Configuration des interruptions SNMP Syslog pour ASA et FTD

Contenu

Introduction

Ce document décrit comment configurer les déroutements SNMP (Simple Network Management Protocol) pour envoyer des messages Syslog sur l'appareil de sécurité adaptatif (ASA) de Cisco et Firepower Threat Defense (FTD).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base de Cisco ASA
- Connaissances de base de Cisco FTD
- Connaissances de base du protocole SNMP

Components Used

Les informations de ce document sont basées sur la version logicielle suivante :

- Cisco Firepower Threat Defense pour AWS 6.6.0
- Firepower Management Center Version 6.6.0
- Logiciel Cisco Adaptive Security Appliance Version 9.12(3)9

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau

est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Cisco ASA et FTD ont plusieurs fonctionnalités pour fournir des informations de journalisation. Cependant, il existe des emplacements spécifiques où un serveur Syslog n'est pas une option. Les déroutements SNMP offrent une alternative si un serveur SNMP est disponible.

Cet outil est utile pour envoyer des messages spécifiques à des fins de dépannage ou de surveillance. Par exemple, s'il existe un problème pertinent qui doit être suivi lors de scénarios de basculement, les interruptions SNMP pour la classe ha sur FTD et ASA peuvent être utilisées pour se concentrer uniquement sur ces messages.

Des informations supplémentaires relatives aux classes Syslog sont disponibles dans ce document.

L'objectif de cet article est de fournir des exemples de configuration pour ASA à l'aide de l'interface de ligne de commande (CLI), de FTD géré par FMC et de FTD géré par Firepower Device Manager (FDM).

Si Cisco Defense Orchestrator (CDO) est utilisé pour FTD, cette configuration doit être ajoutée à l'interface FDM.

> **Attention** : Pour les débits Syslog élevés, il est recommandé de configurer une limite de débit pour les messages Syslog afin d'éviter tout impact dans d'autres opérations.

Il s'agit des informations utilisées pour tous les exemples de ce document.

Version SNMP : **SNMPv3**

Groupe SNMPv3 : **nom-groupe**

Utilisateur SNMPv3 : **admin-user** avec algorithme SHA HMAC pour l'authentification

Adresse IP du serveur SNMP : **10.20.15.12**

Interface ASA/FTD à utiliser pour communiquer avec le serveur SNMP : **Externe**

ID de message Syslog : **111009**

Configuration

Configuration ASA

Ces étapes peuvent être utilisées pour configurer des interruptions SNMP sur un ASA en suivant les informations ci-dessous.

Étape 1. Configurez les messages à ajouter à la liste Syslog.

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

Étape 2. Configurez les paramètres du serveur SNMPv3.

```
snmp-server enable

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

Étape 3. Activez les déroutements SNMP.

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

Étape 4. Ajoutez les déroutements SNMP comme destination de journalisation.

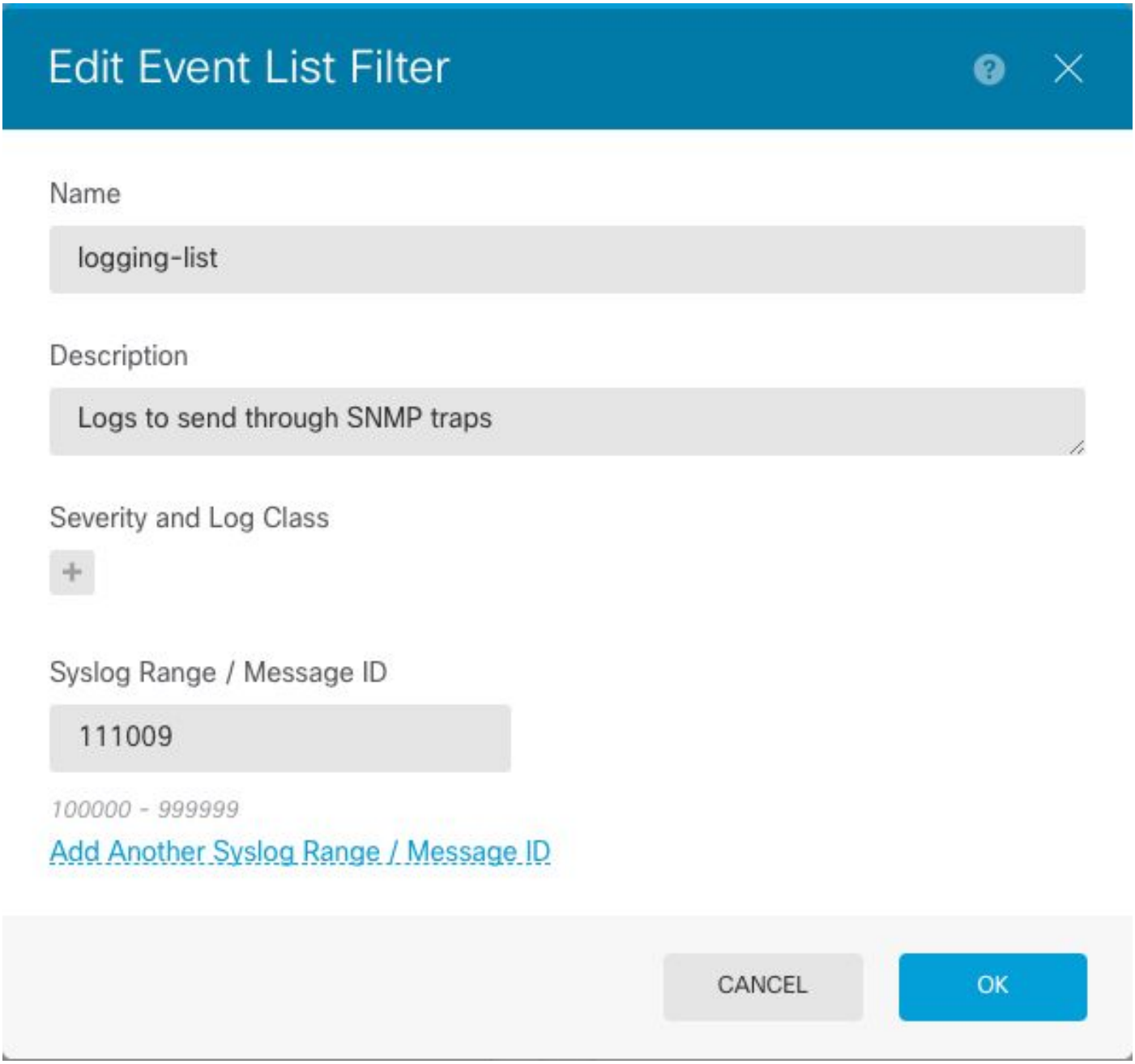
```
logging history syslog-list
```

Configuration FTD gérée par FDM

Ces étapes peuvent être utilisées pour configurer une liste Syslog spécifique à envoyer au serveur SNMP lorsque FTD est géré par FDM.

Étape 1. Accédez à **Objets > Filtres de liste d'événements** et sélectionnez le **+** bouton.

Étape 2. Nommez la liste paire et incluez les classes ou les ID de message appropriés. Sélectionnez ensuite OK.



Étape 3. Accédez à **Configuration** avancée **> FlexConfig > FlexConfig Objects** à partir de l'écran d'accueil FDM et sélectionnez le **+** bouton.

Créez les objets FlexConfig suivants avec les informations répertoriées :

Nom : **SNMP-Server**

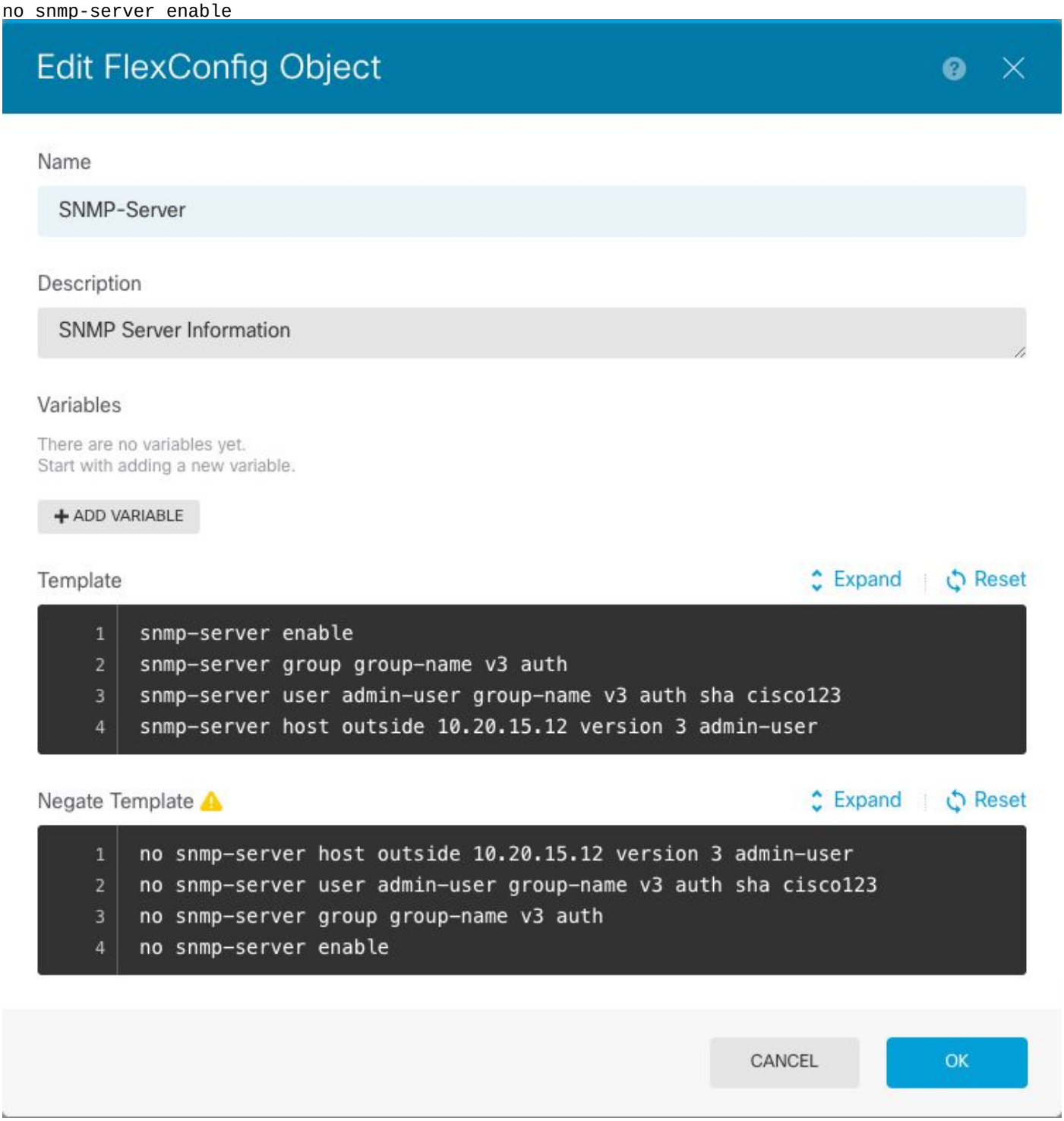
Description (facultatif) : **Informations sur le serveur SNMP**

Modèle :

```
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
```

Modèle négatif :

```
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
```



Nom : **Interruptions SNMP**

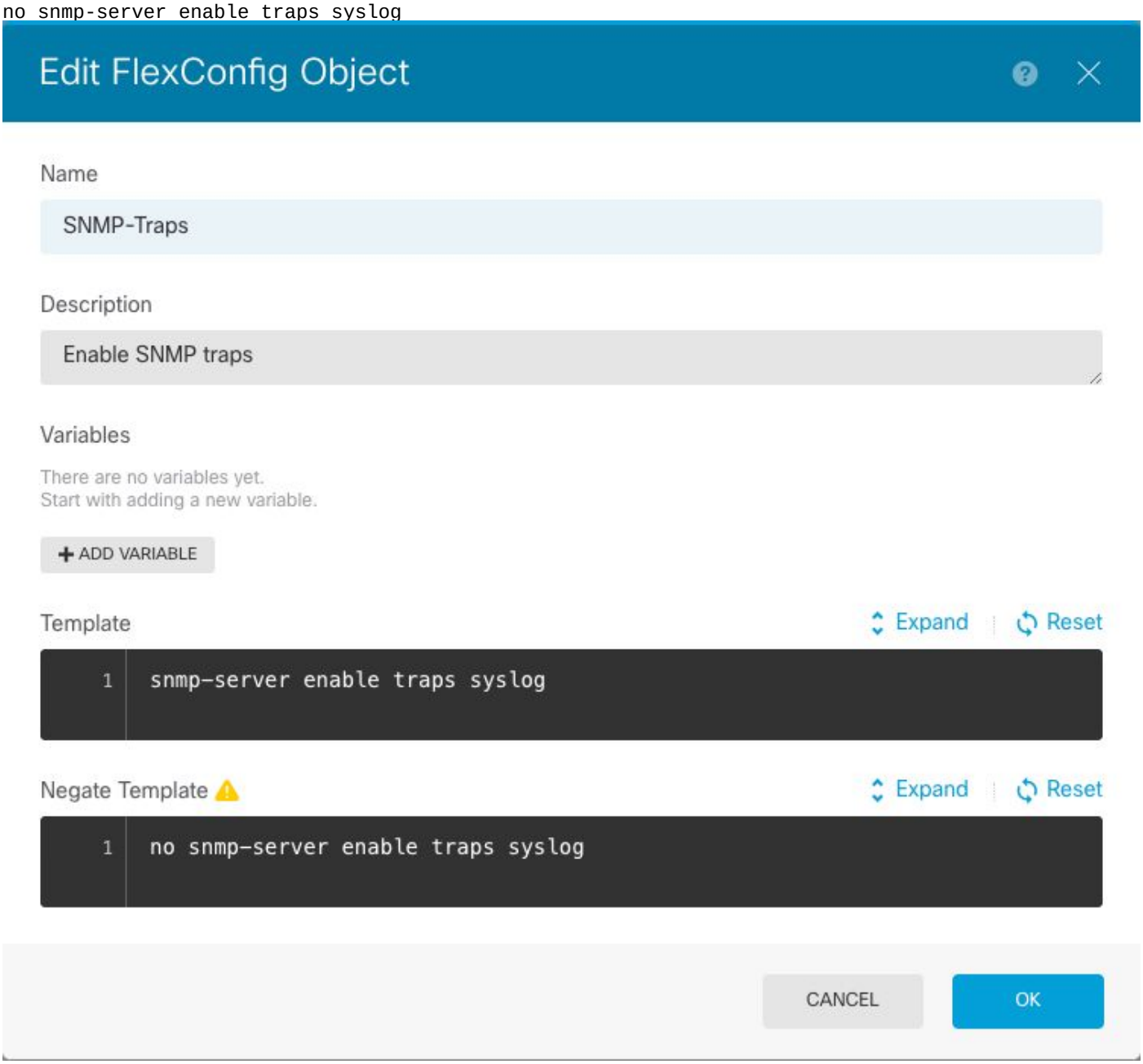
Description (Facultatif) : **Activer les interruptions SNMP**

Modèle :

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

Modèle négatif :

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



Nom : **Historique de journalisation**

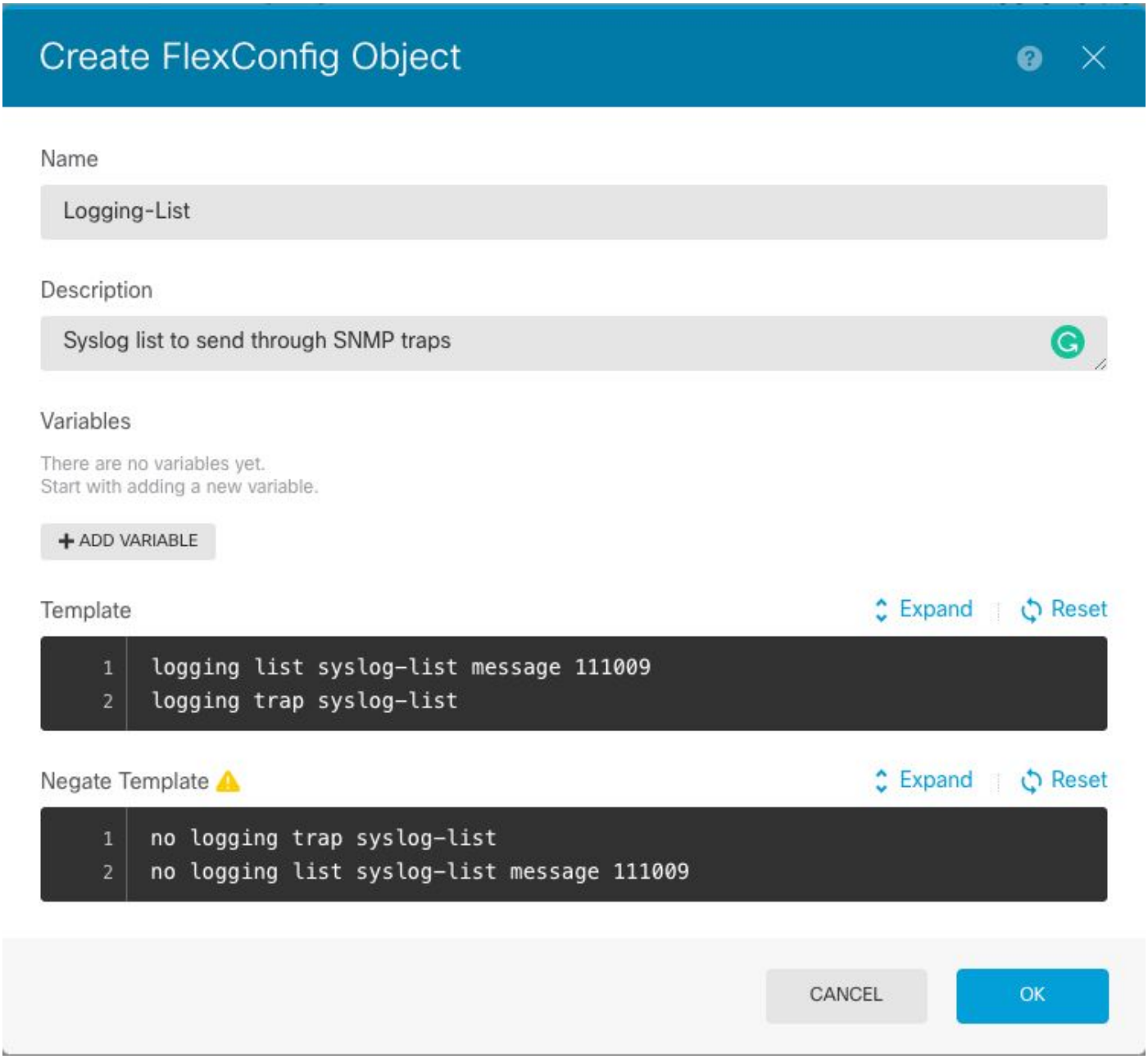
Description (Facultatif) : **Objet permettant de définir les messages syslog d'interruptions SNMP**

Modèle :

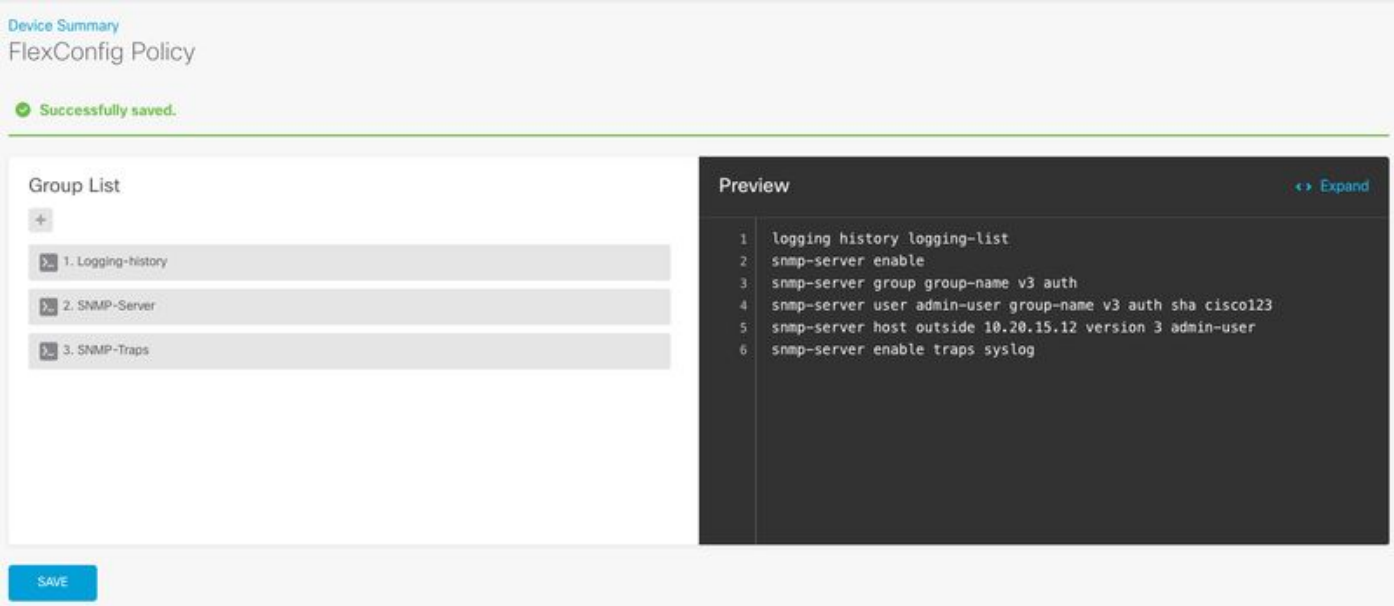
```
logging history logging-list
```

Modèle négatif :

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



Étape 4. Accédez à **Configuration avancée > FlexConfig > FlexConfig Policy** et ajoutez tous les objets créés à l'étape précédente. L'ordre n'est pas pertinent car les commandes dépendantes sont incluses dans le même objet (SNMP-Server). Sélectionnez **Enregistrer** une fois les trois objets présents et la section **Aperçu** affiche la liste des commandes.



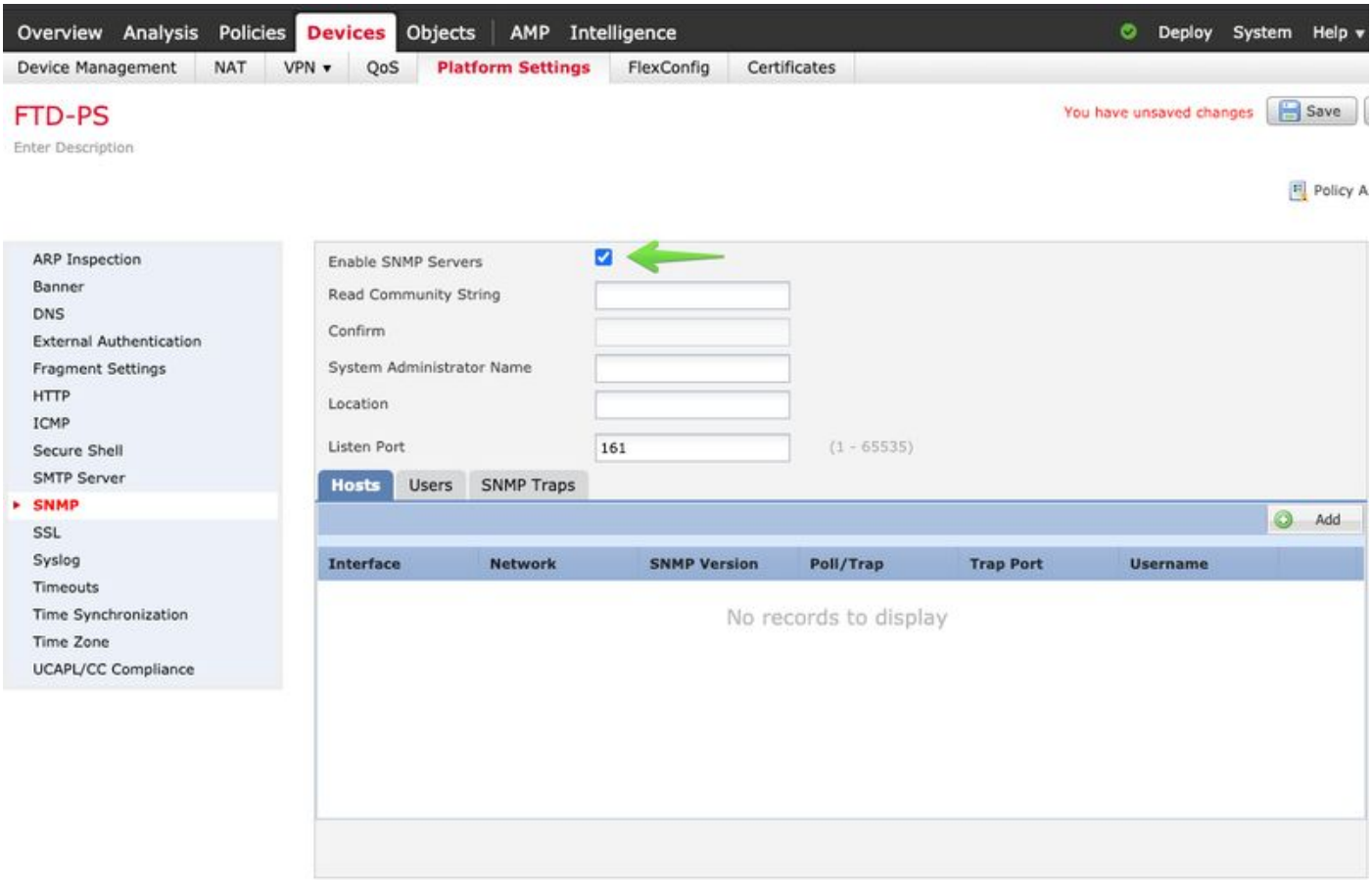
Étape 5. Sélectionnez l'icône **Déployer** pour appliquer les modifications.

Configuration FTD gérée par FMC

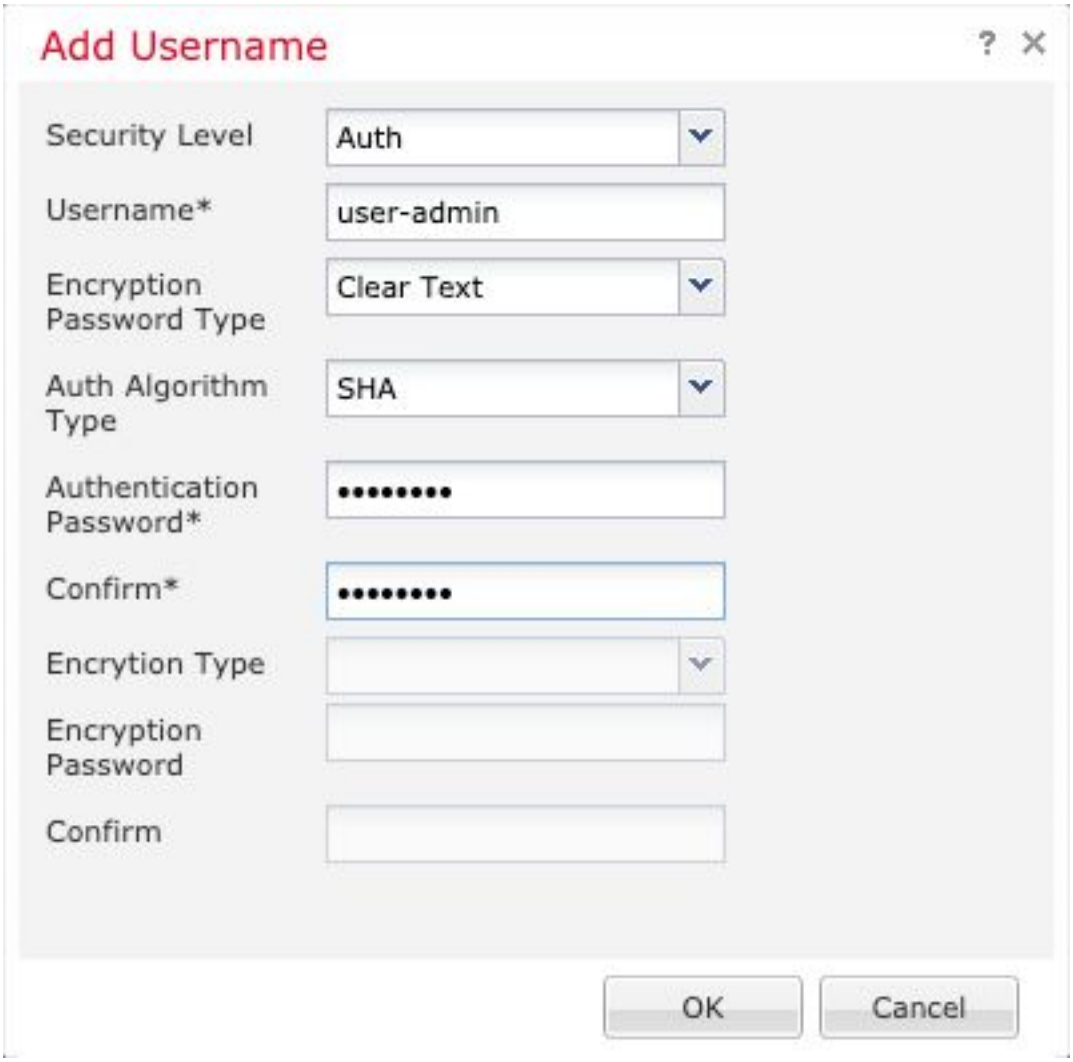
Les exemples ci-dessus illustrent des scénarios similaires aux précédents, mais ces modifications sont configurées sur le FMC, puis déployées sur un FTD géré par celui-ci. SNMPv2 peut également être utilisé. Cet article explique comment utiliser la configuration d'un serveur SNMP avec cette version sur FTD à l'aide de la gestion FMC.

Étape 1. Accédez à **Périphériques > Paramètres de la plate-forme** et sélectionnez **Modifier** sur la stratégie affectée au périphérique géré auquel appliquer la configuration.

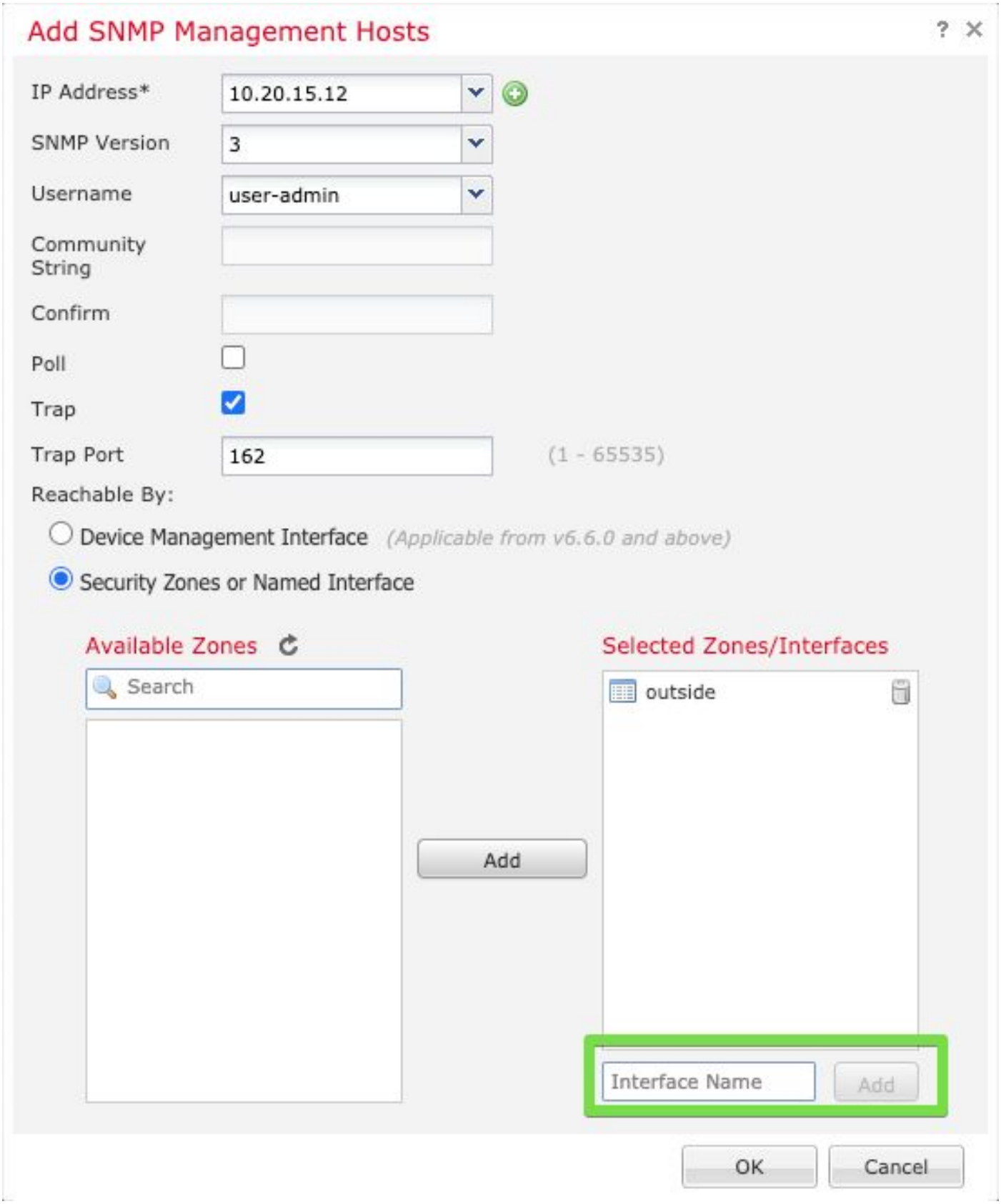
Étape 2. Accédez à **SNMP** et activez l'option **Activer les serveurs SNMP**.



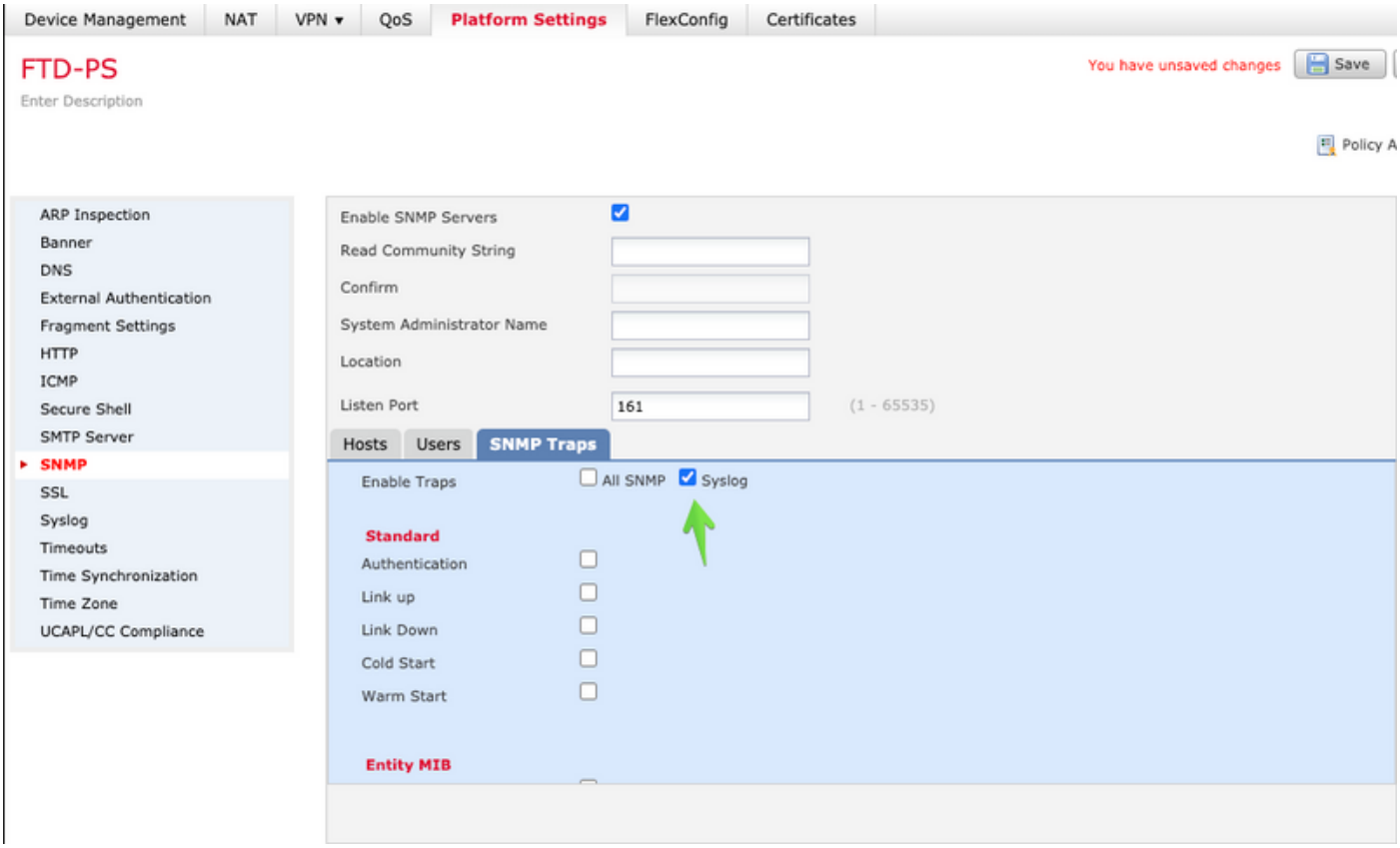
Étape 3. Sélectionnez l'onglet **Utilisateurs** et cliquez sur le bouton **Ajouter**. Renseignez les informations utilisateur.



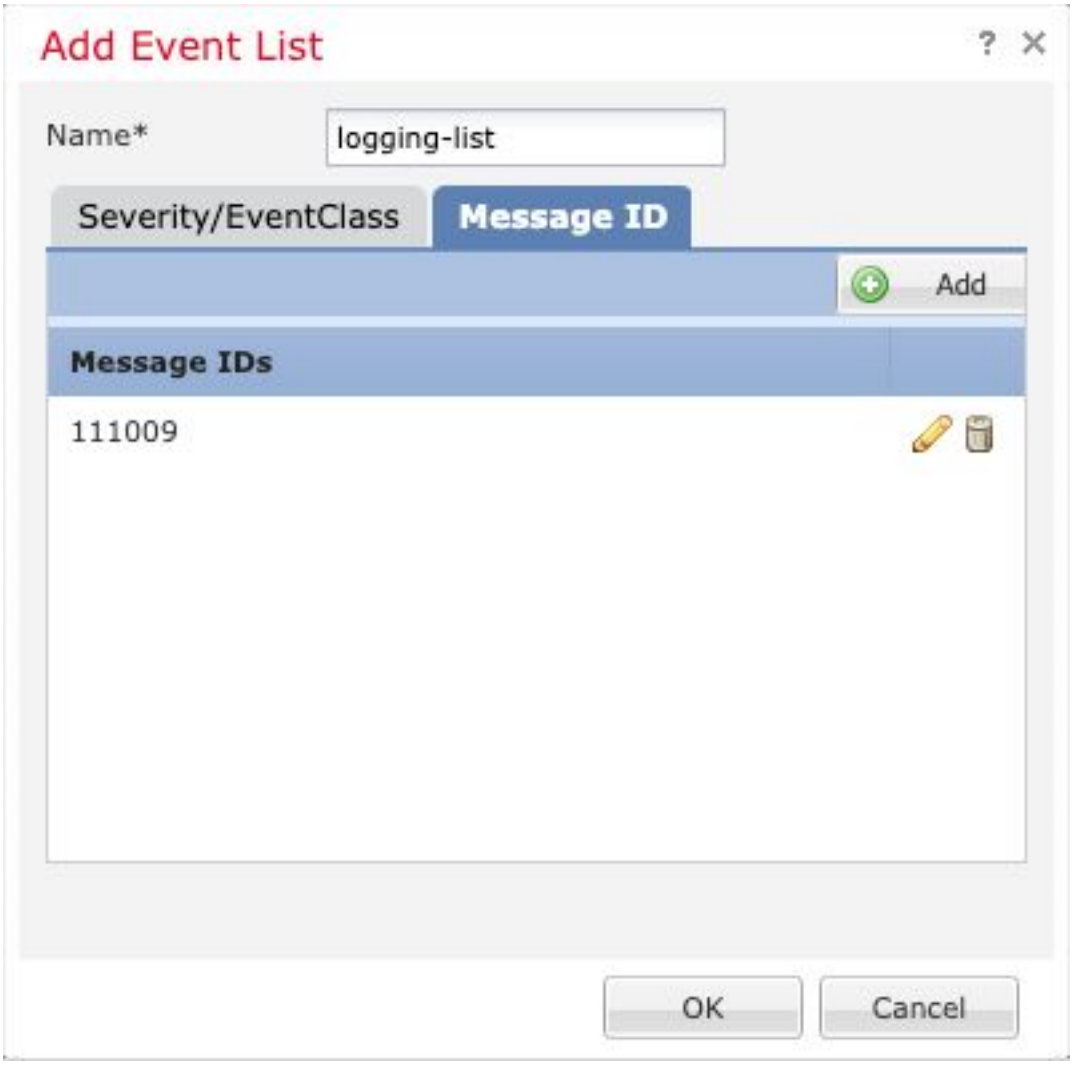
Étape 4. Sélectionnez **Ajouter** dans l'onglet **Hôtes**. Complétez les informations relatives au serveur SNMP. Si vous utilisez une interface au lieu d'une zone, assurez-vous d'ajouter manuellement le nom de l'interface dans la section du coin droit. Sélectionnez OK une fois toutes les informations nécessaires incluses.



Étape 5. Sélectionnez l'onglet **Interruptions SNMP** et cochez la case **Syslog**. Veillez à supprimer toutes les autres coches de déroutement si elles ne sont pas requises.



Étape 6. Accédez à **Syslog** et sélectionnez l'onglet **Event Lists**. Sélectionnez le bouton **Ajouter**. Ajoutez un nom et les messages à inclure dans la liste. Sélectionnez **OK** pour continuer.

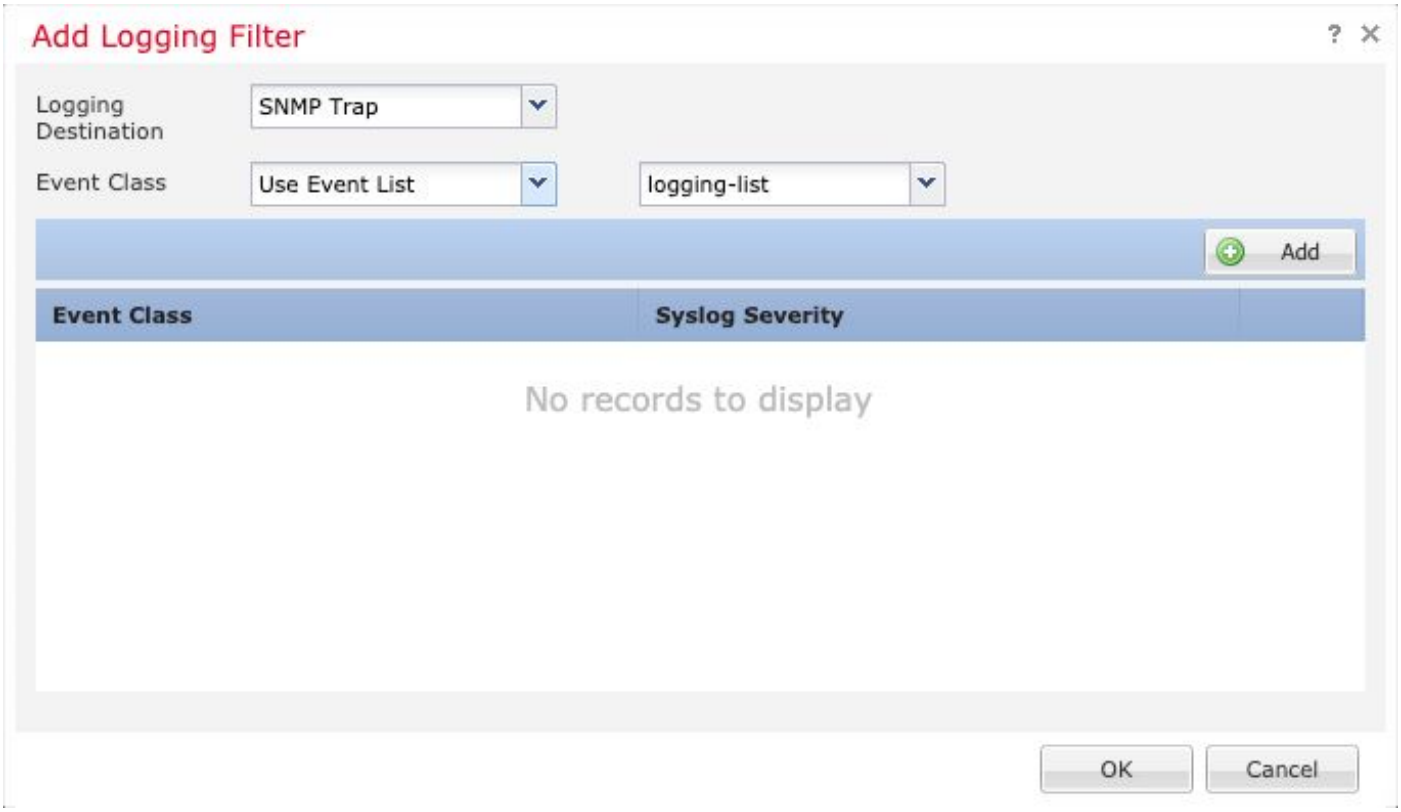


Étape 7. Sélectionnez l'onglet **Destinations de journalisation** et cliquez sur le bouton **Ajouter**.

Modifiez la destination de journalisation en **déroutement SNMP**.

Sélectionnez **Liste d'événements utilisateur** et choisissez la liste d'événements créée à l'étape 6 en regard de celle-ci.

Sélectionnez **OK** pour terminer la modification de cette section.



Étape 8. Sélectionnez le bouton **Enregistrer** et **Déployer** les modifications sur le périphérique géré.

Vérification

Les commandes ci-dessous peuvent être utilisées dans FTD CLISH et ASA CLI.

Afficher les statistiques snmp-server

La commande **show snmp-server statistics** fournit des informations sur le nombre de fois qu'un déroutement a été envoyé. Ce compteur peut inclure d'autres déroutements.

```
# 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
```

L'ID de message utilisé dans cet exemple déclenche chaque fois qu'un utilisateur exécute une commande. Chaque fois qu'une commande show est exécutée, le compteur augmente.

Afficher le paramètre de journalisation

Le **paramètre show logging** fournit des informations sur les messages envoyés par chaque destination. La journalisation de l'historique indique les compteurs des déroutements SNMP. Les statistiques de journalisation des interruptions sont liées aux compteurs hôtes Syslog.

```
# 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
```

Exécutez la commande "**show logging queue**" pour vous assurer qu'aucun message n'est supprimé.

```
# 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
```

Informations connexes

- Messages Syslog de la gamme Cisco ASA
- CII Book 1 : Guide de configuration de la CLI des opérations générales de la gamme Cisco ASA, 9.12
- Configuration du protocole SNMP sur les pare-feu de nouvelle génération Firepower