Configuración de Trampas de Syslog SNMP para ASA y FTD

Contenido

Introducción

Este documento describe cómo configurar las trampas del protocolo simple de administración de red (SNMP) para enviar mensajes de Syslog en Cisco Adaptive Security Appliance (ASA) y Firepower Threat Defense (FTD).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de Cisco ASA
- Conocimiento básico de Cisco FTD
- Conocimiento básico del protocolo SNMP

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software:'

- Cisco Firepower Threat Defense para AWS 6.6.0
- Firepower Management Center versión 6.6.0
- Software Cisco Adaptive Security Appliance versión 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 tiene una red

en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Cisco ASA y FTD tienen varias funciones para proporcionar información de registro. Sin embargo, hay ubicaciones específicas donde un servidor Syslog no es una opción. Las trampas SNMP ofrecen una alternativa si hay un servidor SNMP disponible.

Se trata de una herramienta útil para enviar mensajes específicos con fines de resolución de problemas o supervisión. Por ejemplo, si hay un problema relevante que se debe rastrear durante los escenarios de failover, las trampas SNMP para la clase ha tanto en FTD como en ASA se pueden utilizar para centrarse solamente en esos mensajes.

Puede encontrar más información relacionada con las clases de Syslog en este documento.

El propósito de este artículo es proporcionar ejemplos de configuración para ASA mediante la interfaz de línea de comandos (CLI), FTD gestionado por FMC y FTD gestionado por Firepower Device Manager (FDM).

Si se utiliza Cisco Defense Orchestrator (CDO) para FTD, esta configuración debe agregarse a la interfaz FDM.

> **Precaución:** Para las altas velocidades de syslog, se recomienda configurar un límite de velocidad en los mensajes de syslog para evitar el impacto en otras operaciones.

Esta es la información utilizada para todos los ejemplos de este documento.

Versión SNMP: **SNMPv3**

Grupo SNMPv3: **group-name**

Usuario SNMPv3: **admin-user** con algoritmo HMAC SHA para autenticación

Dirección IP del servidor SNMP: **10.20.15.12**

Interfaz ASA/FTD para comunicarse con el servidor SNMP: **Fuera**

ID de mensaje de Syslog: **111009**

Configurar

Configuración ASA

Estos pasos se pueden utilizar para configurar las trampas SNMP en un ASA siguiendo la siguiente información.

Paso 1. Configure los mensajes que desea agregar a la lista Syslog.

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

Paso 2. Configure los parámetros del servidor SNMPv3.

```
snmp-server enable

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

Paso 3. Habilite las trampas SNMP.

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

Paso 4. Agregue las trampas SNMP como destino de registro.

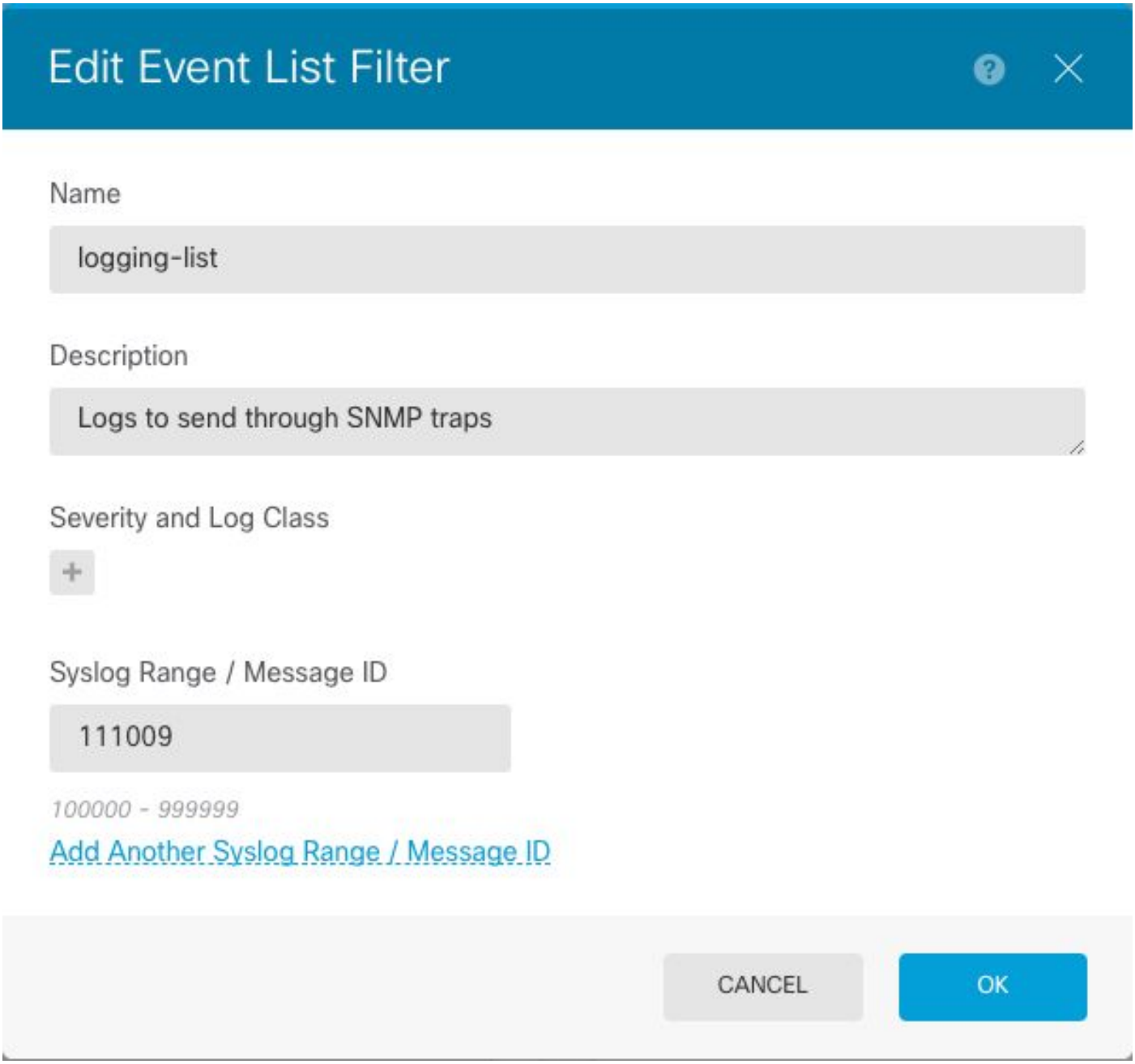
```
logging history syslog-list
```

Configuración de FTD administrada por FDM

Estos pasos se pueden utilizar para configurar una lista de Syslog específica para enviarla al servidor SNMP cuando FTD es administrado por FDM.

Paso 1. Navegue hasta **Objetos > Filtros de lista de eventos** y seleccione en el **+** botón.

Paso 2. Asigne un nombre a la lista par e incluya las clases o ID de mensaje relevantes. A continuación, seleccione OK (Aceptar).



Paso 3. Vaya a Advanced **Configuration > FlexConfig > FlexConfig Objects** desde la pantalla de inicio de FDM y seleccione el **+** botón.

Cree los siguientes objetos FlexConfig con la información que se muestra:

Nombre: **SNMP-Server**

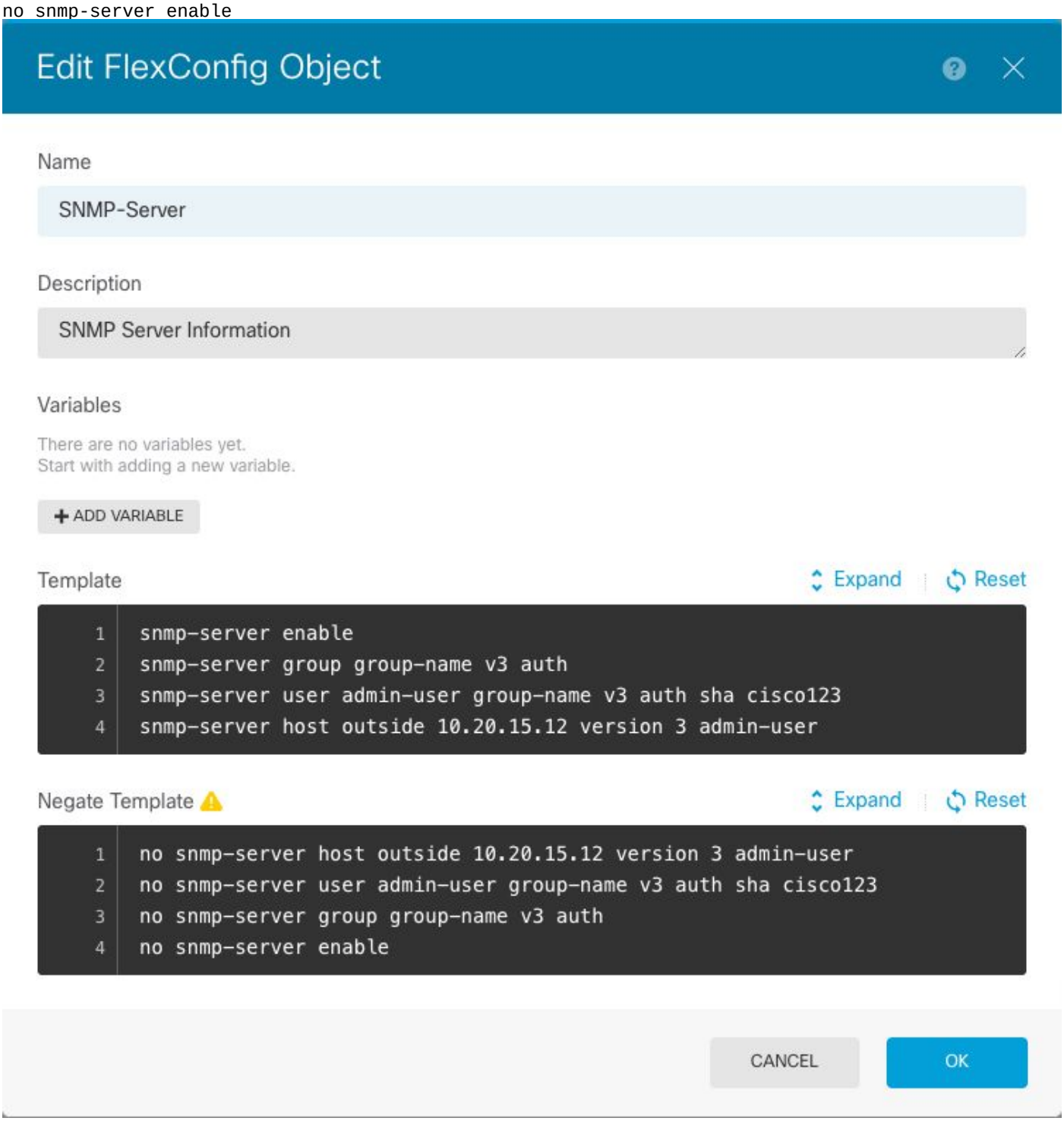
Descripción (opcional): **Información del servidor SNMP**

Plantilla:

```
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
```

Negar plantilla:

```
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
```



Nombre: **SNMP-Traps**

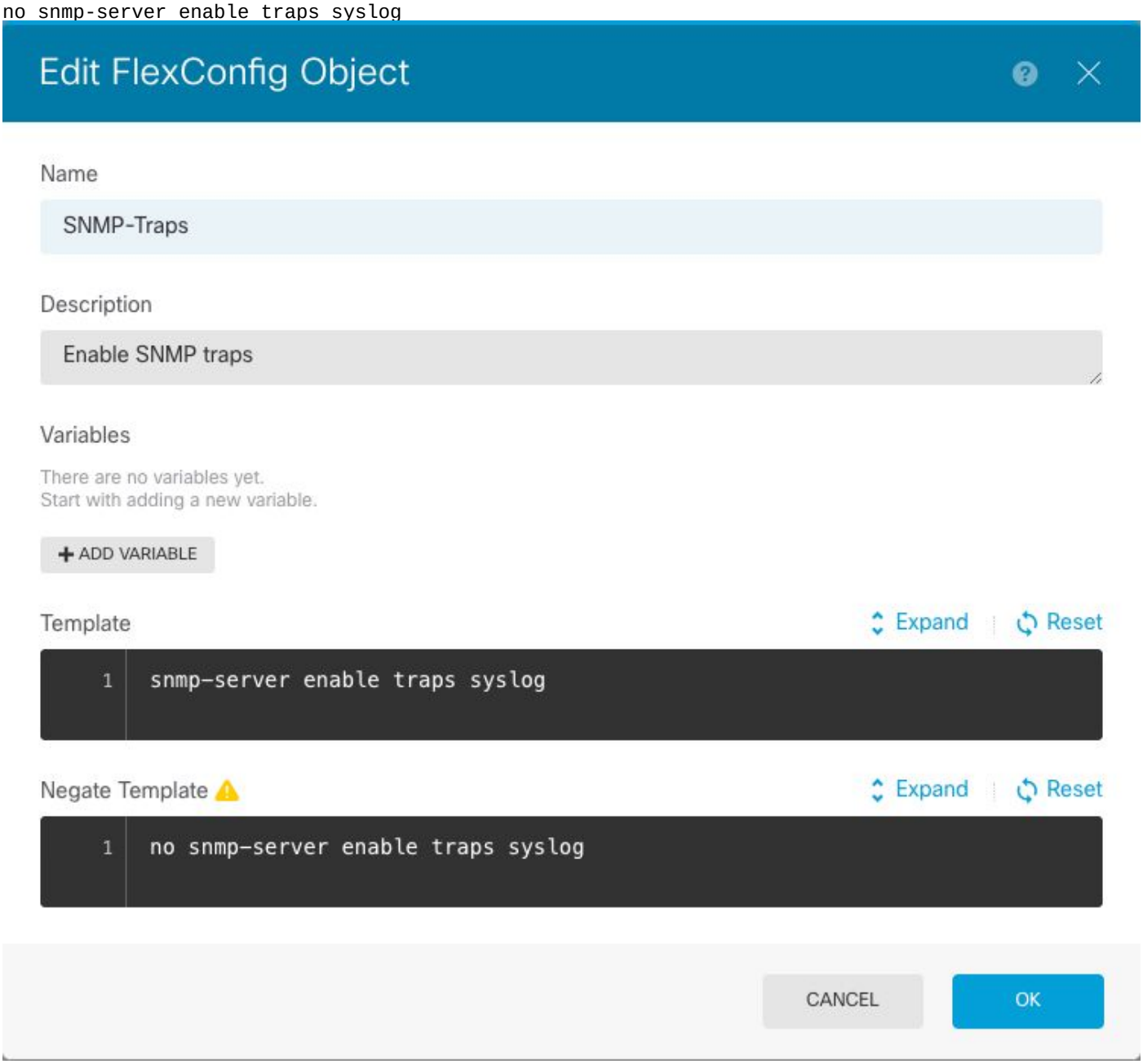
Descripción (opcional): **Habilitar trampas SNMP**

Plantilla:

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

Negar plantilla:

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



Nombre: **Registro-historial**

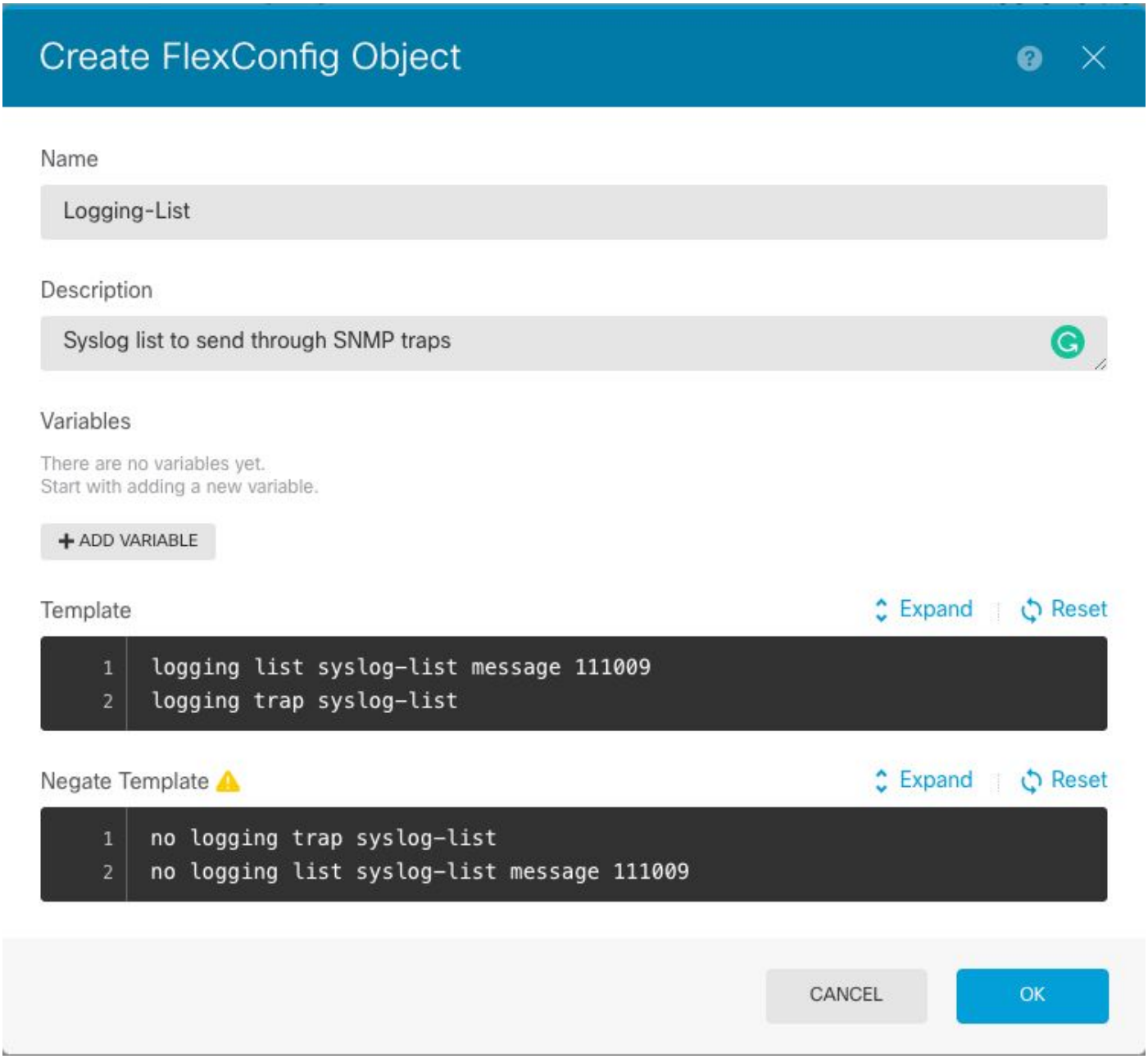
Descripción (opcional): **Objeto para establecer los mensajes de syslog de trampas SNMP**

Plantilla:

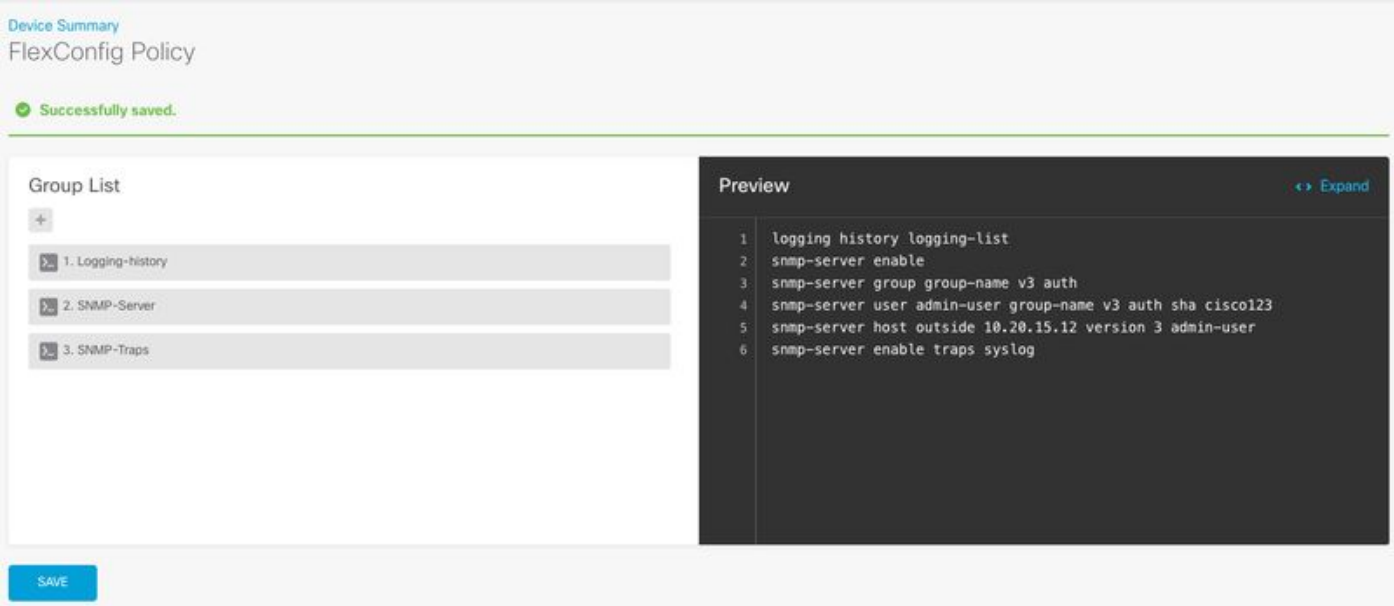
```
logging history logging-list
```

Negar plantilla:

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



Paso 4. Navegue hasta **Configuración avanzada > FlexConfig > Política FlexConfig** y agregue todos los objetos creados en el paso anterior. El orden es irrelevante, ya que los comandos dependientes se incluyen en el mismo objeto (SNMP-Server). Seleccione **Guardar** una vez que los tres objetos estén allí y la sección **Vista previa** muestra la lista de comandos.



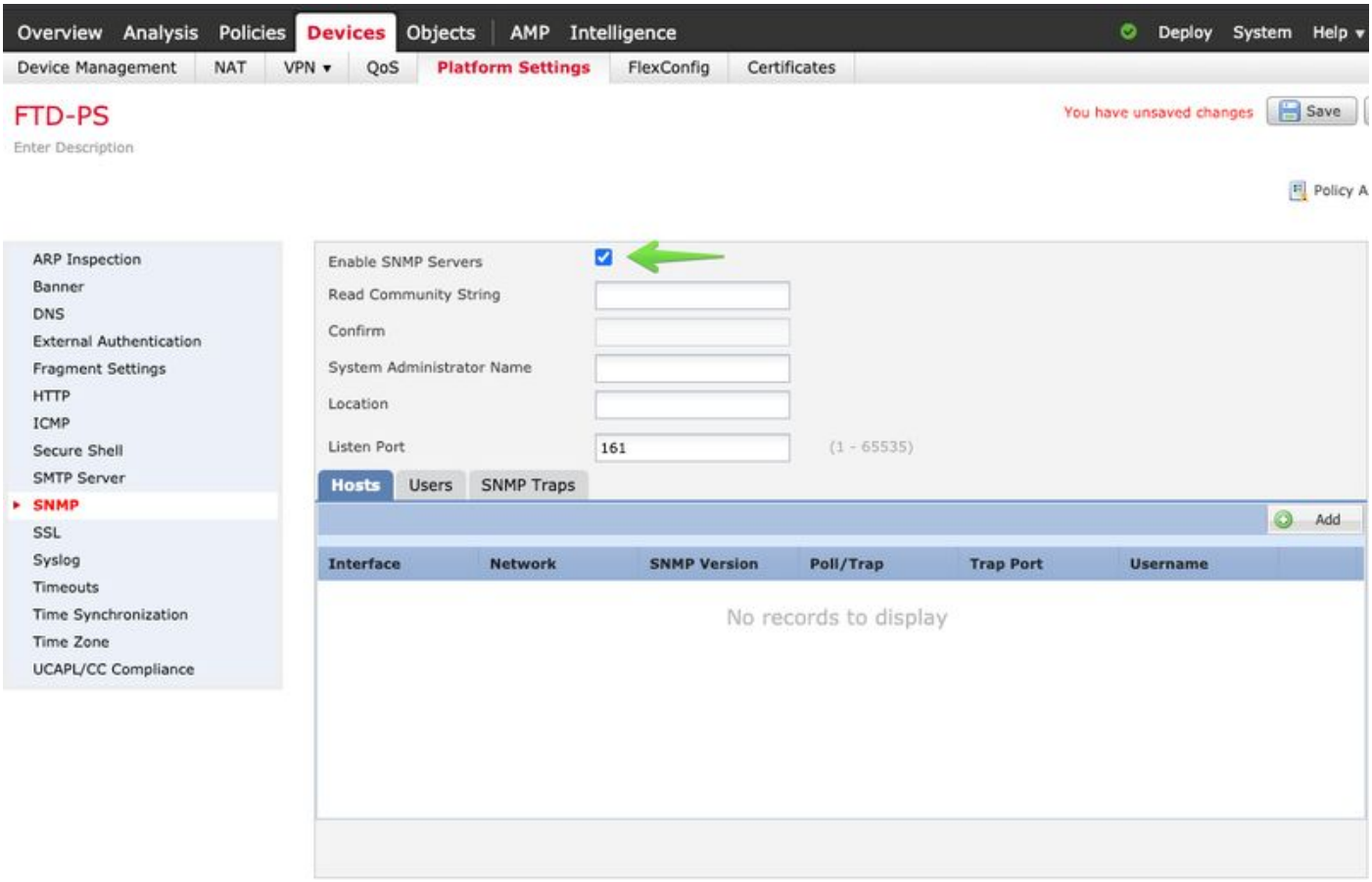
Paso 5. Seleccione el icono **Implementar** para aplicar los cambios.

Configuración de FTD administrada por FMC

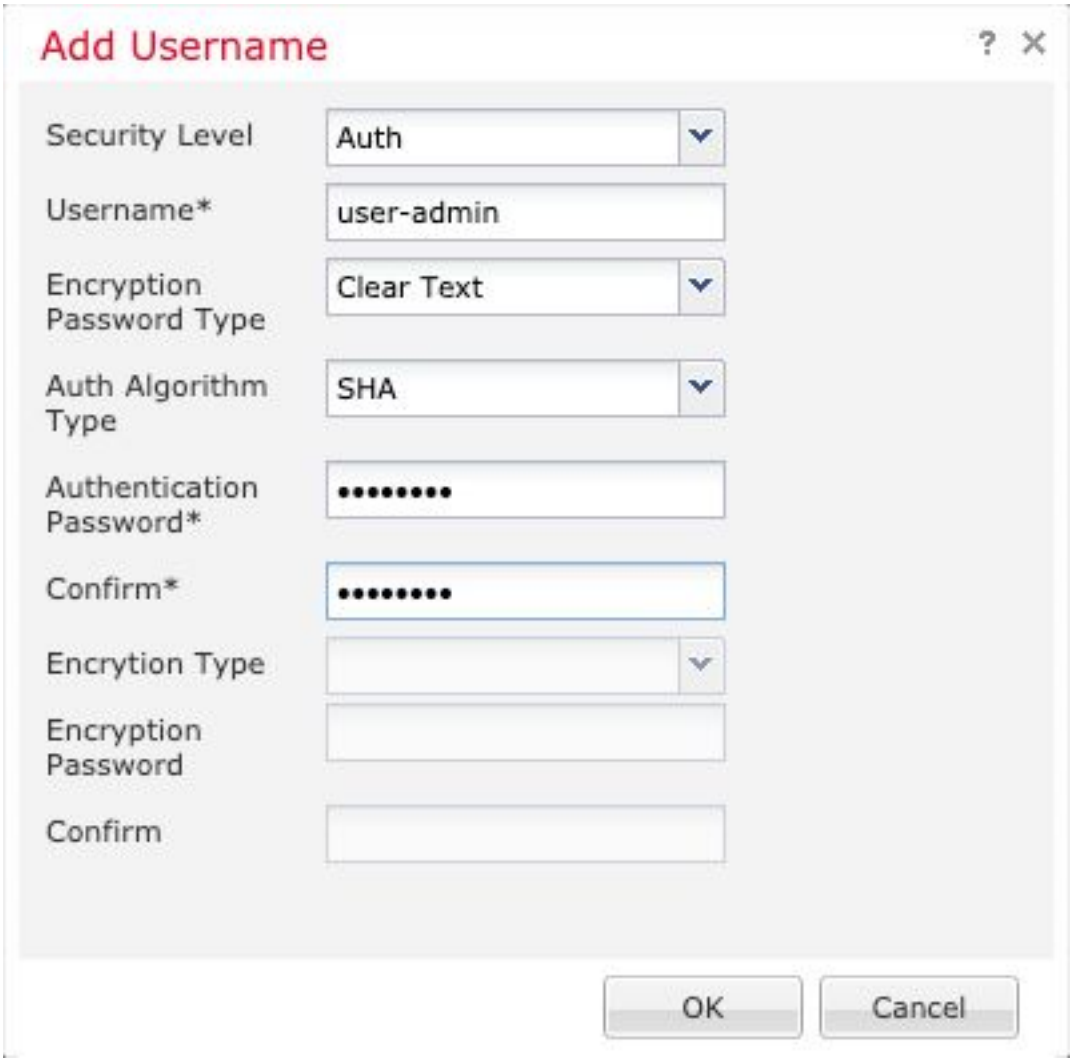
Los ejemplos anteriores ilustran escenarios similares a los anteriores, pero estos cambios se configuran en el FMC y luego se implementan en un FTD administrado por él. También se puede utilizar SNMPv2. Este artículo explica cómo utilizar configurar un servidor SNMP con esta versión en FTD mediante la administración de FMC.

Paso 1. Navegue hasta **Dispositivos > Configuración de plataforma** y seleccione **Editar** en la Política asignada al dispositivo administrado para aplicar la configuración.

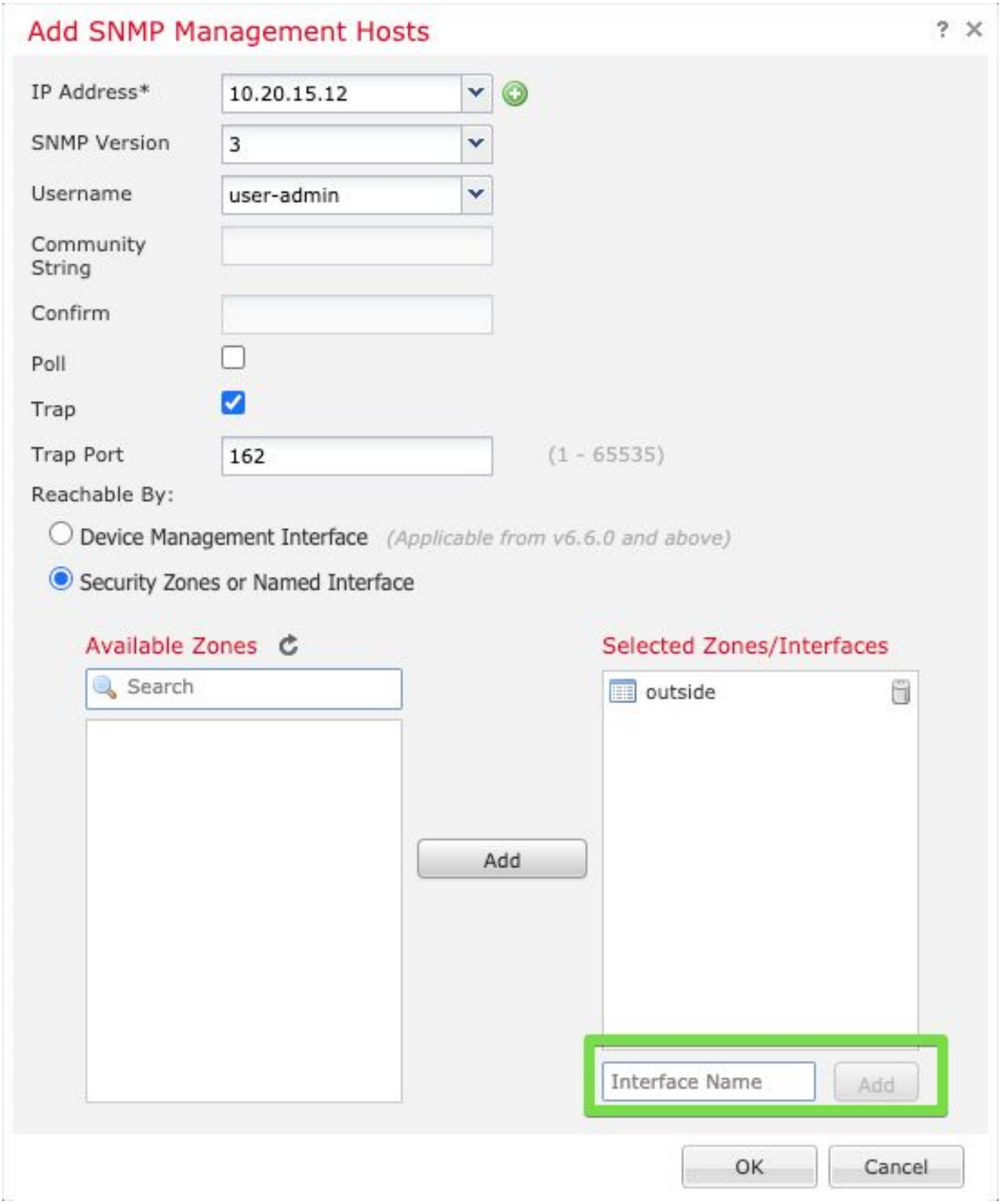
Paso 2. Navegue hasta **SNMP** y verifique la opción **Enable SNMP Servers**.



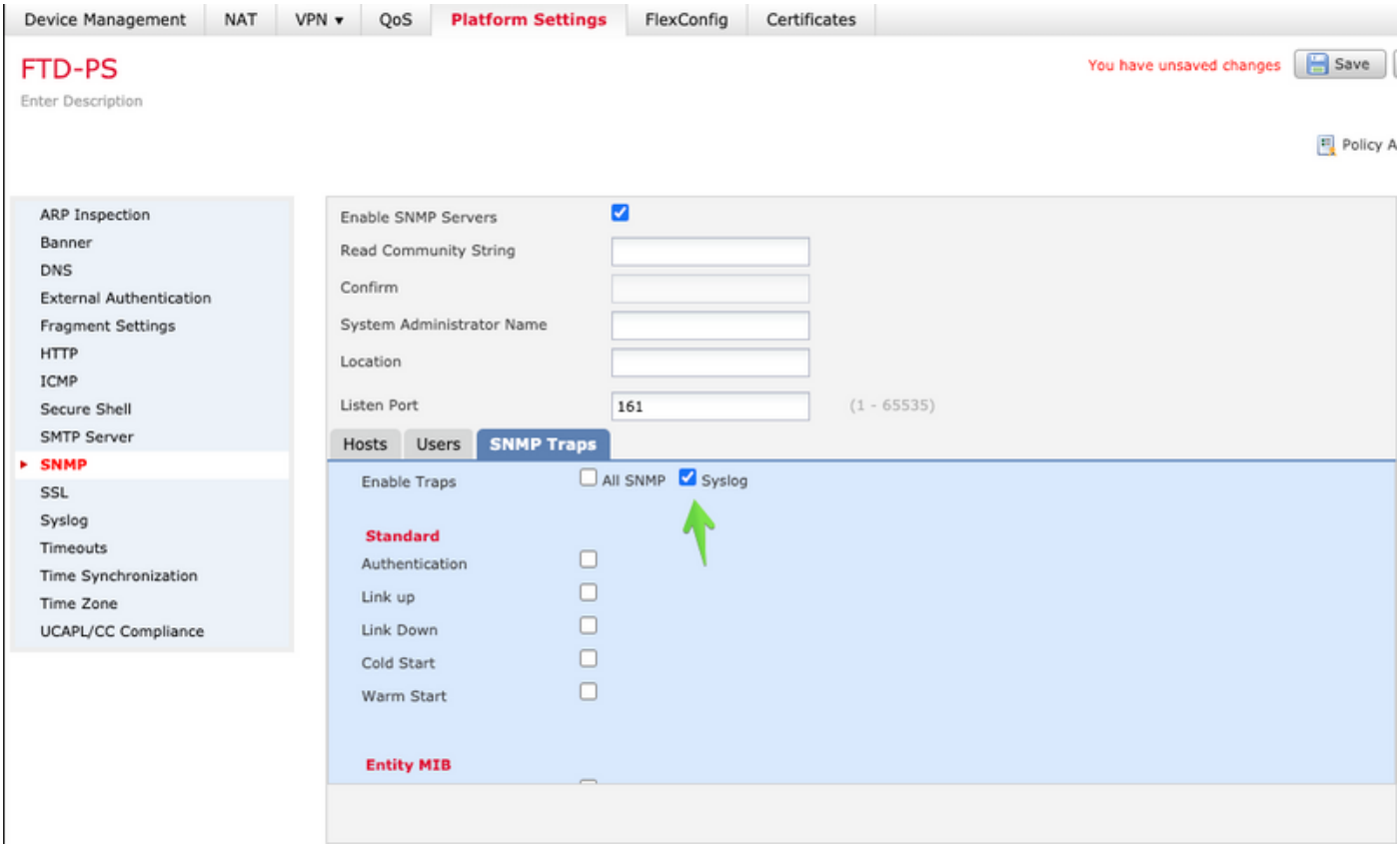
Paso 3. Seleccione la pestaña **Usuarios** y seleccione el **botón Agregar**. Complete la información del usuario.



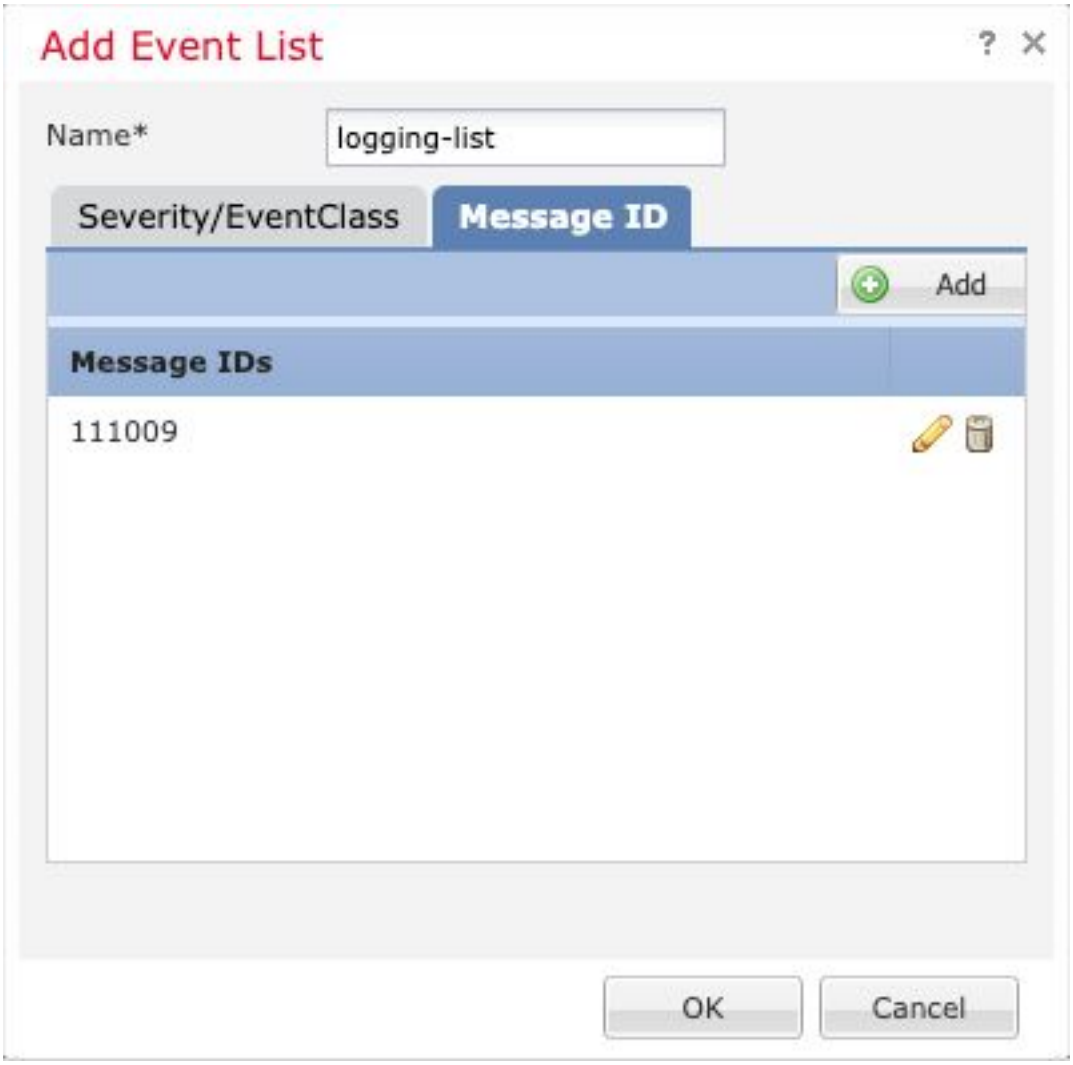
Paso 4. Seleccione **Agregar** en la **pestaña Hosts**. Complete la información relacionada con el servidor SNMP. Si utiliza una interfaz en lugar de una zona, asegúrese de agregar manualmente el nombre de la interfaz en la sección de la esquina derecha. Seleccione OK (Aceptar) una vez que se haya incluido toda la información necesaria.



Paso 5. Seleccione la pestaña **SNMP Traps** y marque la **casilla Syslog**. Asegúrese de eliminar todas las demás marcas de verificación de trampas si no son necesarias.



Paso 6. Navegue hasta **Syslog** y seleccione la **pestaña Listas de Eventos**. Seleccione el botón **Agregar**. Agregue un nombre y los mensajes que desea incluir en la lista. Seleccione **Aceptar** para continuar.

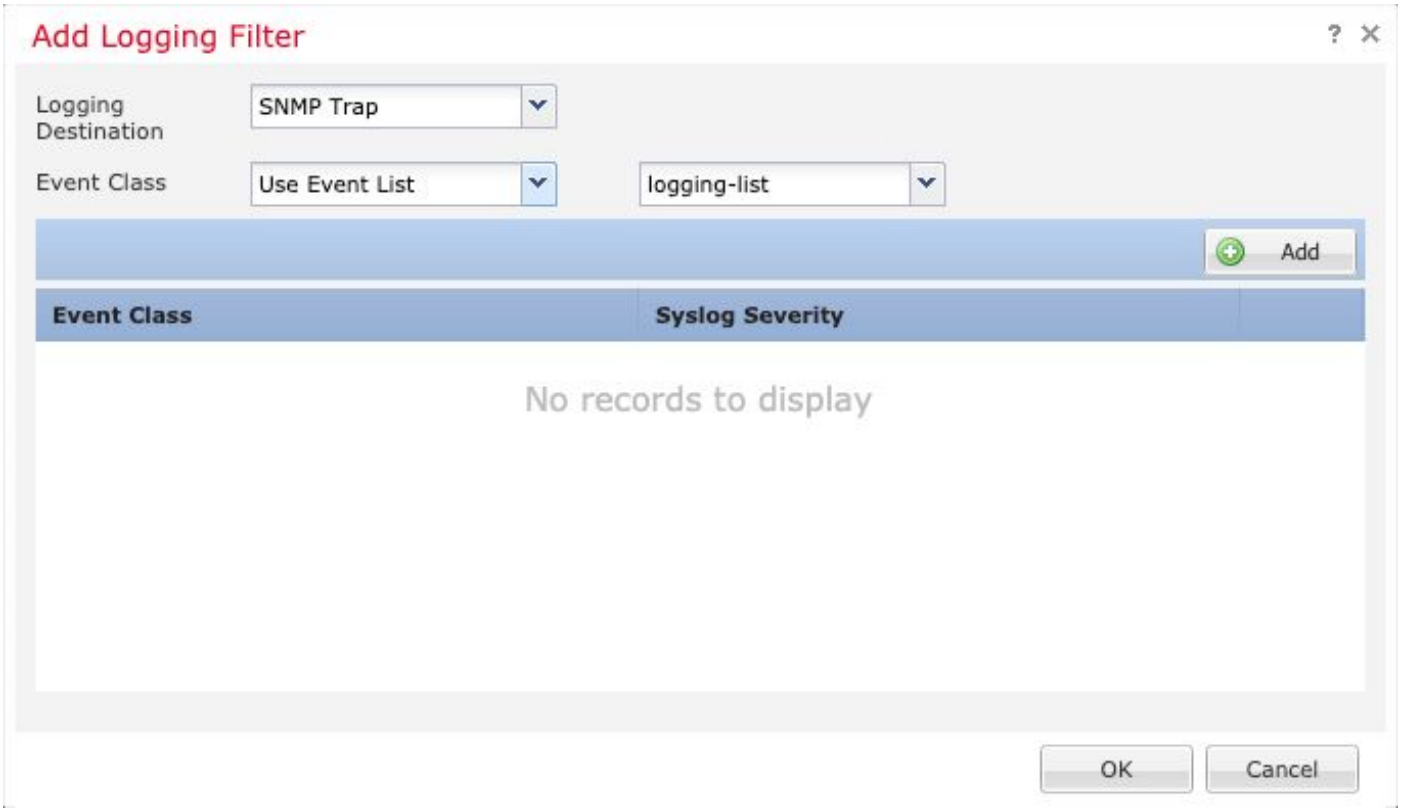


Paso 7. Seleccione la pestaña **Destinos de registro** y seleccione el **botón Agregar**.

Cambie el Destino de Registro a **Trampa SNMP**.

Seleccione **User Event List** y elija la lista de eventos creada en el Paso 6 junto a ella.

Seleccione **Aceptar** para finalizar la edición de esta sección.



Paso 8. Seleccione el botón **Guardar** y **Implementar** los cambios en el dispositivo administrado.

Verificación

Los siguientes comandos se pueden utilizar tanto en FTD CLISH como en ASA CLI.

Show snmp-server statistics

El comando "**show snmp-server statistics**" proporciona información sobre cuántas veces se ha enviado una trampa. Este contador puede incluir otras trampas.

```
# 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
```

El ID de mensaje utilizado en este ejemplo se activa cada vez que un usuario ejecuta un comando. Cada vez que se ejecuta un comando "show", el contador aumenta.

Mostrar configuración de registro

El "**show logging setting**" proporciona información sobre los mensajes enviados por cada destino. El registro del historial indica los contadores para las trampas SNMP. Las estadísticas de registro de trampas están relacionadas con los contadores de hosts 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
```

Ejecute el comando "**show logging queue**" para asegurarse de que no se descarten mensajes.

```
# 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
```

Información Relacionada

- Mensajes de Syslog de la serie ASA de Cisco
- Libro CLI 1: Guía de Configuración de la CLI de Cisco ASA Series General Operations, 9.12
- Configuración de SNMP en dispositivos Firepower NGFW