ASAおよびFTDのSNMP syslogトラップの設定

内容

概要

このドキュメントでは、Cisco適応型セキュリティアプライアンス(ASA)およびFirepower Threat Defense(FTD)でSyslogメッセージを送信するようにSimple Network Management Protocol(SNMP)トラップを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco ASAの基礎知識
- Cisco FTDの基礎知識
- SNMPプロトコルに関する基礎知識

使用するコンポーネント

この文書の情報は、次のソフトウェアのバージョンに基づいています。

- Cisco Firepower Threat Defense for AWS 6.6.0
- Firepower Management Centerバージョン6.6.0
- Cisco適応型セキュリティアプライアンスソフトウェアバージョン9.12(3)9

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Cisco ASAとFTDには、ロギング情報を提供する複数の機能があります。ただし、Syslogサーバがオプションではない特定の場所があります。使用可能なSNMPサーバがある場合、SNMPトラップは代替として使用できます。

これは、トラブルシューティングやモニタリングの目的で特定のメッセージを送信するのに便利なツールです。たとえば、フェールオーバーシナリオ中に関連する問題を追跡する必要がある場合、FTDとASAの両方でクラスhaのSNMPトラップを使用して、これらのメッセージだけに焦点を当てることができます。

Syslogクラスの詳細については、このドキュメントを参照してください。

この記事の目的は、コマンドラインインターフェイス(CLI)、FMCによって管理されるFTD、およびFirepower Device Manager(FDM)によって管理されるFTDを使用したASAの設定例を示すことです。

FTDにCisco Defense Orchestrator(CDO)を使用する場合は、この設定をFDMインターフェイスに追加する必要があります。

> **注意**：高いsyslogレートでは、他の操作への影響を防ぐために、syslogメッセージにレート制限を設定することを推奨します。

これは、このドキュメントのすべての例で使用される情報です。

SNMPバージョン：**SNMPv3**

SNMPv3グループ：**group-name**

SNMPv3ユーザ：**認証用のHMAC SHAアルゴ**リズムを持つadmin-user

SNMPサーバのIPアドレス：**10.20.15.12**

SNMPサーバとの通信に使用するASA/FTDインターフェイス：**外部**

Syslog Message-ID:**111009**

設定

ASA の設定

次の手順を使用して、ASAで次の情報に従ってSNMPトラップを設定できます。

ステップ1:syslogリストに追加するメッセージを設定します。

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

ステップ2:SNMPv3サーバパラメータを設定します。

```
snmp-server enable

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

ステップ3:SNMPトラップを有効にします。

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

ステップ4:SNMPトラップを口ギング先として追加します。

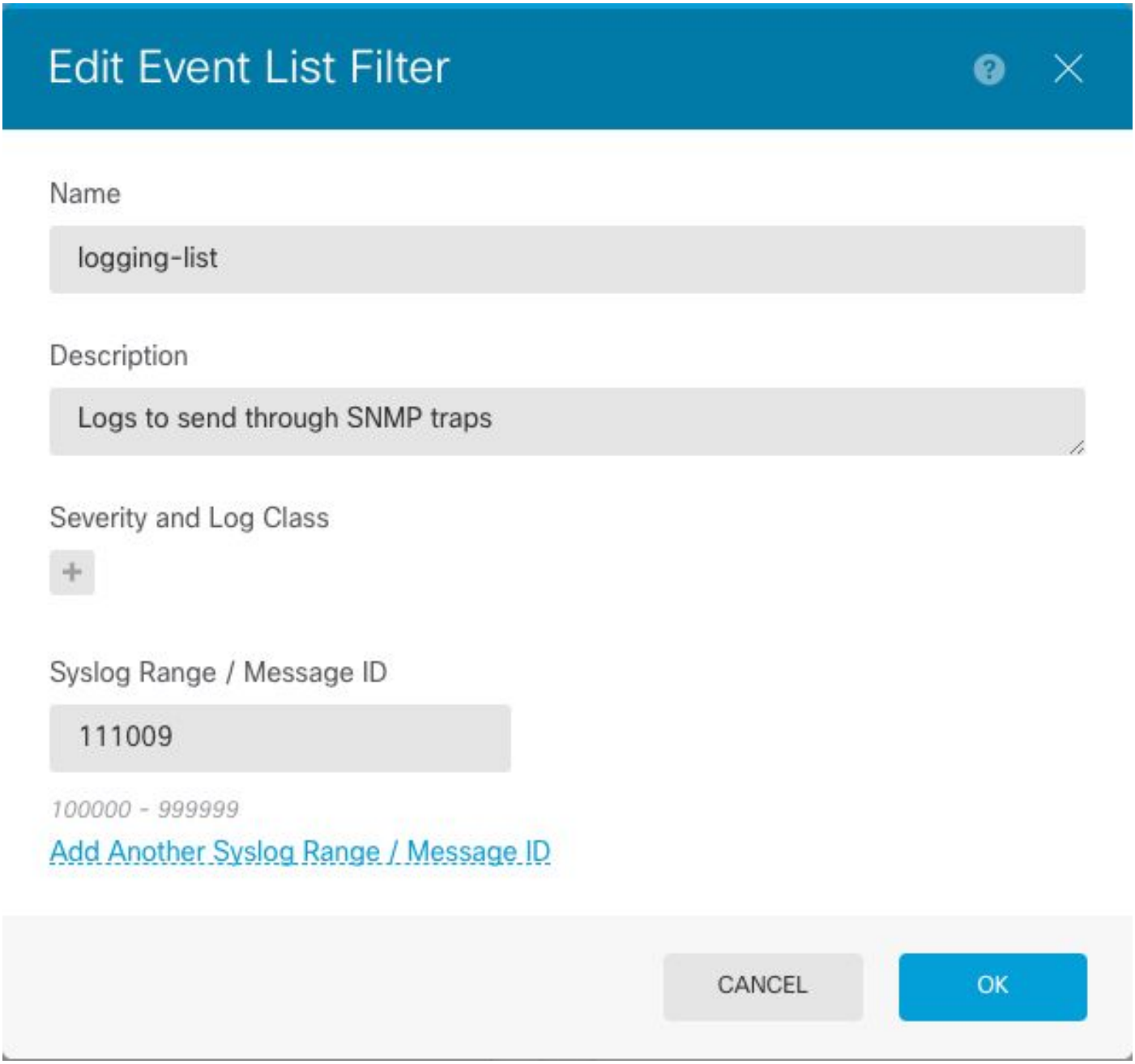
```
logging history syslog-list
```

FDMによって管理されるFTD構成

FTDがFDMによって管理されている場合に、SNMPサーバに送信する特定のSyslogリストを設定するには、次の手順を使用できます。

ステップ1:[Objects] > [Event List Filters]に移動し、[+]ボタンを選択します。

ステップ2:Even Listに名前を付け、関連するクラスまたはメッセージIDを含めます。次に、[OK]を選択します。



ステップ3:FDMホーム画面から「高度な構成」>「FlexConfig」>「FlexConfigオブジェクト」に移動し、+ボタンを選択します。

次のFlexConfigオブジェクトを作成し、次の情報を表示します。

名前： **SNMP-Server**

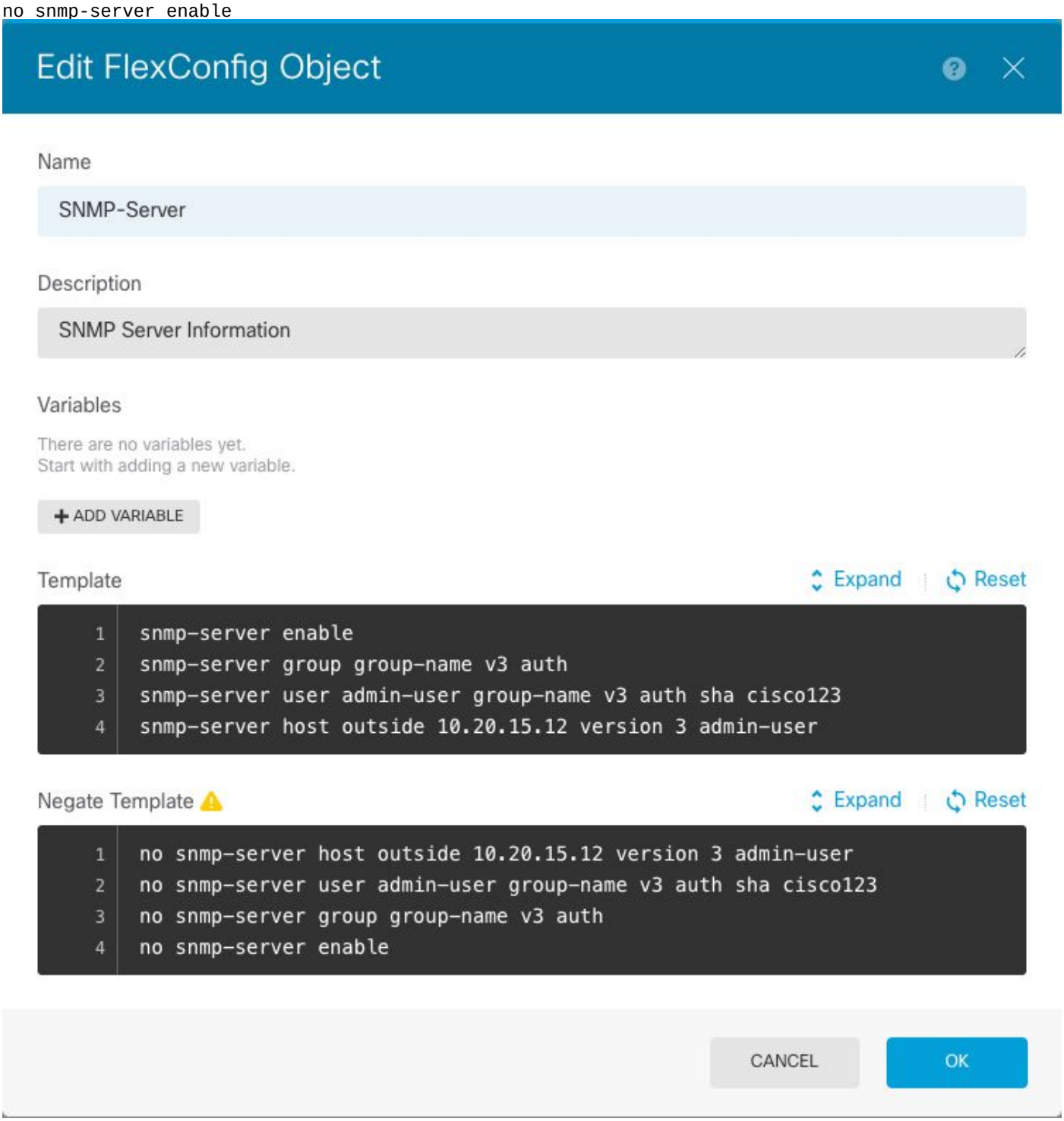
説明（オプション）:**SNMPサーバ情報**

テンプレート：

```
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
```

ネゲートテンプレート：

```
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
```



名前： **SNMP-Traps**

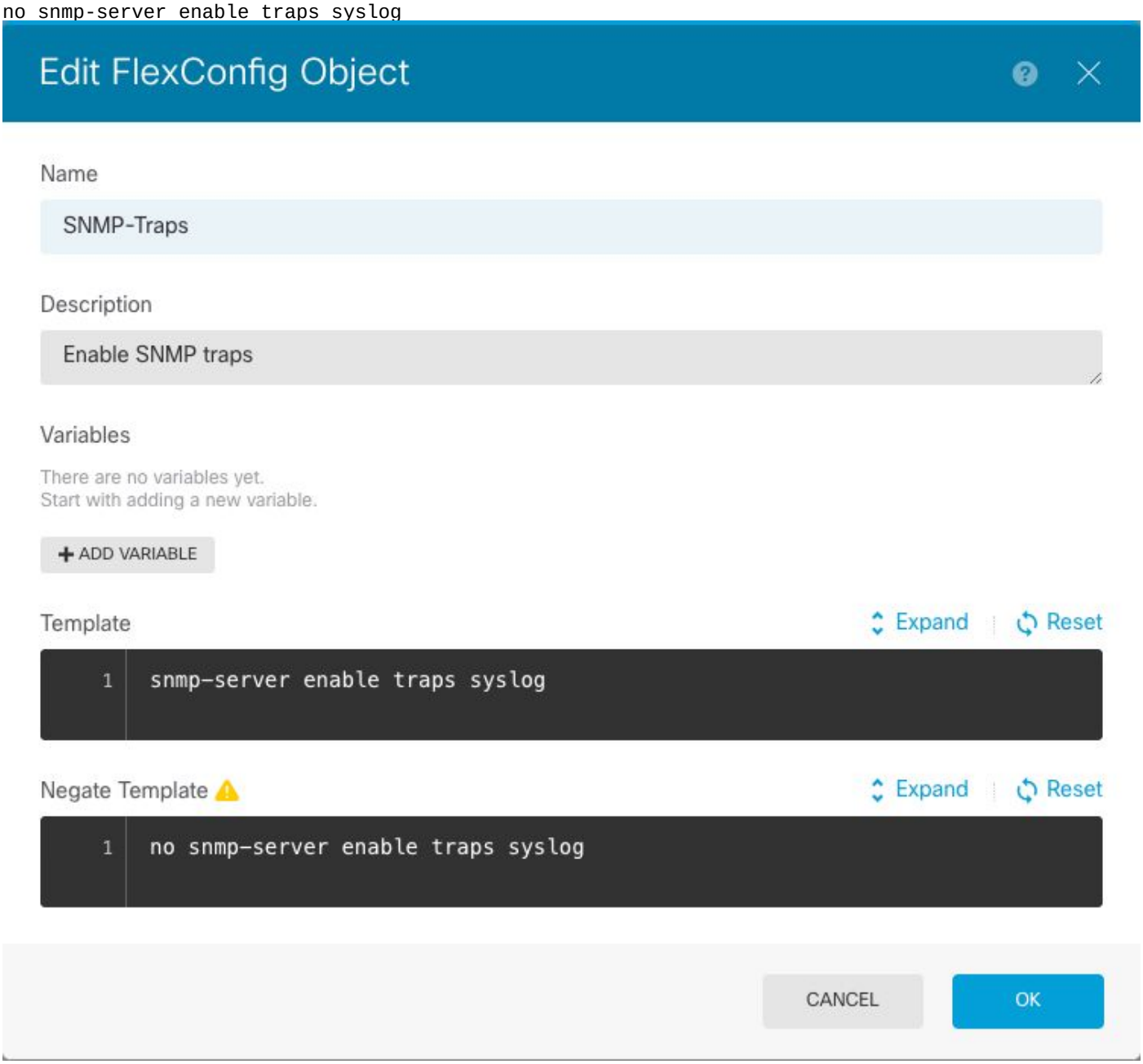
説明（オプション）:**Enable SNMP Traps**

テンプレート：

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

ネゲートテンプレート：

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



名前： **Logging-history**

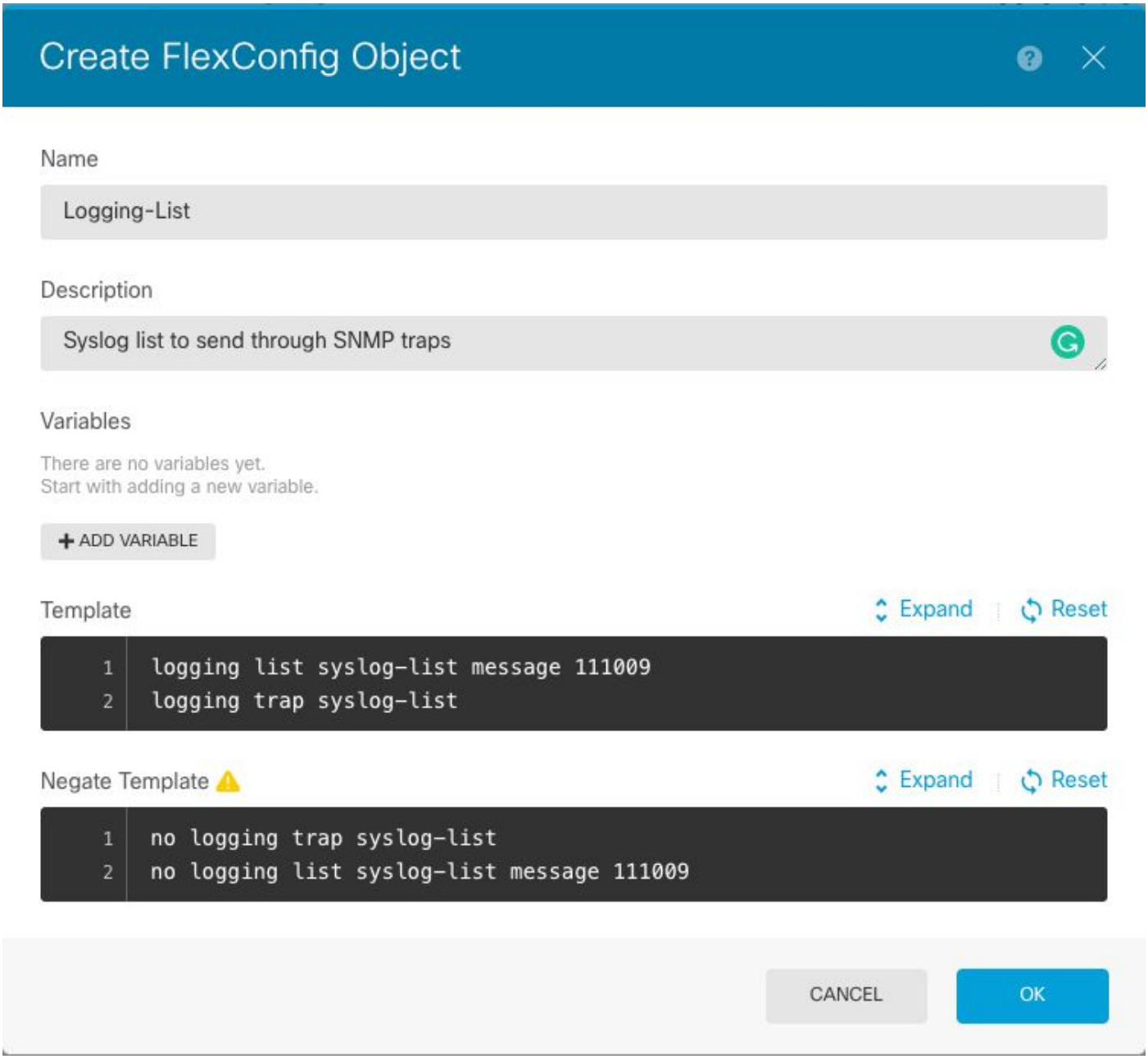
説明（オプション）:SNMPトラップsyslog**メッセージを設定するオブジェクト**

テンプレート：

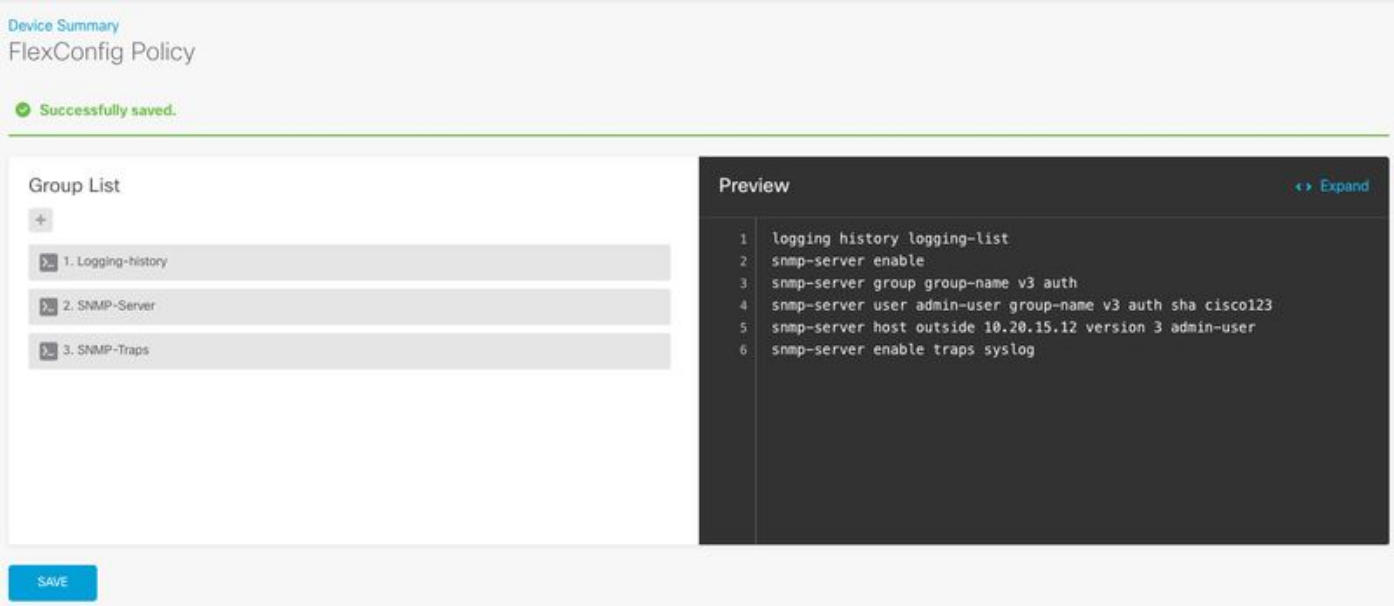
```
logging history logging-list
```

ネゲートテンプレート：

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



ステップ4:[Advanced Configuration] > [FlexConfig] > [FlexConfig Policy]に移動し、前のステップで作成したすべてのオブジェクトを追加します。この順序は、依存コマンドが同じオブジェクト(SNMP-Server)に含まれるため、関係ありません。 3つのオブジェクトが存在し、[プレビュー]セクションにコマンドのリストが表示されたら、[保存]を選択します。



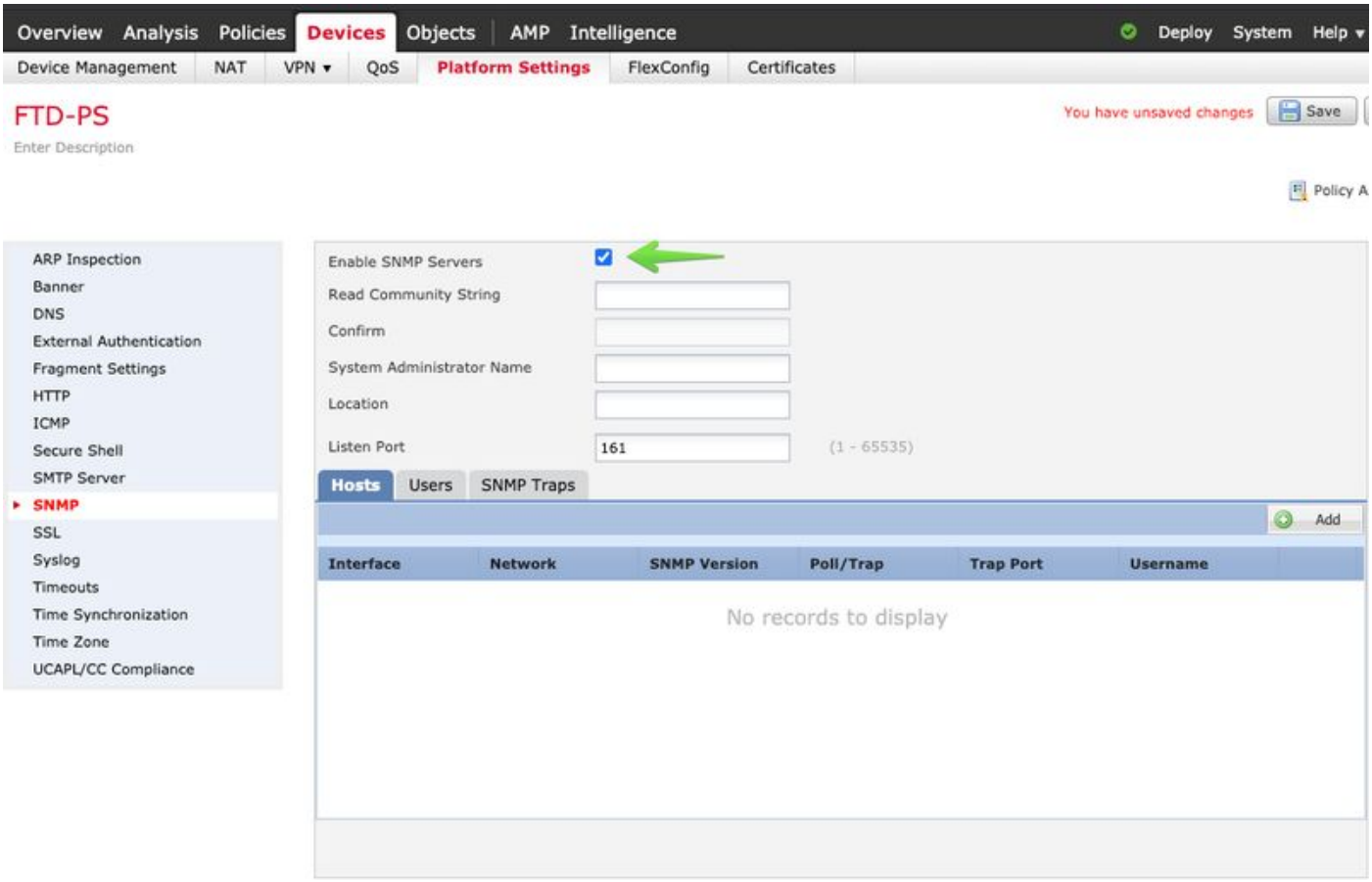
ステップ5：変更を適用するには、[**Deploy**]アイコンを選択します。

FMCによって管理されるFTD設定

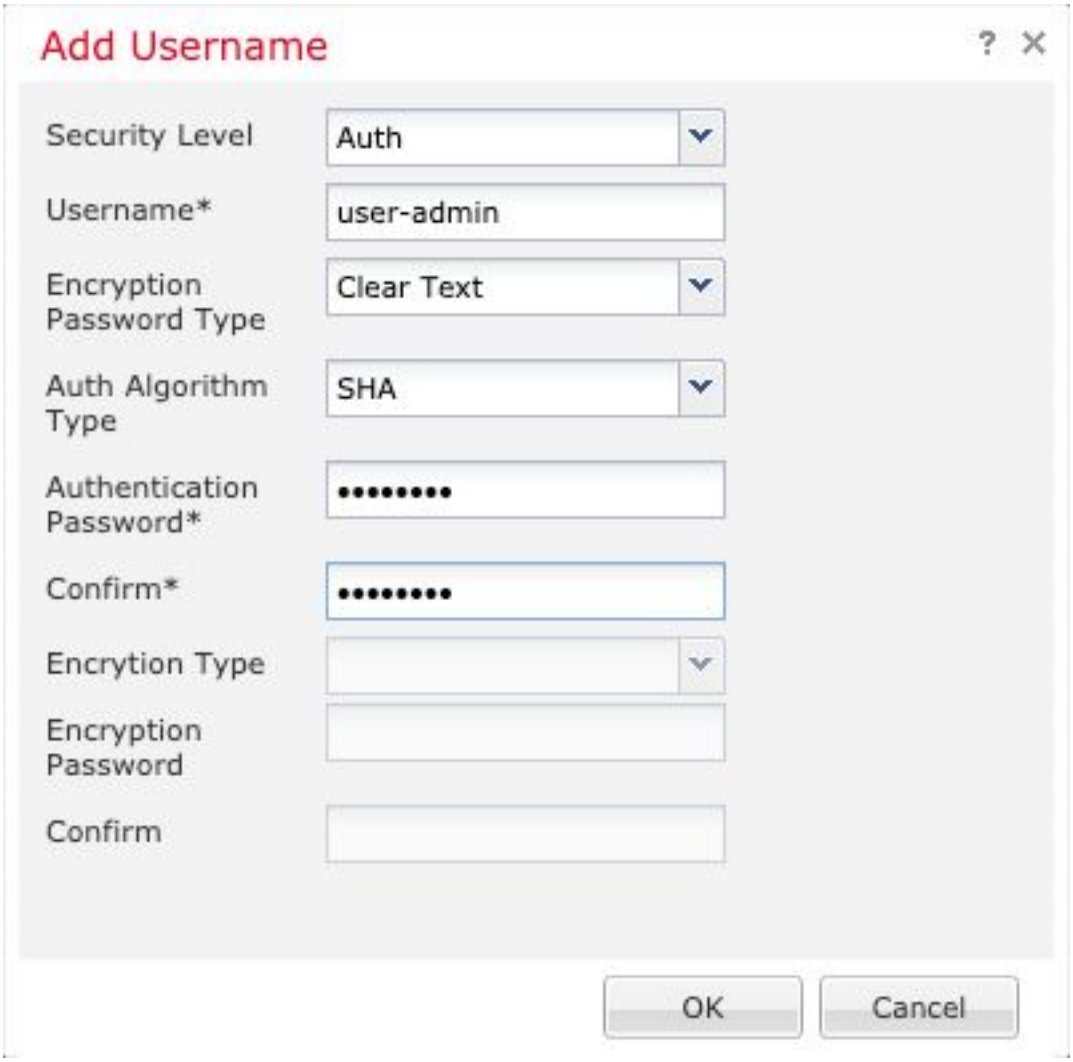
上記の例は、前のシナリオと同様のシナリオを示していますが、これらの変更はFMCで設定され、FMCによって管理されるFTDに展開されています。SNMPv2も使用できます。この記事では、FMC管理を使用してFTDでこのバージョンのSNMPサーバをセットアップする方法について説明します。

ステップ1:[Devices] > [Platform Settings] に移動し、管理対象デバイスに割り当てられたポリシーの[**Edit**]を選択して、設定を適用します。

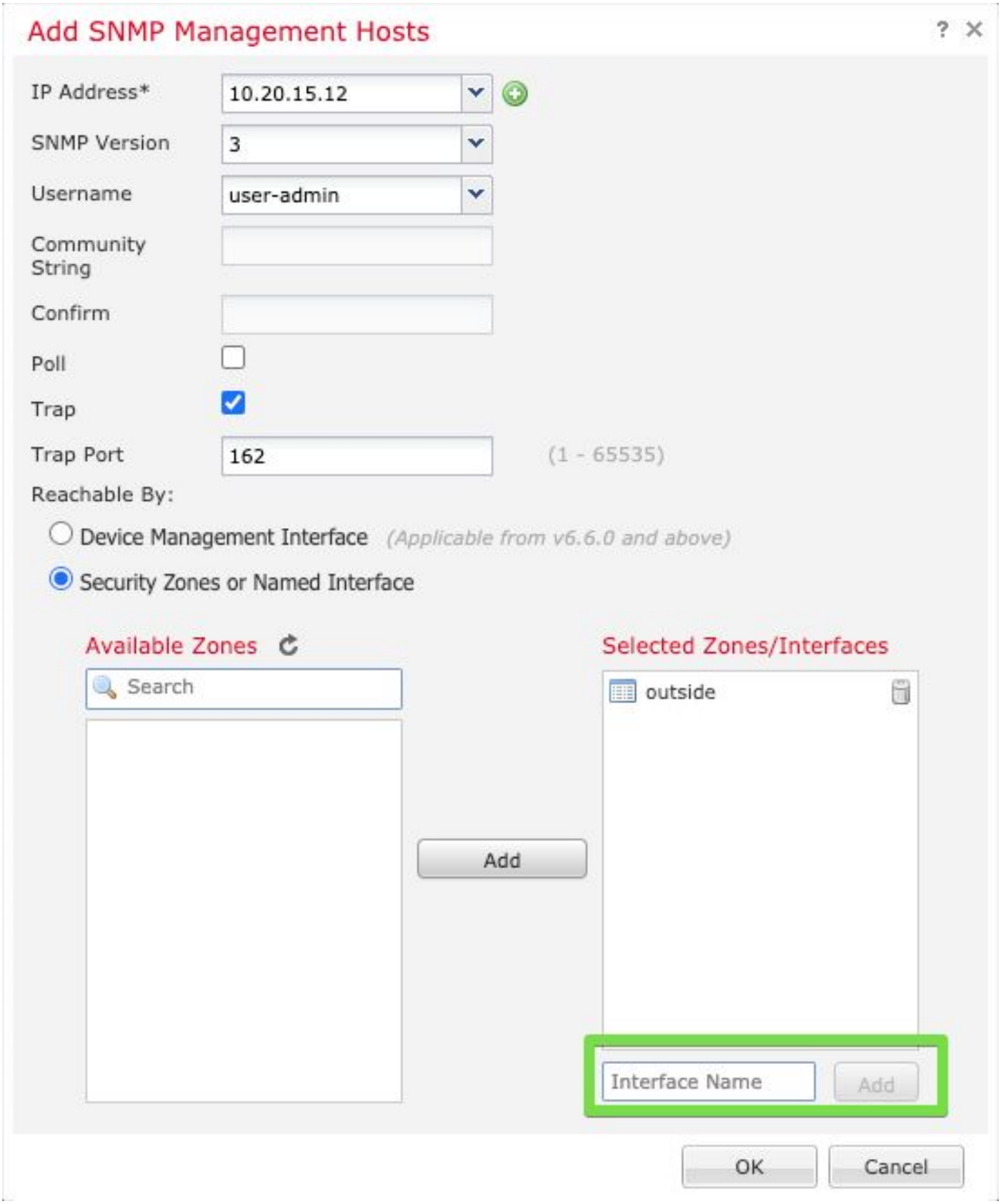
ステップ2:[SNMP]に移動し、[Enable SNMP Servers]**オプションをオン**にします。



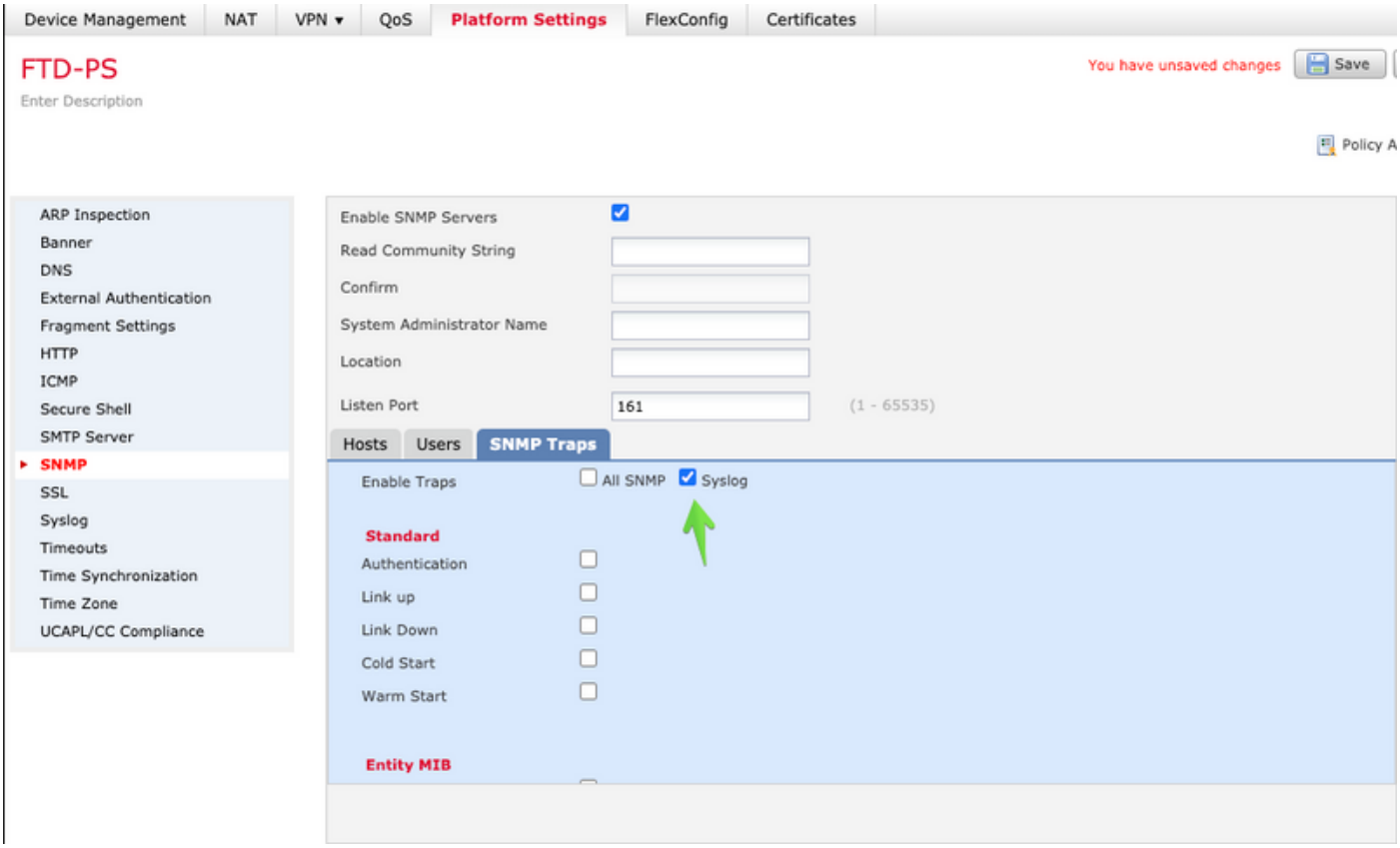
ステップ3:[Users]タブを選択し、[Add]ボタンを選択します。ユーザ情報を入力します。



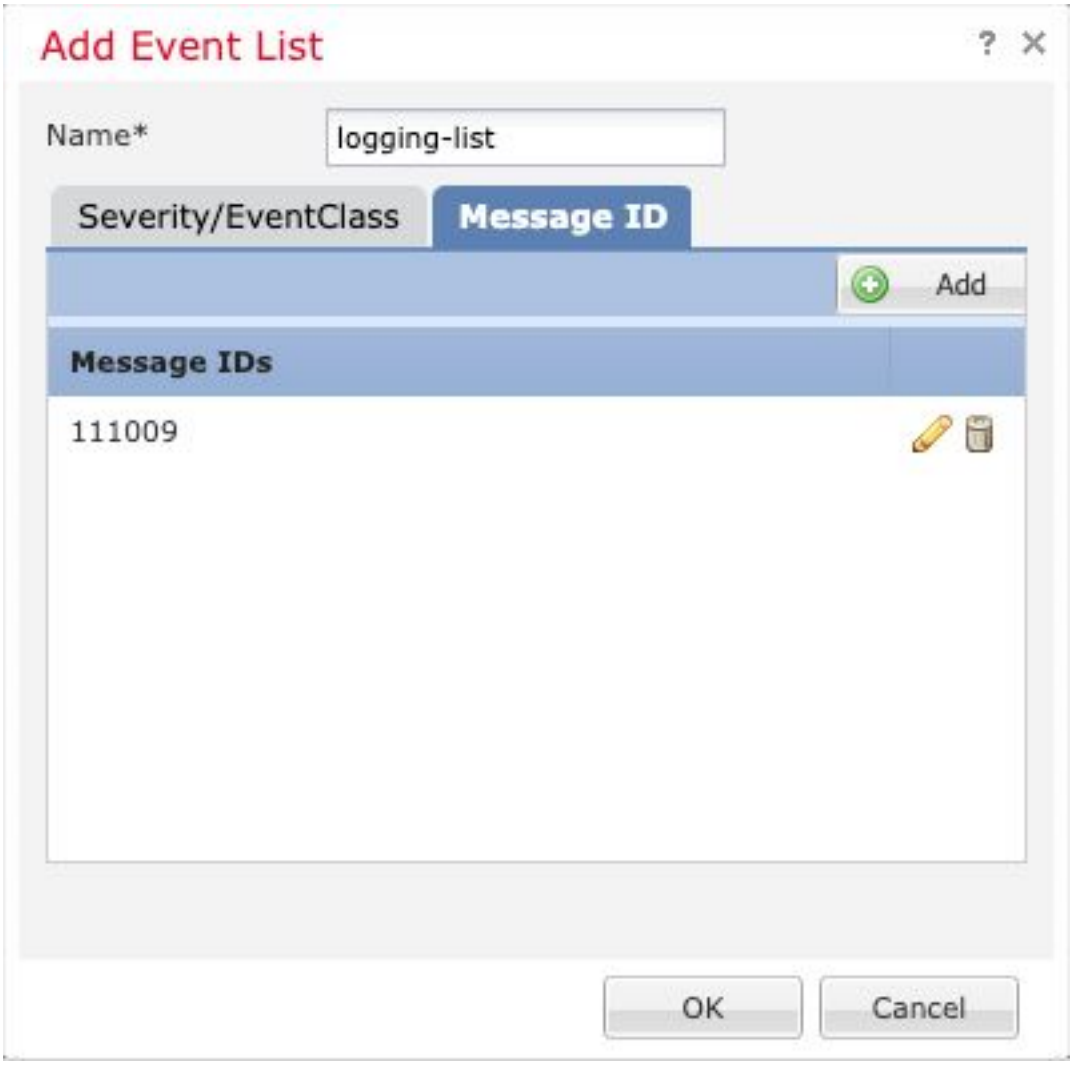
ステップ4:[ホスト]タブで[追加]を選択します。SNMPサーバに関連する情報を入力します。ゾーンの代わりにインターフェイスを使用する場合は、右側のセクションでインターフェイス名を手動で追加してください。必要なすべての情報が含まれたら、[OK]を選択します。



ステップ5:[SNMP Traps]タブを**選択し**、[**Syslog**]ボックスを**オンに**します。不要な場合は、他のすべてのトラップのチェックマークを削除してください。



ステップ6:[Syslog]に移動し、[Event **Lists]タブを選択**します。「追加」ボタン**を選択**します。リストに含める名前とメッセージを追加します。Ok を選択して処理を続けます。

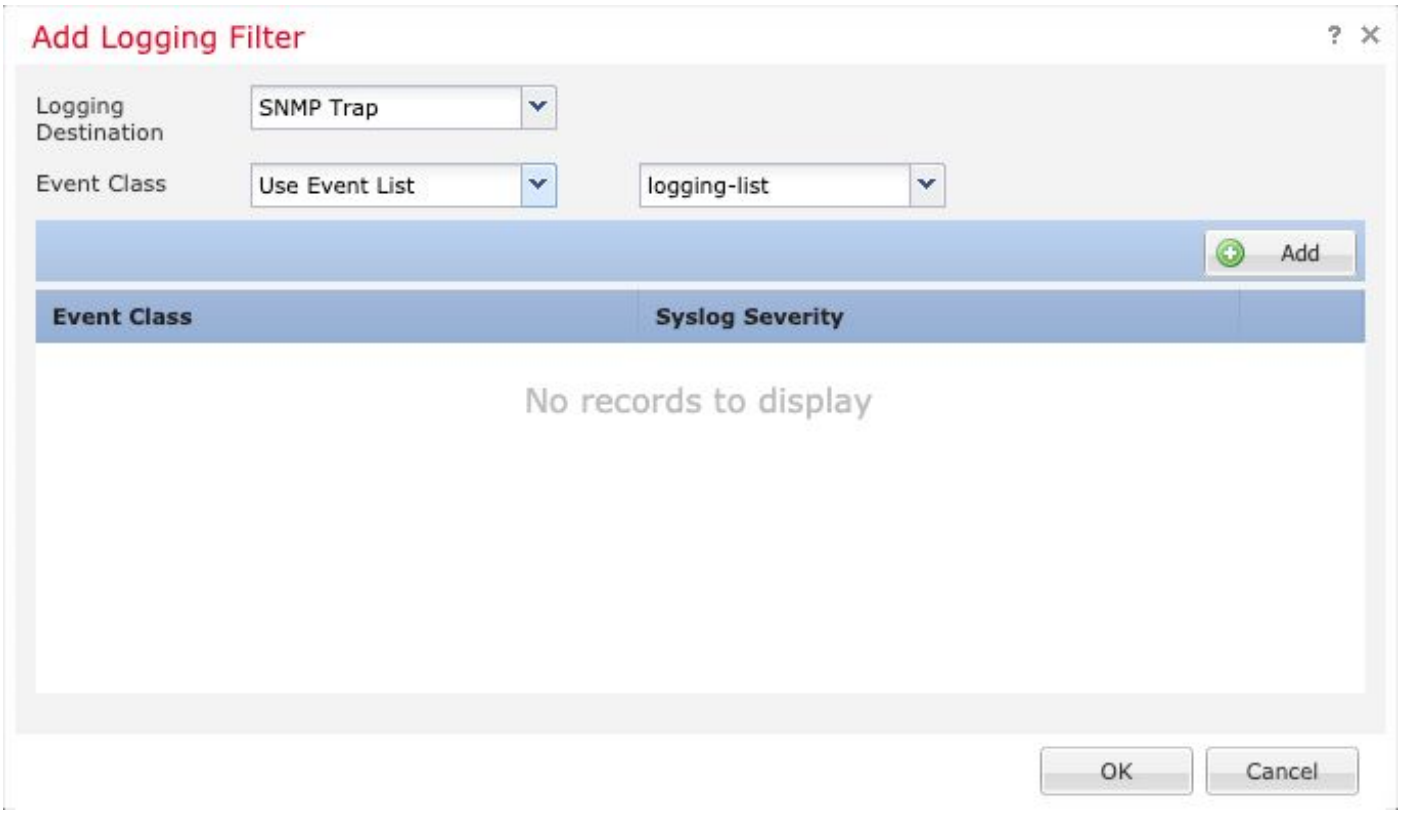


ステップ7:[Logging Destinations]タブ**を選択**し、[**Add**]ボタンを**選択**します。

[Logging Destination]を[**SNMP Trap**]に**変更します**。

[User Event List]**を選択**し、その横にあるステップ6で作成したイベントリストを選択します。

[**OK**]**を選択**して、このセクションの編集を終了します。



ステップ8:[**Save**]ボタンを**選択し**、[**Deploy** the changes to the managed device]を選択します。

確認

次のコマンドは、FTD CLISHとASA CLIの両方で使用できます。

Show snmp-server statistics

「**show snmp-server statistics**」コマンドは、トラップの送信回数に関する情報を提供します。このカウンタには、他のトラップを含めることができます。

```
# 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
```

この例で使用するメッセージIDは、ユーザがコマンドを実行するたびにトリガーされます。「show」コマンドを発行するたびに、カウンタが増加します。

ロギング設定の表示

「show logging setting」は、各宛先から送信されたメッセージに関する情報を提供します。履歴ロギングは、SNMPトラップのカウンタを示します。Trapロギング統計情報は、Syslogホストのカウンタに関連しています。

```
# 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
```

show logging queueコマンドを発行して、メッセージがドロップされていないことを確認します。

```
# 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
```

関連情報

- Cisco ASA シリーズ Syslog メッセージ
- CLI ブック 1：Cisco ASAシリーズCLIコンフィギュレーションガイド9.12
- Firepower NGFWアプライアンスでのSNMPの設定