitoring firepower /monitoring # show snmp [host] firepower /monitoring # show snmp-user [detail] firepower /monitoring # show snmp-trap	Überprüfen der FXOS-SNMP-Konfiguration



firepower# show fault	Überprüfen auf FXOS-Fehler
firepower# connect local-mgmt firepower(local-mgmt)# dir cores_fxos firepower(local-mgmt)# dir cores	Auf FXOS-Core-Dateien (Tracebacks) prüfen

FMC â€“ Was Sie erfassen müssen, bevor Sie einen Case beim Cisco TAC erstellen

Command	Beschreibung
admin@FS2600-2:~\$ sudo tcpdump -i eth0 udp port 161 -n	Erfassen von Traffic auf der Managementschnittstelle für SNMP-Abfrage
admin@FS2600-2:~\$ sudo tcpdump -i eth0 udp port 161 -n -w /var/common/FMC_SNMP.pcap	Erfassen von Traffic auf der Managementschnittstelle für SNMP-Abfragen und Speichern in einer Datei
admin@FS2600-2:~\$ sudo pmtool status   grep snmpd	Überprüfen des SNMP-Prozessstatus
admin@FS2600-2:~\$ ls -al /var/common   grep snmpd	Auf SNMP-Core-Dateien (Tracebacks) prüfen
admin@FS2600-2:~\$ sudo cat /etc/snmpd.conf	Überprüfen des Inhalts der SNMP-Konfigurationsdatei

### snmpwalk-Beispiele

Die folgenden Befehle können zur Überprüfung und Fehlerbehebung verwendet werden:

Command	Beschreibung
# snmpwalk -c Cisco123 -v2c 192.0.2.1	Ruft mithilfe von SNMP v2c alle OIDs vom Remote-Host ab.  Cisco123 = Community-String  192.0.2.1 = Zielhost
# snmpwalk -v2c -c Cisco123 -OS 192.0.2.1 10.3.1.1.4.1.9.9.109.1.1.1.3	Ruft mithilfe von SNMP v2c eine bestimmte OID vom Remote-Host ab

iso.3.6.1.4.1.9.9.109.1.1.1.1.3.1 = Gage32: 0	
# snmpwalk -c Cisco123 -v2c 192.0.2.1 .10.3.1.4.1.9.9.109.1.1.1.1 -Ein .10.3.1.1.4.1.9.9.109.1.1.1.1.6.1 = Gauge32: 0	Zeigt die abgerufenen OIDs im numerischen Format an
# snmpwalk -v3 -l authPriv -u cisco -a SHA -A Cisco123 -x AES -X Cisco123 192.0.2.1	Ruft mithilfe von SNMP v3 alle OIDs vom Remote-Host ab.  SNMPv3-Benutzer = cisco  SNMPv3-Authentifizierung = SHA.  SNMPv3-Autorisierung = AES
# snmpwalk -v3 -l authPriv -u cisco -a MD5 -A Cisco123 -x AES -X Cisco123 192.0.2.1	Ruft mithilfe von SNMP v3 (MD5 und AES128) alle OIDs vom Remote-Host ab
# snmpwalk -v3 -l auth -u cisco -a SHA -A Cisco123 192.0.2.1	SNMPv3 nur mit Authentifizierung

## So suchen Sie nach SNMP-Fehlern

1. Navigieren Sie zu <https://bst.cloudapps.cisco.com/bugsearch/search?kw=snmp&pf=prdNm&sb=anfr&bt=custV>.
2. Geben Sie das Schlüsselwort **snmp ein**, und wählen Sie **Select from list aus**.

Tools & Resources

### Bug Search Tool

Save Search Load Saved Search Clear Search Email Current Search

Search For:  × ⓘ  
Examples: CSCtd10124, router crash, etc...

Product:  ▼

Releases:  ▼

Filter: Modified Date:  Status:  Severity:  Rating:  Support Cases:  Bug Type:

Save Search Load Saved Search Clear Search Email Current Search

Search For:  Examples: CSCtd10124, router crash, etc...

Product:   Select from list

Releases:

Modified Date: Status: Severity: Rating: Support Cases: Bug Type:

Filter:

Viewing 1 - 25 of 159 results Sort by  Ex

**CSCvh32876 - ENH:Device level settings of FP2100 should allow to configure ACL and SNMP location**

**Symptom:** This is a feature request for an option to configure access-list to restrict specific host/network to poll device using SNMP and SNMP location. FP2100 allows you to configure ...

Severity: 6 | Status: **Terminated** | Updated: Jan 3, 2021 | Cases: 2 | ☆☆☆☆☆ (0)

Häufigste Produkte:

- Cisco Adaptive Security Appliance (ASA)-Software
- Cisco Firepower 9300-Serie
- Cisco Firepower Management Center Virtual Appliance
- Cisco Firepower NGFW

## Zugehörige Informationen

- [Konfigurieren von SNMP für Threat Defense](#)
- [Konfigurieren von SNMP auf FXOS \(UI\)](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.