Konfigurieren von SNMP-Syslog-Traps für ASA und FTD

Inhalt

Einführung

Dieses Dokument beschreibt, wie die SNMP-Traps (Simple Network Management Protocol) konfiguriert werden, um Syslog-Meldungen an die Cisco Adaptive Security Appliance (ASA) und FirePOWER Threat Defense (FTD) zu senden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundkenntnisse der Cisco ASA
- Grundkenntnisse der Cisco FTD
- Grundkenntnisse des SNMP-Protokolls

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der folgenden Softwareversion:

- Cisco FirePOWER Threat Defense für AWS 6.6.0
- Firepower Management Center Version 6.6.0
- Cisco Adaptive Security Appliance Software Version 9.12(3)9

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Cisco ASA und FTD verfügen über mehrere Funktionen zur Bereitstellung von Protokollinformationen. Es gibt jedoch bestimmte Orte, an denen ein Syslog-Server nicht verfügbar ist. SNMP-Traps bieten eine Alternative, wenn ein SNMP-Server verfügbar ist.

Dies ist ein nützliches Tool, um bestimmte Meldungen zu Fehlerbehebungs- oder Überwachungszwecken zu senden. Wenn es beispielsweise ein relevantes Problem gibt, das während Failover-Szenarien nachverfolgt werden muss, können SNMP-Traps für die Klasse sowohl für FTD als auch für ASA verwendet werden, um sich auf diese Meldungen zu konzentrieren.

Weitere Informationen zu Syslog-Klassen finden Sie in diesem Dokument.

Dieser Artikel enthält Konfigurationsbeispiele für ASA mit CLI (Command Line Interface), FTD mit FMC-Management und FTD mit FirePOWER Device Manager (FDM).

Wenn Cisco Defense Orchestrator (CDO) für FTD verwendet wird, muss diese Konfiguration der FDM-Schnittstelle hinzugefügt werden.

> **Vorsicht**: Für hohe Syslog-Raten wird empfohlen, eine Ratenbeschränkung für Syslog-Meldungen zu konfigurieren, um Auswirkungen auf andere Vorgänge zu verhindern.

Dies sind die Informationen, die für alle Beispiele in diesem Dokument verwendet werden.

SNMP-Version: **SNMPv3**

SNMPv3-Gruppe: **Gruppenname**

SNMPv3-Benutzer: **Admin-User** mit HMAC SHA-Algorithmus für Authentifizierung

IP-Adresse des SNMP-Servers: **10.20.15.12**

ASA/FTD-Schnittstelle für die Kommunikation mit dem SNMP-Server: **Außenbereiche**

Syslog-Nachrichten-ID: **11009**

Konfigurieren

ASA-Konfiguration

Diese Schritte können verwendet werden, um SNMP-Traps auf einem ASA-Gerät zu konfigurieren, indem die folgenden Informationen verwendet werden.

Schritt 1: Konfigurieren Sie die Meldungen, die der Syslog-Liste hinzugefügt werden sollen.

```
logging list syslog-list message 111009
```

Schritt 2: Konfigurieren von SNMPv3-Serverparametern

```
snmp-server enable

snmp-server group group-name v3 auth
snmp-server user admin-user group-name v3 auth sha cisco123
```

Schritt 3: Aktivieren Sie SNMP-Traps.

```
snmp-server enable traps syslog
```

Schritt 4: Fügen Sie die SNMP-Traps als Protokollierungsziel hinzu.

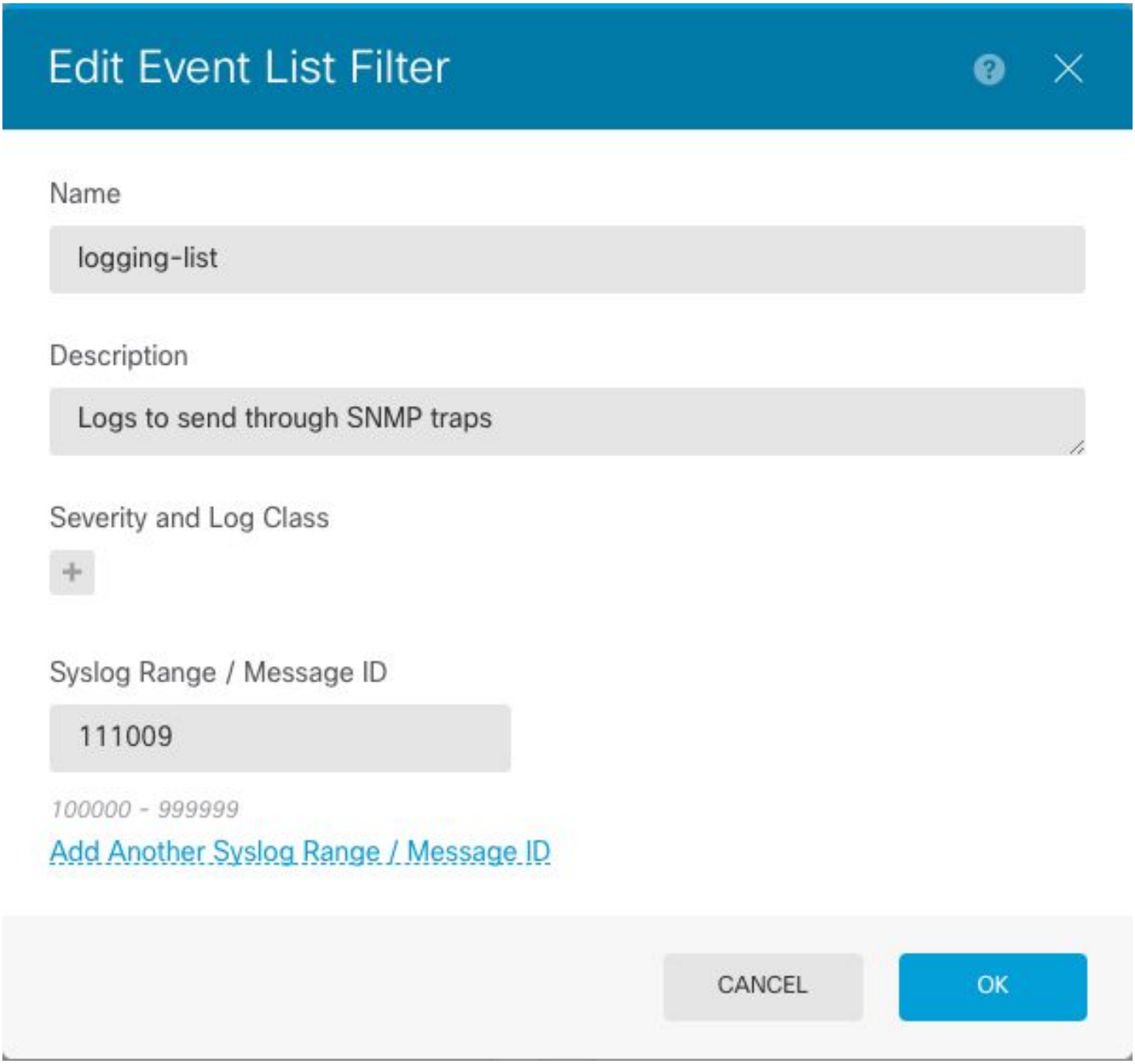
```
logging history syslog-list
```

Von FDM verwaltete FTD-Konfiguration

Diese Schritte können verwendet werden, um eine bestimmte Syslog-Liste zu konfigurieren, die an den SNMP-Server gesendet wird, wenn FTD von FDM verwaltet wird.

Schritt 1: Navigieren Sie zu **Objekte > Ereignislistenfilter**, und wählen Sie auf der Schaltfläche **+** aus.

Schritt 2: Nennen Sie die Event List (Ereignisliste), und fügen Sie die relevanten Klassen oder Nachrichten-IDs ein. Wählen Sie anschließend OK aus.



Schritt 3: Navigieren Sie vom FDM-Hauptbildschirm zu Advanced **Configuration > FlexConfig > FlexConfig Objects**, und wählen Sie die **+** Schaltfläche aus.

Erstellen Sie die nächsten FlexConfig-Objekte mit den aufgeführten Informationen:

Name: **SNMP-Server**

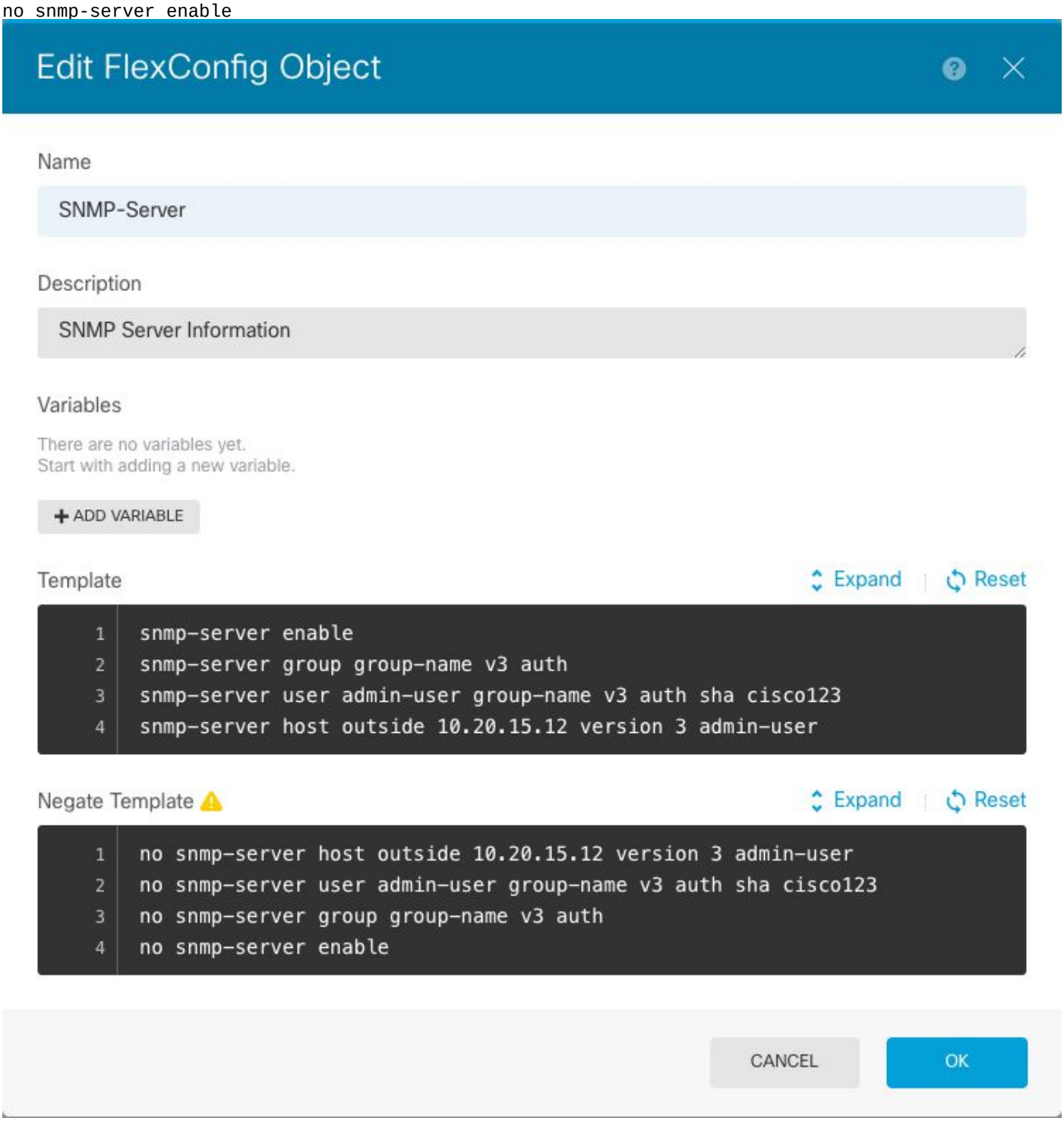
Beschreibung (Optional): **SNMP-Serverinformationen**

Vorlage:

```
snmp-server enable
snmp-server group group-name v3 auth
snmp-server user admin-user group-name v3 auth sha cisco123
snmp-server host outside 10.20.15.12 version 3 admin-user
```

Vorlage negieren:

```
no snmp-server host outside 10.20.15.12 version 3 admin-user
no snmp-server user admin-user group-name v3 auth sha cisco123
no snmp-server group group-name v3 auth
no snmp-server enable
```



Name: **SNMP-Traps**

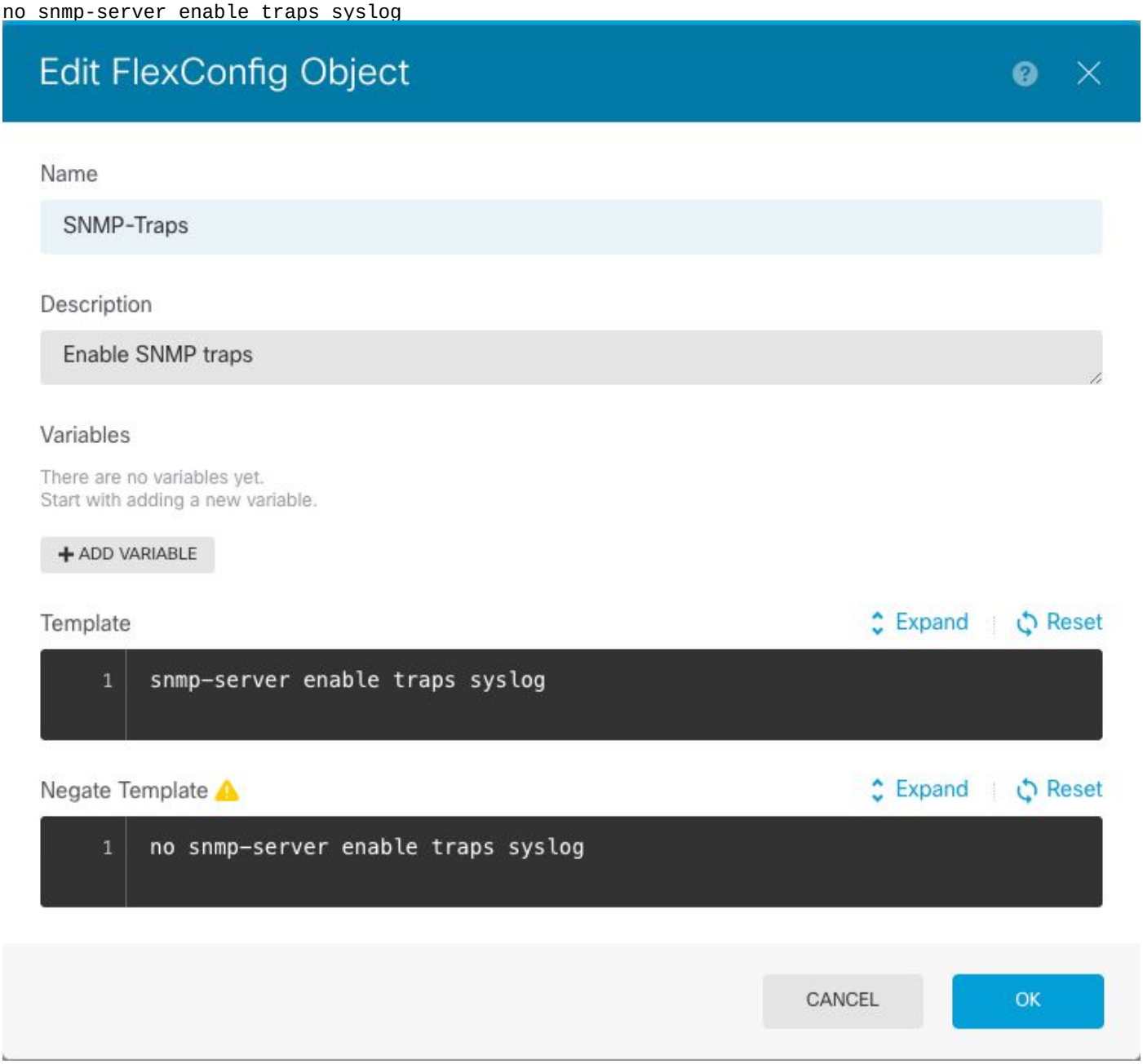
Beschreibung (Optional): **SNMP-Traps aktivieren**

Vorlage:

```
snmp-server enable traps syslog
```

Vorlage negieren:

```
no snmp-server enable traps syslog
```



Name: **Protokollierungsverlauf**

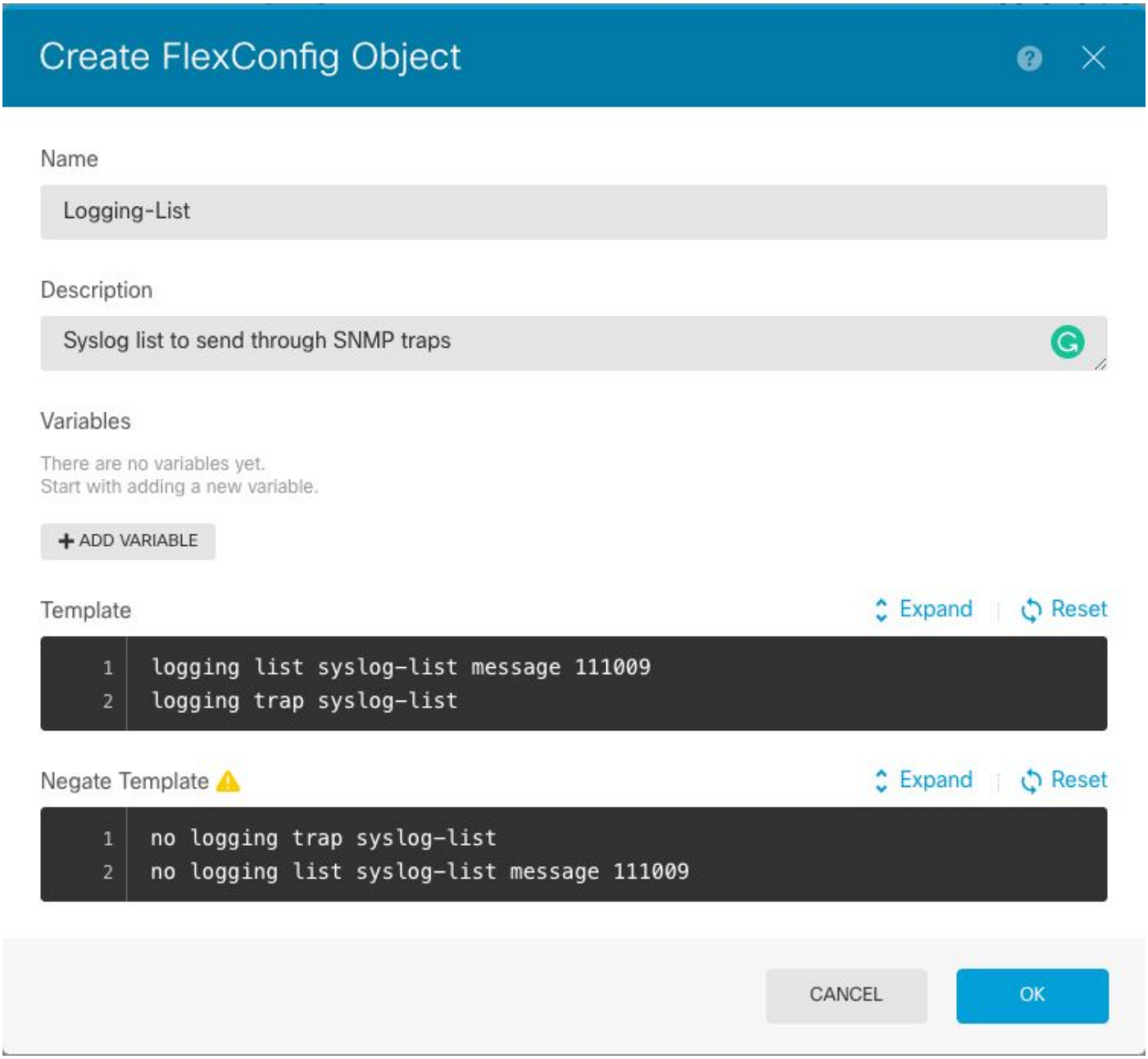
Beschreibung (Optional): **Objekt zum Festlegen von SNMP-Traps für Syslog-Meldungen**

Vorlage:

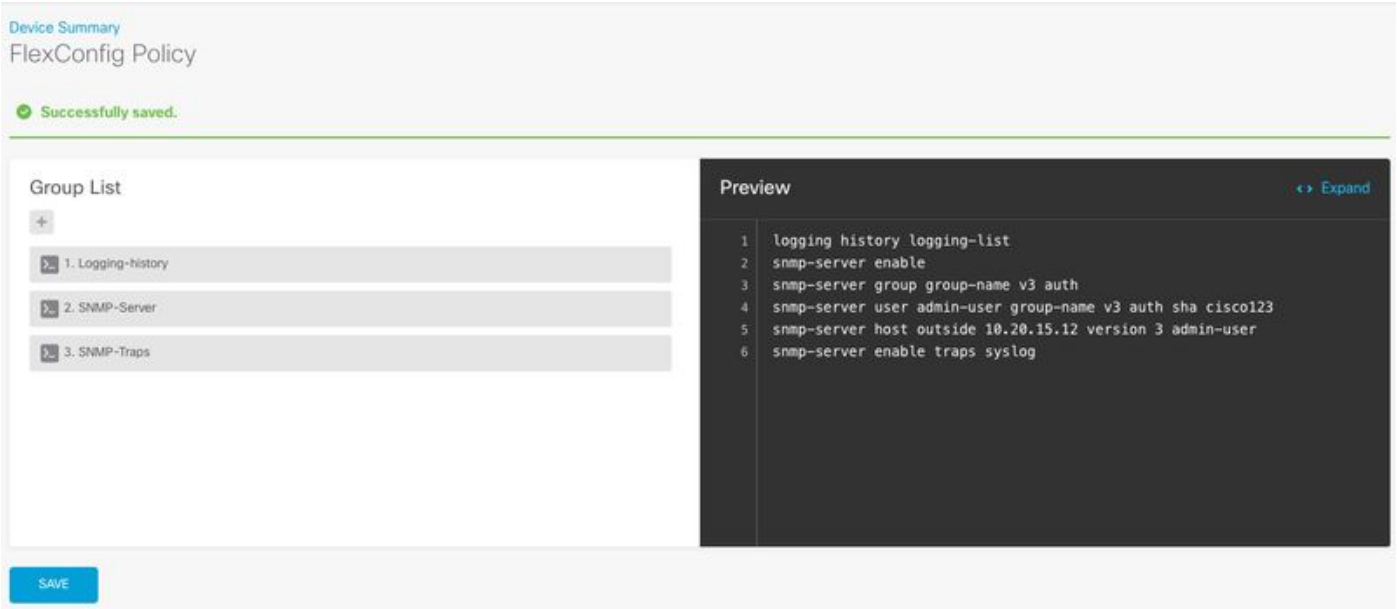
```
logging history logging-list
```

Vorlage negieren:

```
no logging history logging-list
```



Schritt 4: Navigieren Sie zu **Erweiterte Konfiguration > FlexConfig > FlexConfig Policy**, und fügen Sie alle im vorherigen Schritt erstellten Objekte hinzu. Die Reihenfolge ist irrelevant, da die abhängigen Befehle im gleichen Objekt enthalten sind (SNMP-Server). Wählen Sie **Speichern aus**, sobald die drei Objekte vorhanden sind und der Abschnitt **Vorschau** die Liste der Befehle anzeigt.



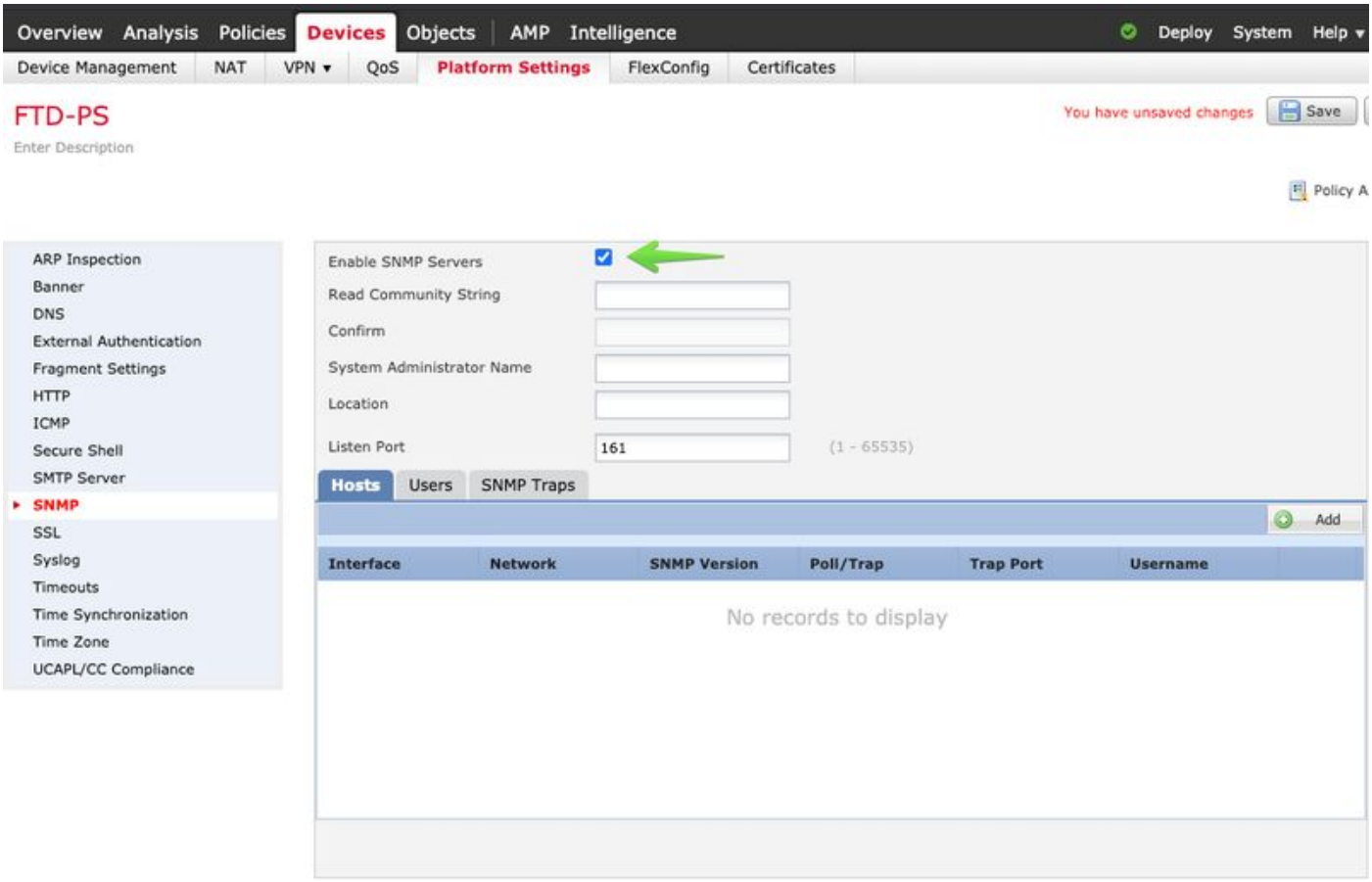
Schritt 5: Wählen Sie das Symbol **Bereitstellen**, um Änderungen anzuwenden.

Von FMC verwaltete FTD-Konfiguration

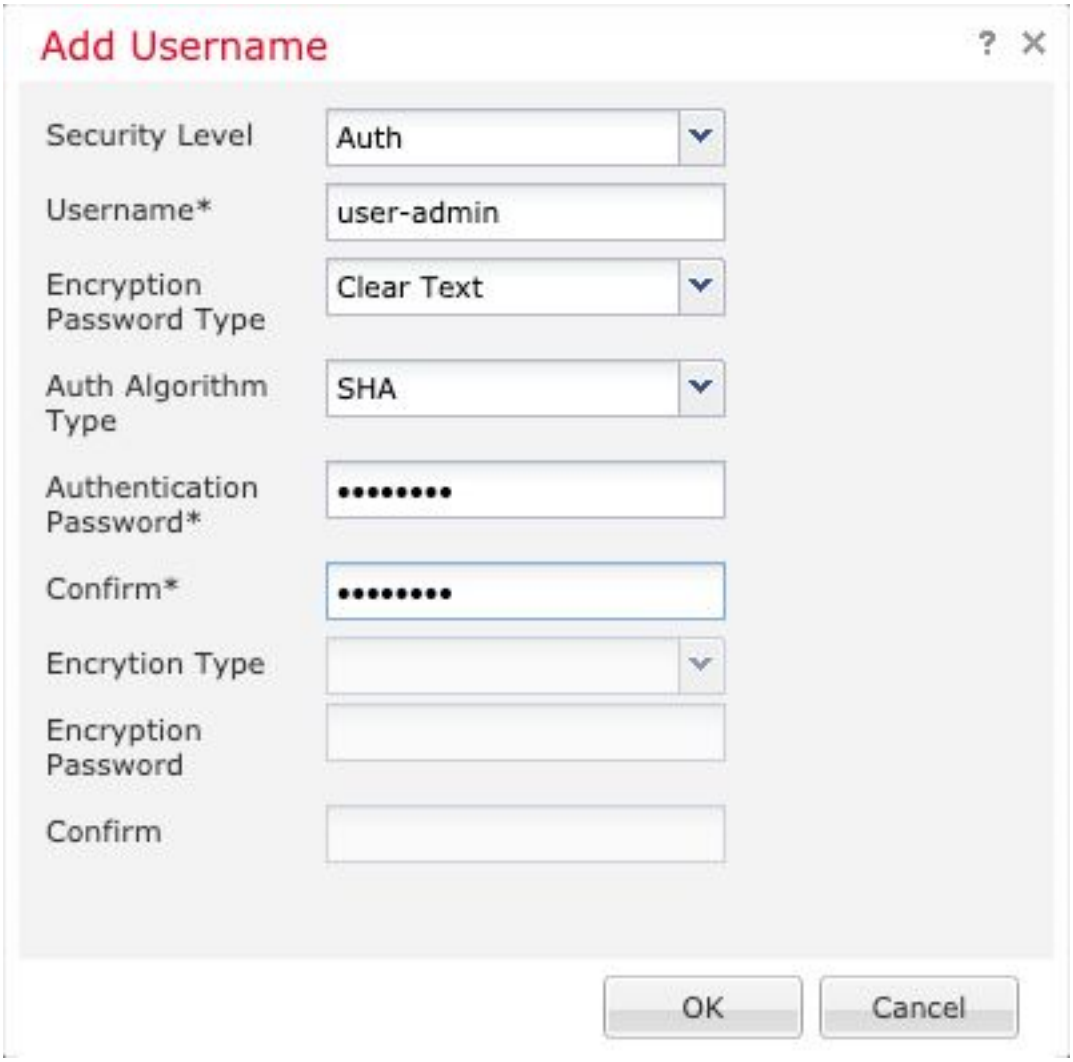
In den obigen Beispielen werden ähnliche Szenarien veranschaulicht, die jedoch auf dem FMC konfiguriert und dann in einem von ihm verwalteten FTD bereitgestellt werden. SNMPv2 kann auch verwendet werden. In diesem Artikel wird erläutert, wie Sie mit FTD einen SNMP-Server mithilfe der FMC-Verwaltung einrichten.

Schritt 1: Navigieren Sie zu **Devices > Platform Settings**, und wählen Sie **Edit** in der Richtlinie aus, die dem verwalteten Gerät zugewiesen ist, um die Konfiguration auf das zu übernehmen.

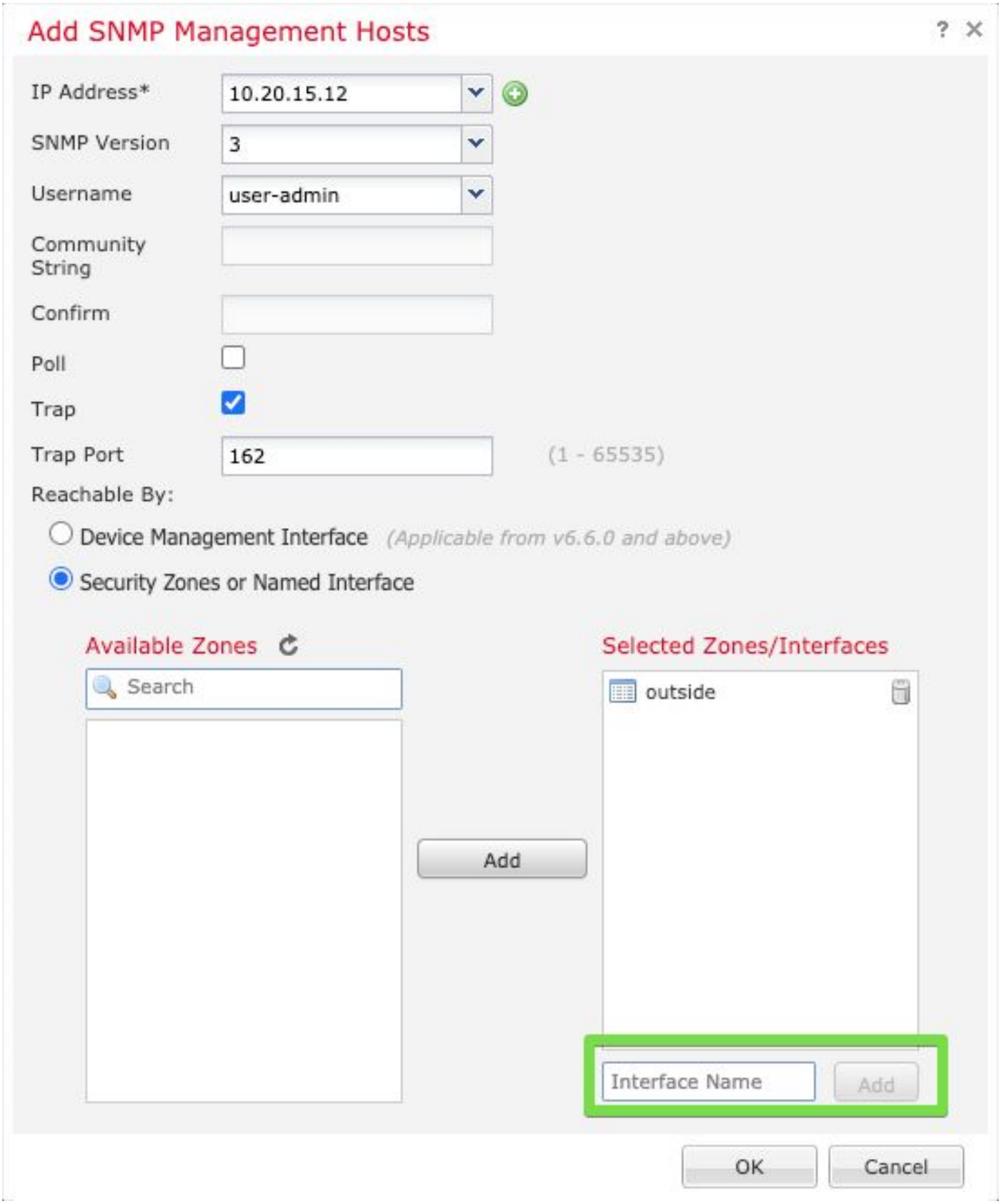
Schritt 2: Navigieren Sie zu **SNMP**, und aktivieren Sie die Option **SNMP-Server aktivieren**.



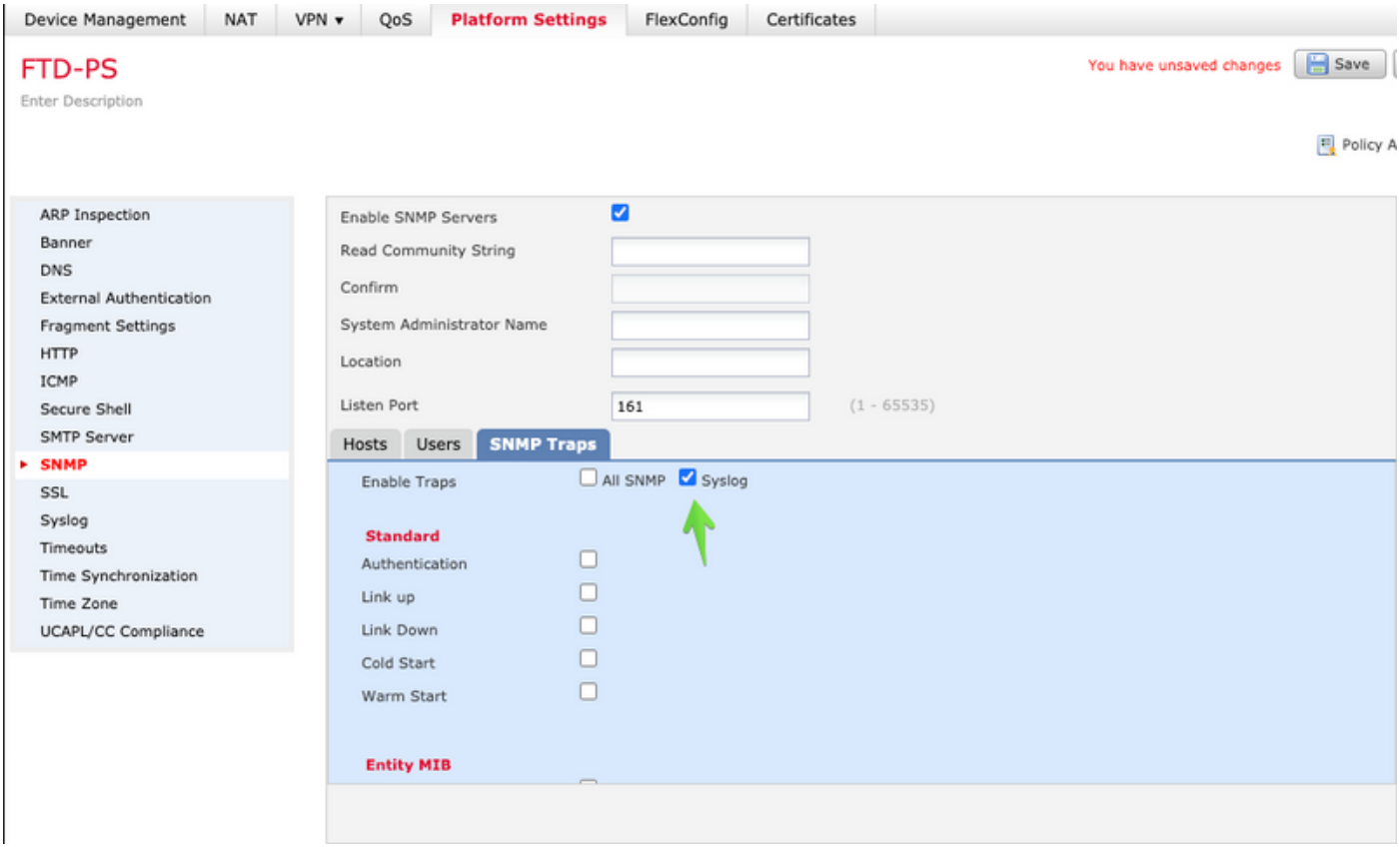
Schritt 3: Wählen Sie die Registerkarte **Benutzer** und anschließend die Schaltfläche **Hinzufügen** aus. Füllen Sie die Benutzerinformationen aus.



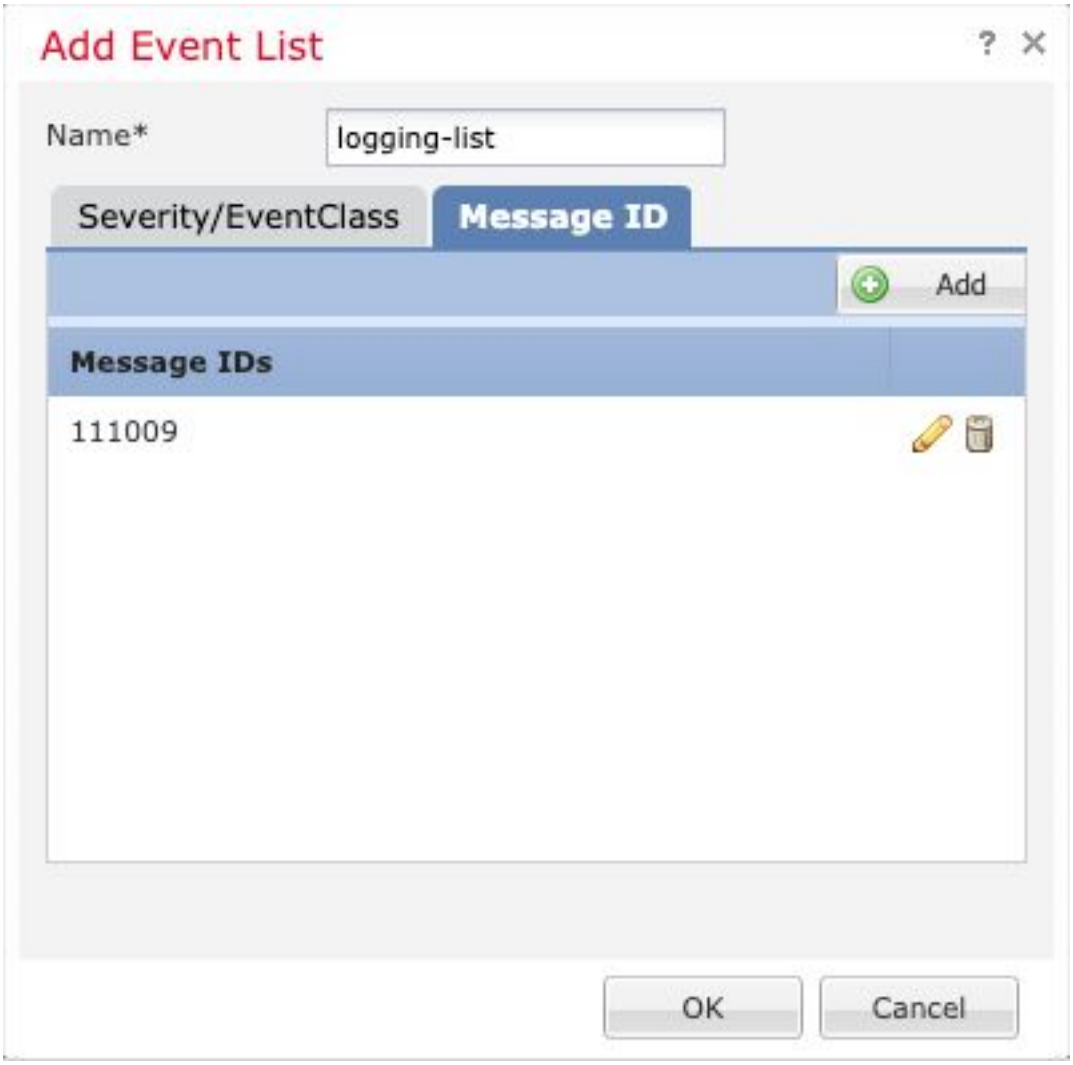
Schritt 4: Wählen Sie **Add** in der Registerkarte **Hosts aus**. Füllen Sie die Informationen zum SNMP-Server aus. Wenn Sie statt einer Zone eine Schnittstelle verwenden, stellen Sie sicher, dass Sie den Schnittstellennamen manuell im rechten Bereich hinzufügen. Wählen Sie OK, sobald alle erforderlichen Informationen enthalten sind.



Schritt 5: Wählen Sie die Registerkarte **SNMP-Traps** aus, und aktivieren Sie das Kontrollkästchen **Syslog**. Entfernen Sie alle anderen Traps-Markierungen, falls diese nicht erforderlich sind.



Schritt 6: Navigieren Sie zu **Syslog**, und wählen Sie die Registerkarte **Ereignislisten aus**. Wählen Sie die Schaltfläche **Hinzufügen**. Fügen Sie einen Namen und die Meldungen hinzu, die in die Liste aufgenommen werden sollen. Wählen Sie **OK**, um fortzufahren.

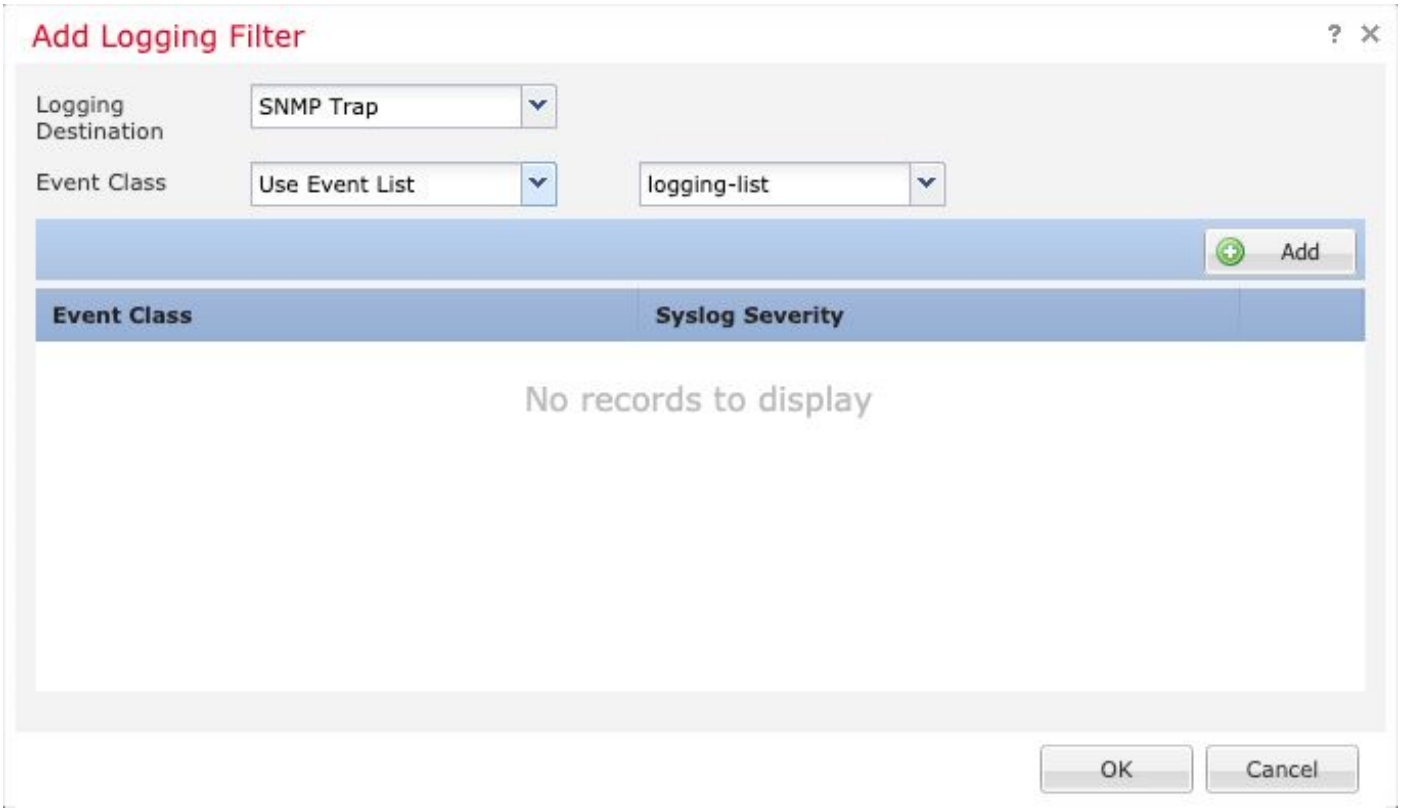


Schritt 7: Wählen Sie die Registerkarte **Protokollierungsziele** aus, und wählen Sie die Schaltfläche **Hinzufügen aus**.

Ändern Sie das Protokollierungsziel in **SNMP-Trap**.

Wählen Sie die **Benutzerereignisliste aus**, und wählen Sie die in Schritt 6 erstellte Ereignisliste aus.

Wählen Sie **OK**, um die Bearbeitung dieses Abschnitts abzuschließen.



Schritt 8: Wählen Sie die **Schaltfläche Speichern** und **Bereitstellen** der Änderungen am verwalteten Gerät.

Überprüfen

Die folgenden Befehle können sowohl in der FTD-CLISH als auch in der ASA CLI verwendet werden.

SNMP-Serverstatistiken anzeigen

Der Befehl "**show snmp-server statistics**" gibt Auskunft darüber, wie oft ein Trap gesendet wurde. Dieser Zähler kann andere Traps enthalten.

```
# show snmp-server statistics
0 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)
2 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
 2 Trap PDUs
```

Die in diesem Beispiel verwendete Nachrichten-ID löst jedes Mal aus, wenn ein Benutzer einen Befehl ausführt. Jedes Mal, wenn ein Befehl "show" ausgegeben wird, erhöht sich der Zähler.

Protokollierungseinstellungen anzeigen

Die **Anzeige der Protokollierungseinstellungen** liefert Informationen über die Nachrichten, die von den einzelnen Zielen gesendet wurden. Die Verlaufsprotokollierung zeigt die Zähler für SNMP-Traps an. Die Trap-Protokollierungsstatistiken beziehen sich auf Syslog-Hosts.

```
# show logging setting
Syslog logging: enabled
Facility: 20
Timestamp logging: enabled
Hide Username logging: enabled
Standby logging: disabled
Debug-trace logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: level debugging, 30 messages logged
Trap logging: level debugging, facility 20, 30 messages logged
Global TCP syslog stats::
NOT_PUTABLE: 0, ALL_CHANNEL_DOWN: 0
CHANNEL_FLAP_CNT: 0, SYSLOG_PKT_LOSS: 0
PARTIAL_REWRITE_CNT: 0
Permit-hostdown logging: disabled
 History logging: list syslog-list, 14 messages logged
Device ID: disabled
Mail logging: disabled
ASDM logging: disabled
```

Geben Sie den Befehl "**show logging queue**" ein, um sicherzustellen, dass keine Nachrichten verworfen werden.

```
# show logging queue

Logging Queue length limit : 512 msg(s)
0 msg(s) discarded due to queue overflow
0 msg(s) discarded due to memory allocation failure
Current 0 msg on queue, 231 msgs most on queue
```

Zugehörige Informationen

- Syslog-Meldungen der Cisco ASA-Serie
- CLI-Buch 1: Konfigurationsleitfaden für die CLI der Cisco ASA-Serie, 9.12
- SNMP auf FirePOWER NGFW-Appliances konfigurieren