تكوين ملائمات SNMP Syslog ل ASA و FTD

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
معلومات أساسية
التكوين
تكوين ASA
تكوين FTD المدار من قبل FDM
تكوين FTD المدار من قبل FMC
التحقق من الصحة
إظهار إحصائيات خادم SNMP
إظهار إعداد التسجيل
معلومات ذات صلة

المقدمة

يصف هذا المستند كيفية تكوين إختبارات بروتوكول إدارة الشبكة البسيط (SNMP) للإرسال رسائل syslog على جهاز الأمان القابل للتكيف (ASA) من Cisco والدفاع عن تهديد FirePOWER (FTD).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة أساسية ب Cisco ASA
- معرفة أساسية ب Cisco FTD
- معرفة أساسية ببروتوكول SNMP

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدار البرنامج التالي:

- الدفاع ضد تهديد Cisco Firepower ل AWS 6.6.0
- Firepower Management Center، الإصدار 6.6.0
- برنامج جهاز الأمان القابل للتكيف من Cisco، الإصدار 9.12(3)9

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يحتوي ASA و FTD من Cisco على إمكانات متعددة لتوفير معلومات التسجيل. ومع ذلك، هناك عوامل محددة حيث لا يكون خادم syslog خيارا. تقدم إختبارات SNMP بديلا إذا كان هناك خادم SNMP متوفر.

هذه أداة مفيدة لإرسال رسائل خاصة لأغراض أستكشاف الأخطاء وإصلاحها أو المراقبة. على سبيل المثال، إذا كانت هناك مشكلة ذات صلة يلزم تعقبها أثناء سيناريوهات تجاوز الفشل، يمكن إستخدام إختبارات SNMP للفئة HA على كل من FTD و ASA للتركيز على هذه الرسائل فقط.

يمكن العثور على مزيد من المعلومات المتعلقة بفئات Syslog في هذا المستند.

الغرض من هذه المقالة هو توفير أمثلة تكوين ل ASA باستخدام واجهة سطر الأوامر (CLI)، وميزة FTD التي تتم إدارتها بواسطة FMC، وميزة FTD التي تتم إدارتها بواسطة FirePOWER Device Manager (FDM).

إذا تم إستخدام Cisco Defense Orchestrator (CDO) ل FTD، فيجب إضافة هذا التكوين إلى واجهة FDM.

> **تحذير**: بالنسبة لمعدلات syslog المرتفعة، يوصى بتكوين حد معدل على رسائل syslog لمنع التأثير في العمليات الأخرى.

هذه هي المعلومات المستخدمة لجميع الأمثلة الواردة في هذا المستند.

إصدار SNMP: **SNMPv3**

مجموعة SNMPv3: **اسم المجموعة**

مستخدم SNMPv3: **admin-user** مع خوارزمية HMAC SHA للمصادقة

عنوان IP لخادم SNMP: **10.20.15.12**

واجهة ASA/FTD المطلوب إستخدامها للاتصال بخادم SNMP: **خارج**

Syslog Message-id: **11009**

التكوين

تكوين ASA

يمكن إستخدام هذه الخطوات لتكوين مثال SNMP على ASA بعد المعلومات التالية.

الخطوة 1. قم بتكوين الرسائل لإضافتها إلى قائمة syslog.

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

الخطوة 2. تكوين معلمات خادم SNMPv3.

```
snmp-server enable

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

الخطوة 3. تمكين مالئمات SNMP.

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

الخطوة 4. إضافة مالئمات SNMP كوجهة تسجيل.

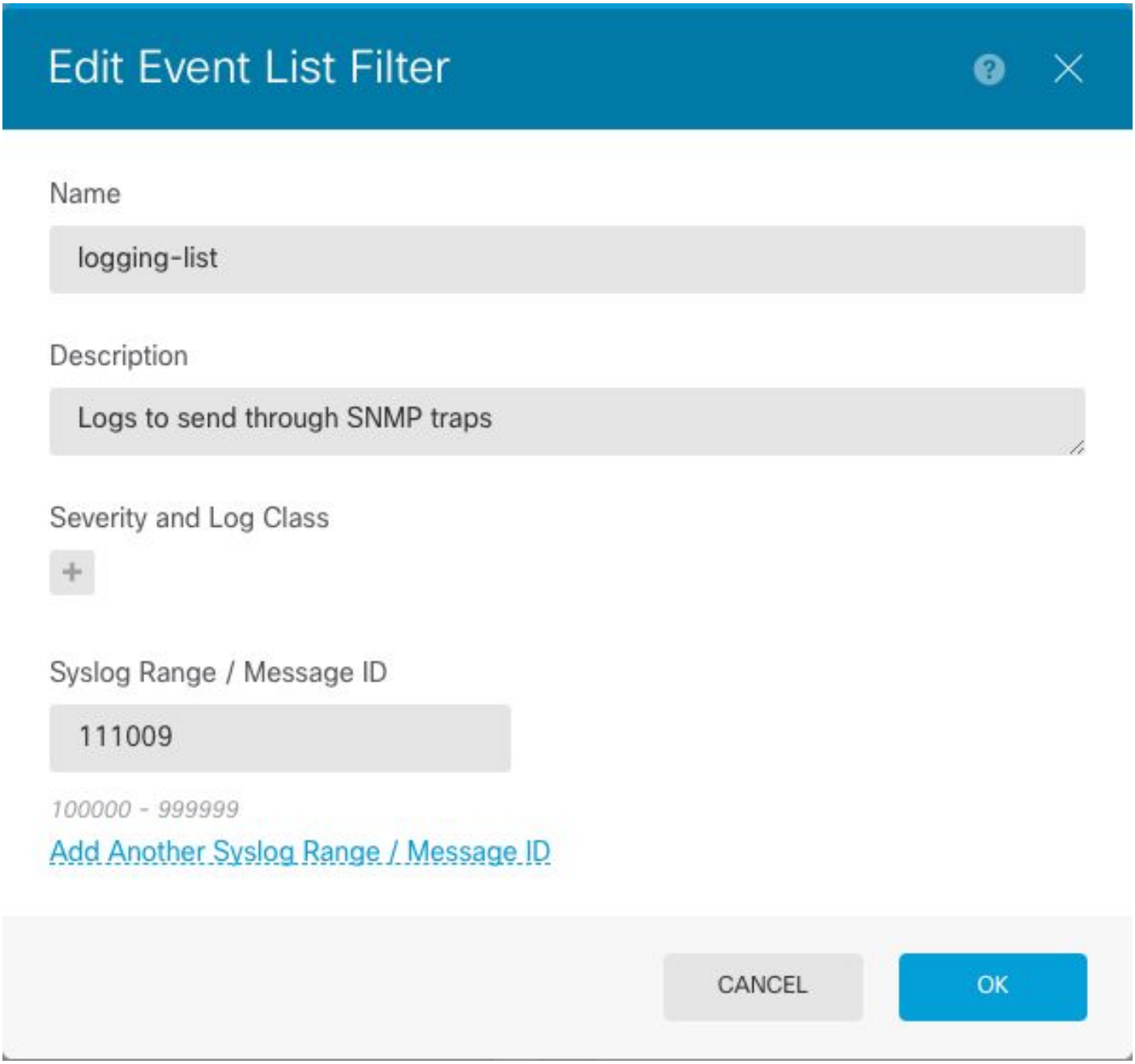
```
logging history syslog-list
```

تكوين FTD المدار من قبل FDM

يمكن إستخدام هذه الخطوات لتكوين قائمة syslog معينة لإرسالها إلى خادم SNMP عند إدارة FTD بواسطة FDM.

الخطوة 1. انتقل إلى **كائنات > مرشحات قائمة الأحداث** وحدد على زر **+**.

الخطوة 2. قم بتسمية قائمة الوزجية وقم بتضمين الفئات أو معرفات الرسائل ذات الصلة. ثم حدد موافق.



الخطوة 3. انتقل إلى **تكوين** متقدم > **FlexConfig** > **كائنات FlexConfig** من الشاشة الرئيسية ل FDM وحدد الزر **+**.

قم بإنشاء كائنات FlexConfig التالية باستخدام المعلومات المدرجة:

الاسم: **خادم SNMP**

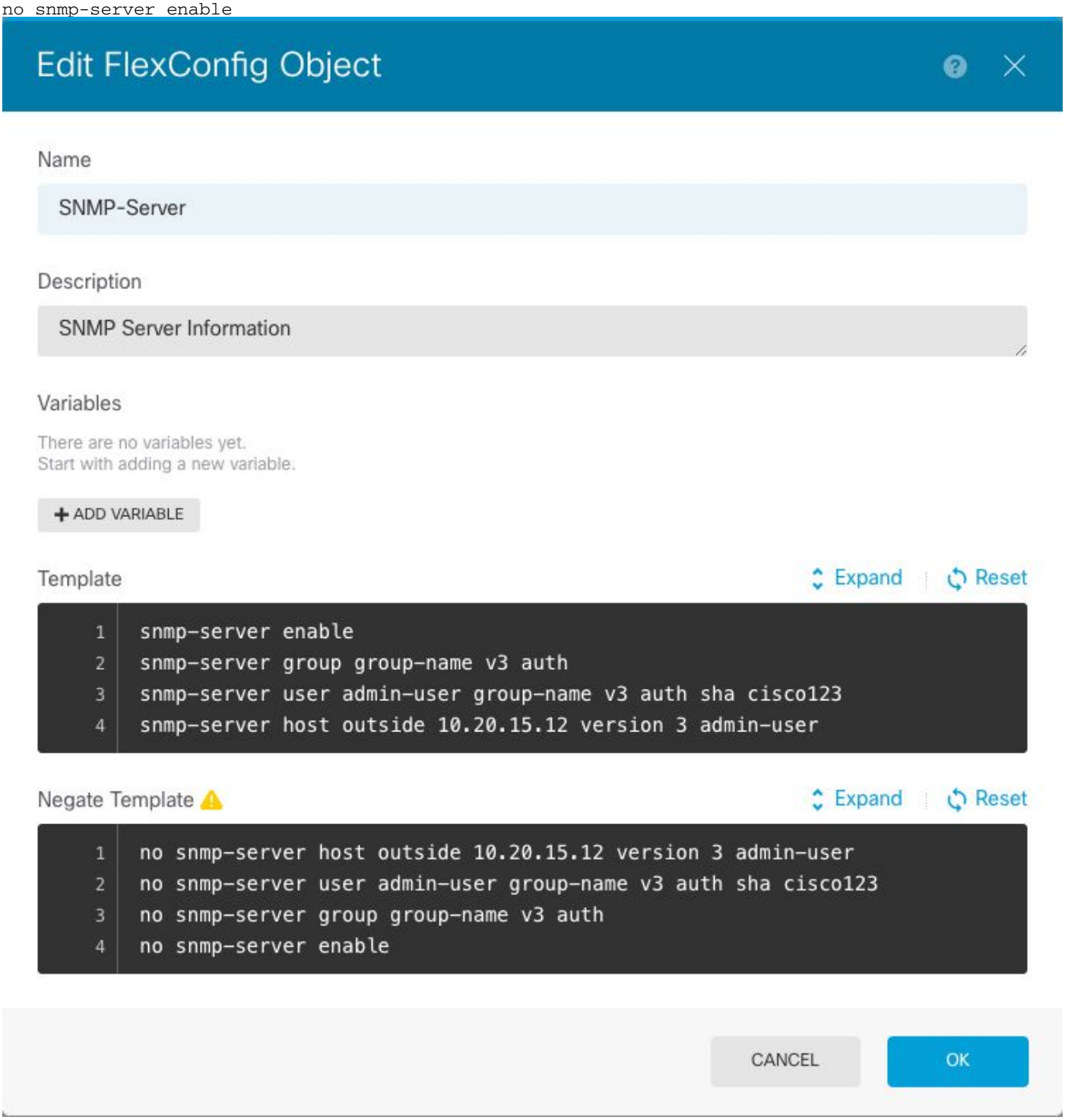
الوصف (إختياري): **معلومات خادم SNMP**

القالب:

```
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
```

قالب غير صالح:

```
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
```



الاسم: **SNMP-TRAPS**

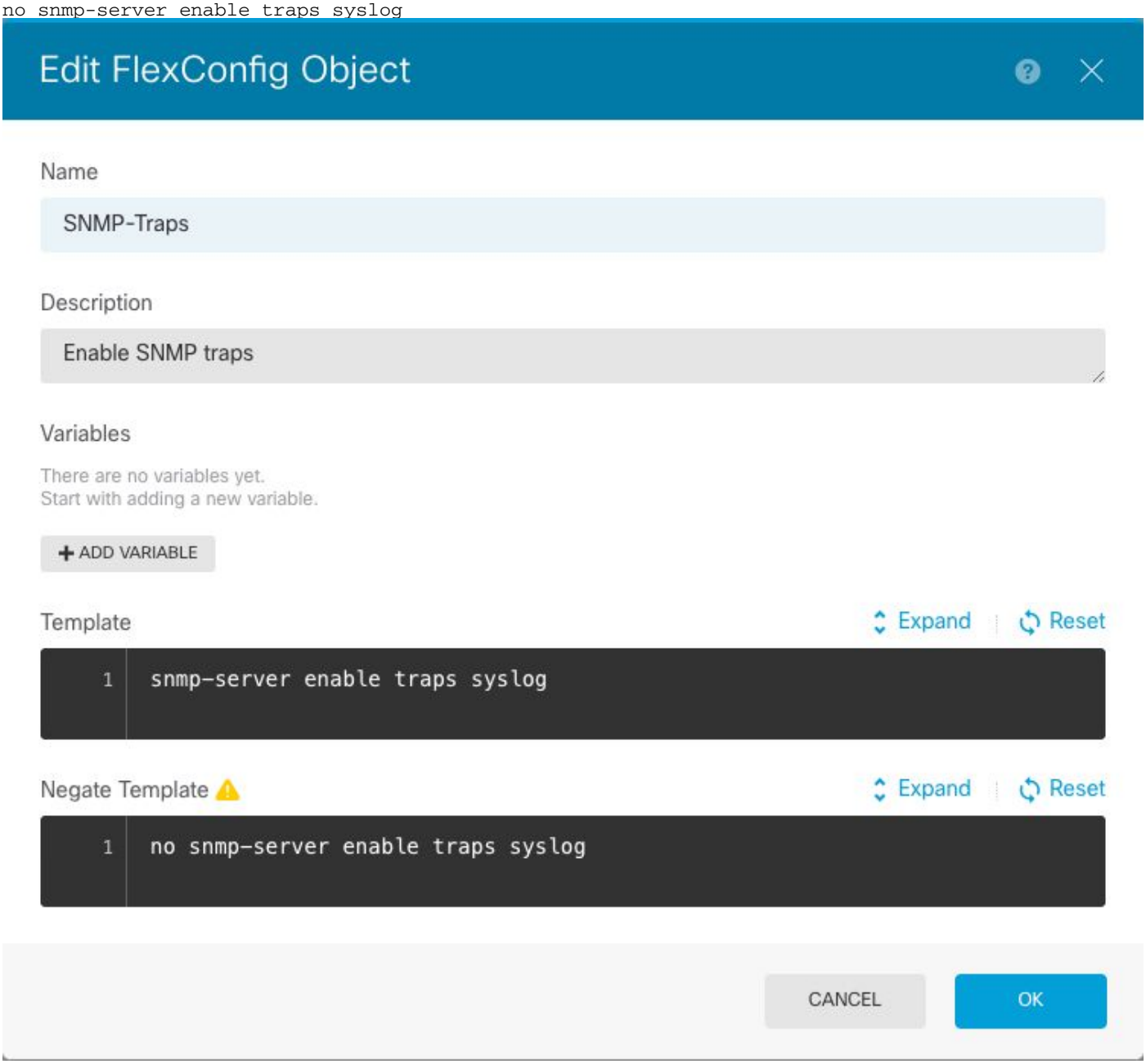
الوصف (إختياري): **تمكين مصائد SNMP**

القالب:

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

قالب غير صالح:

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



الاسم: **محفوظات التسجيل**

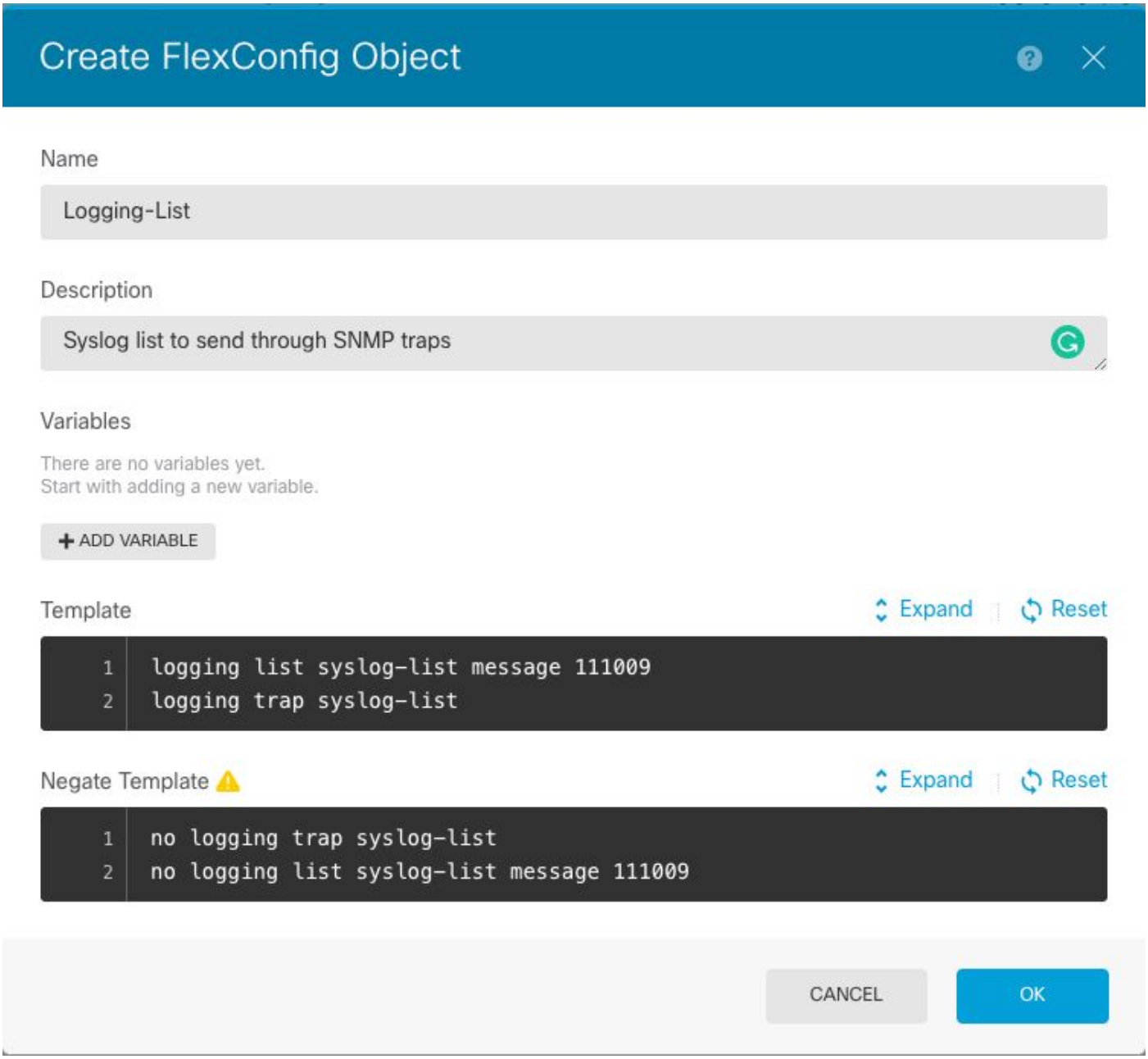
الوصف (إختياري): **كائن لتعيين رسائل syslog لمواقع SNMP**

القالب:

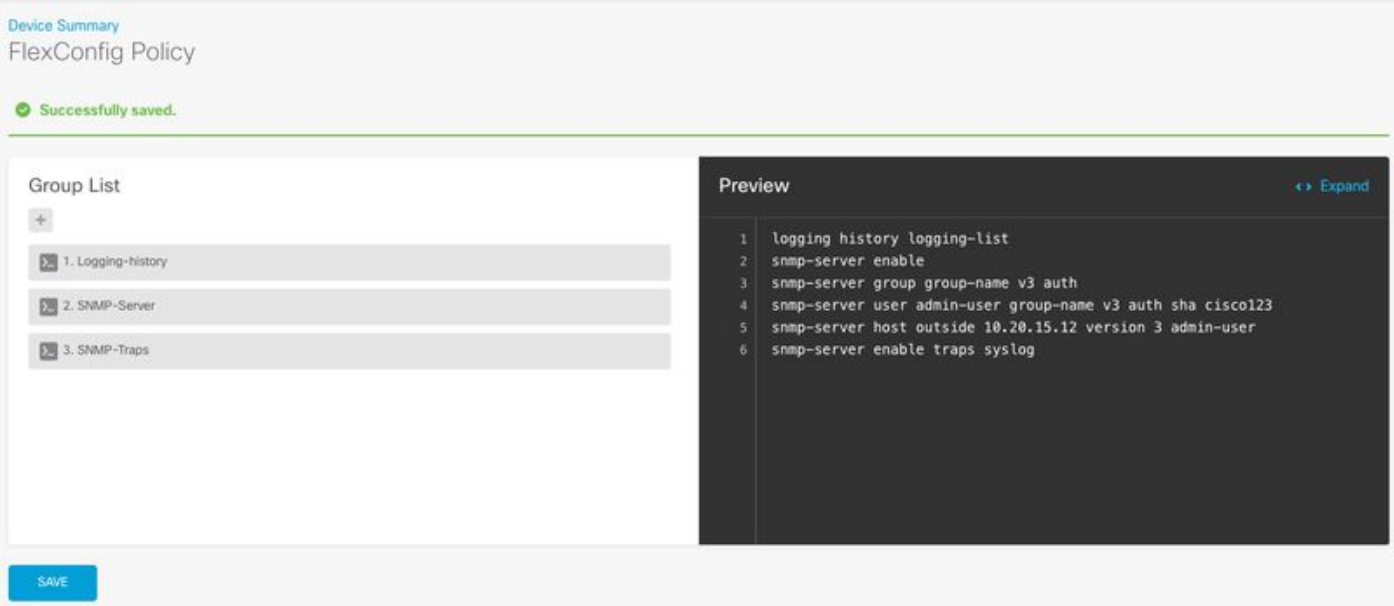
```
logging history logging-list
```

قالب غير صالح:

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



الخطوة 4. انتقل إلى **تكوين متقدم > FlexConfig > نهج FlexConfig** وأضف جميع الكائنات التي تم إنشاؤها في الخطوة السابقة. الأمر غير ذي صلة حيث أن الأوامر التابعة يتم تضمينها في نفس الكائن (خادم SNMP). حدد **حفظ** بمجرد أن تكون الكائنات الثلاثة هناك ويظهر قسم **المعاينة** قائمة الأوامر.



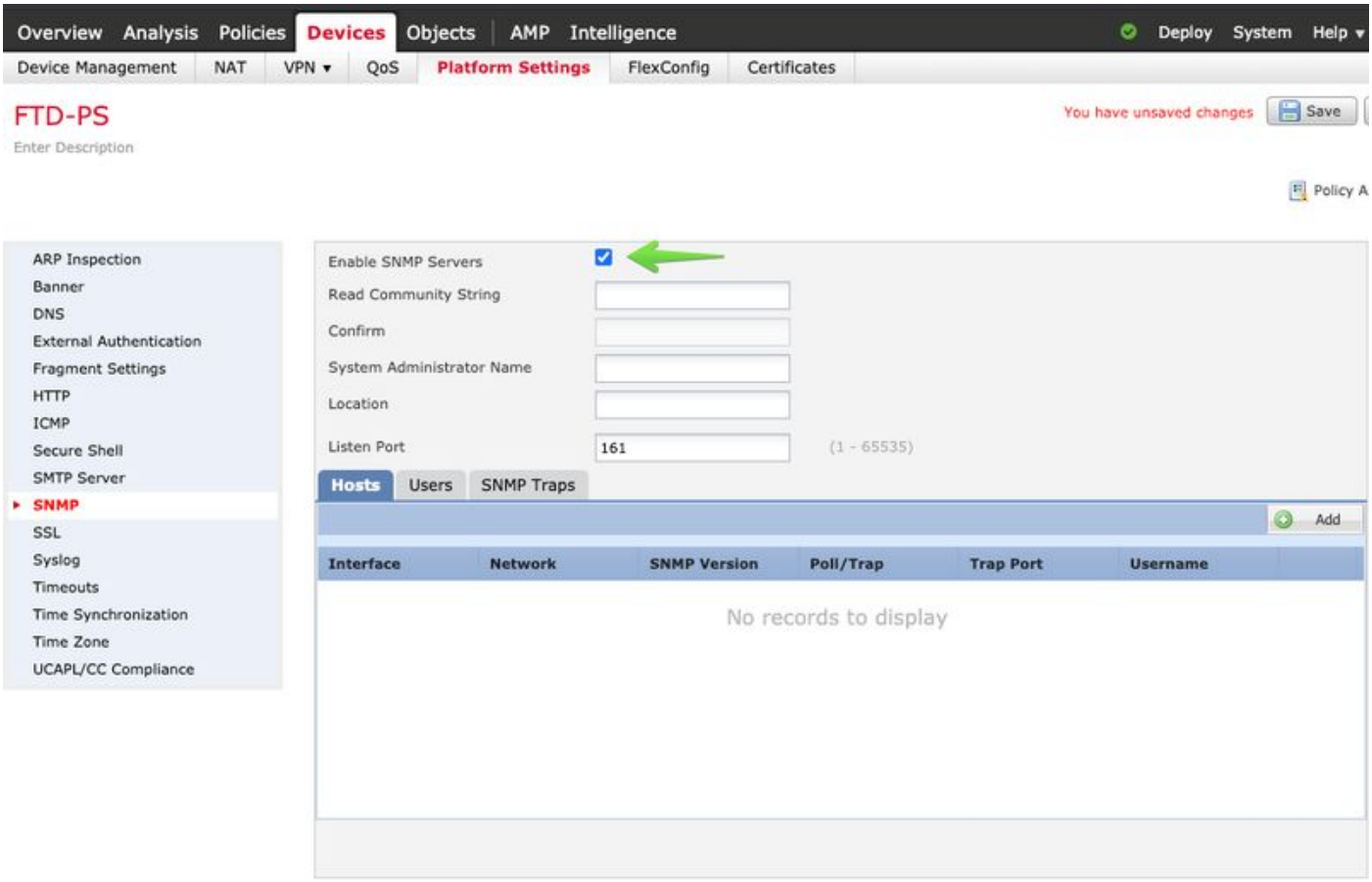
الخطوة 5. حدد أيقونة **توزيع** لتطبيق التغييرات.

تكوين FTD المدار من قبل FMC

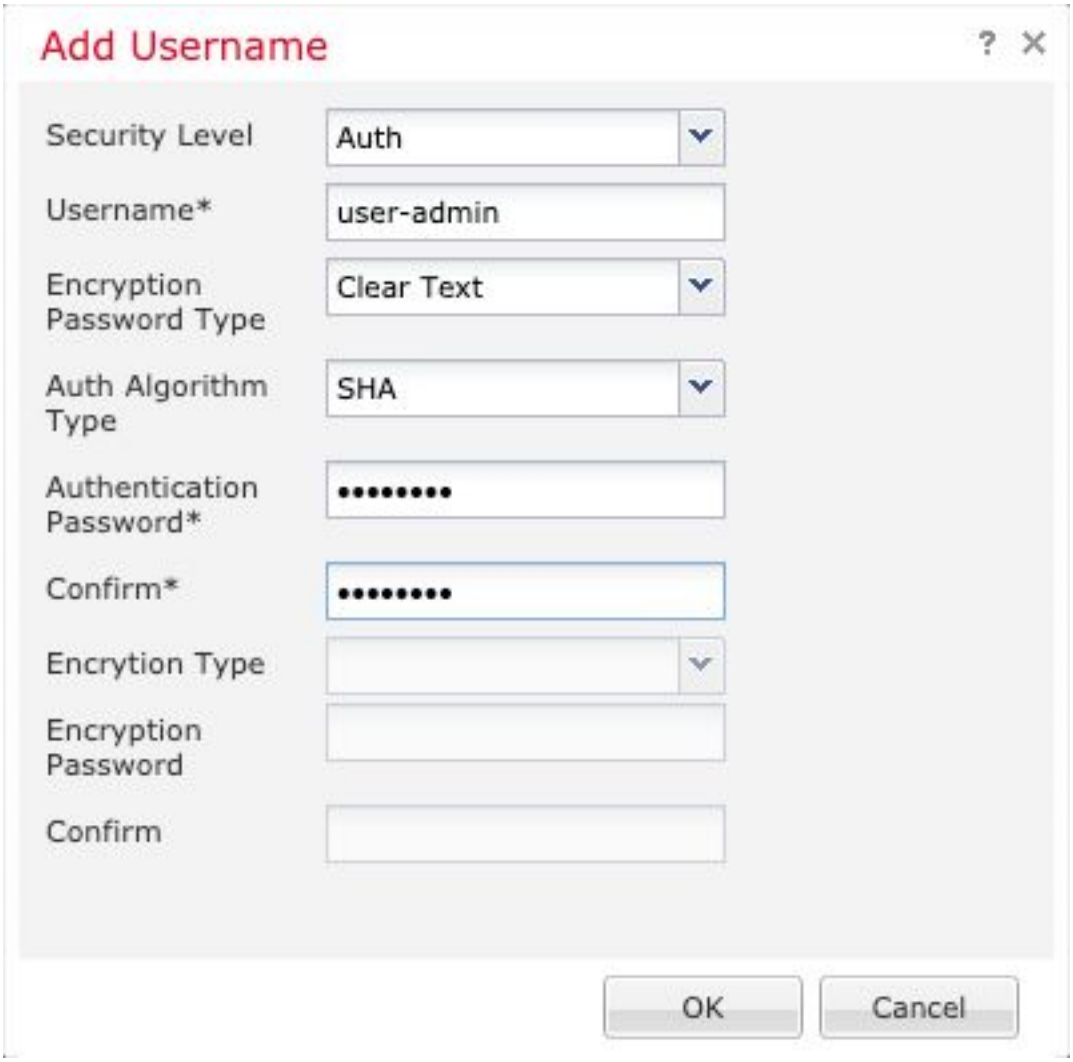
توضح الأمثلة الواردة أعلاه سيناريوهات مماثلة لتلك التي كانت موجودة في السابق، ولكن تم تكوين هذه التغييرات على وحدة التحكم في إدارة اللوحة الأساسية (FMC) ثم تم نشرها إلى "برنامج الإرسال فائق السرعة (FTD)" الذي تديره. كما يمكن إستخدام SNMPv2. يشرح هذا المقال كيفية إستخدام إعداد خادم SNMP باستخدام هذا الإصدار على FTD باستخدام إدارة FMC.

الخطوة 1. انتقل إلى **الأجهزة > إعدادات النظام الأساسي** وحدد **تحرير** في النهج المعين إلى الجهاز المدار لتطبيق التكوين عليه.

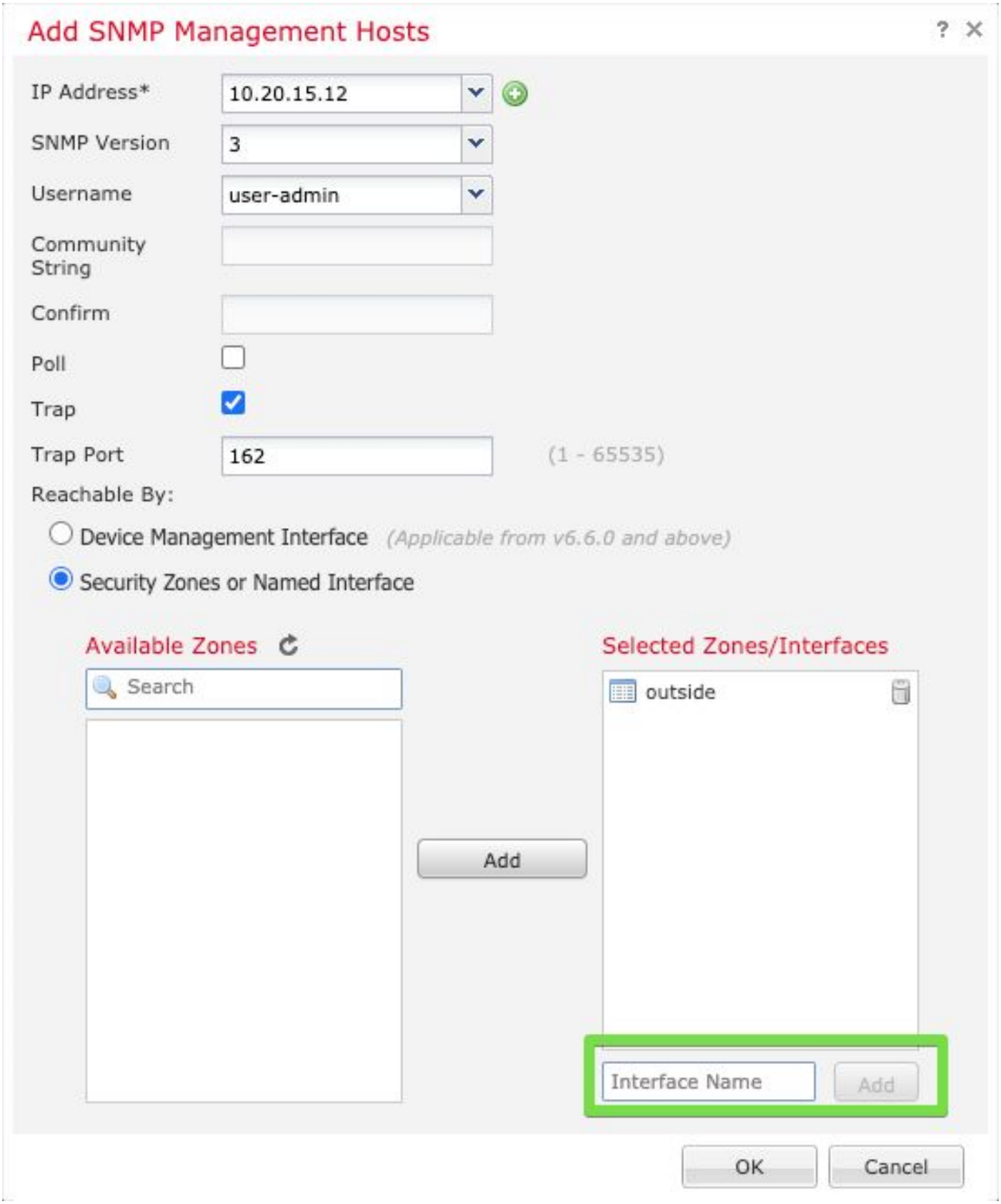
الخطوة 2. انتقل إلى **SNMP** وحدد خيار **تمكين خوادم SNMP**.



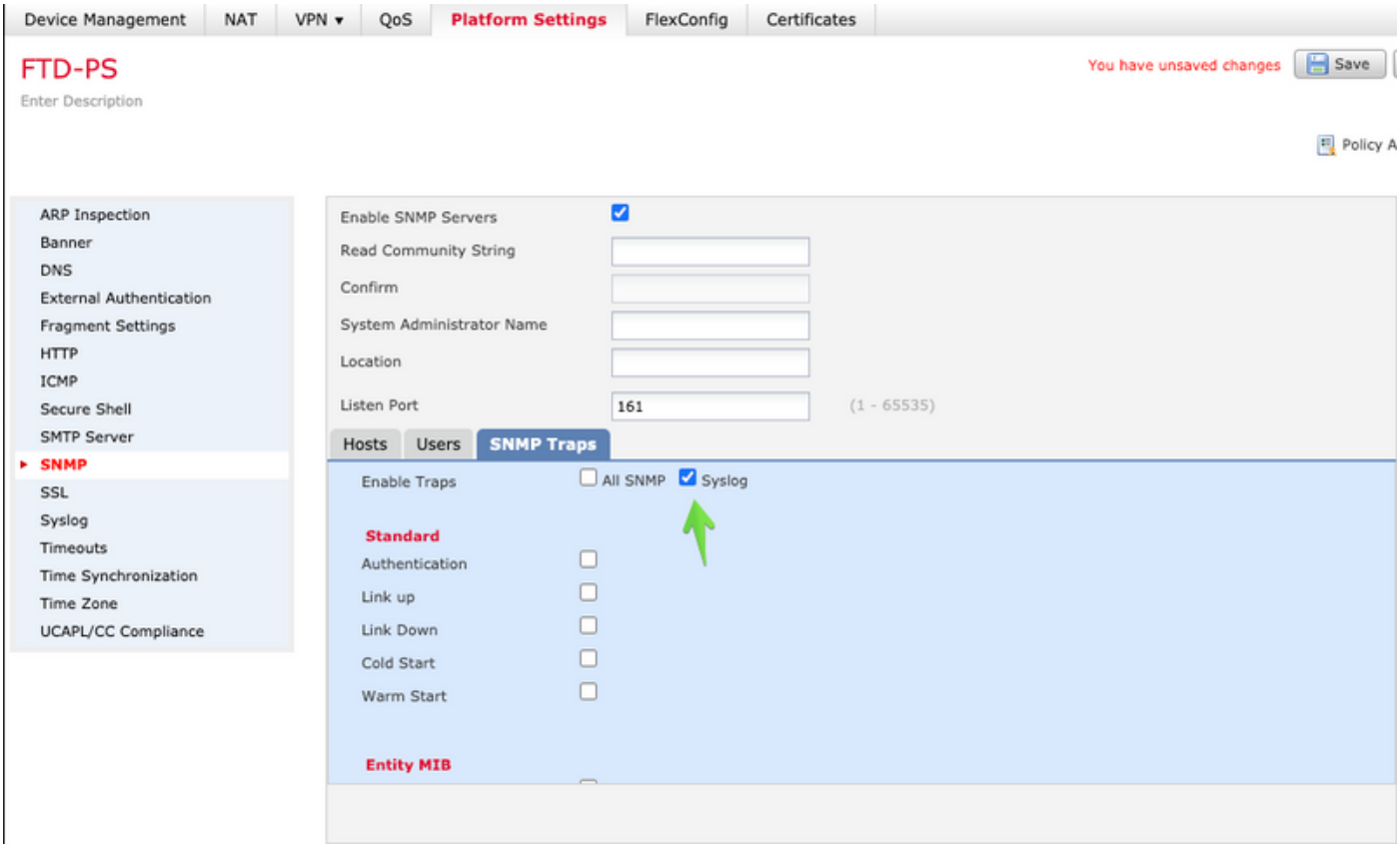
الخطوة 3. حدد علامة التبويب **مستخدمون** وحدد الزر **إضافة**. املأ معلومات المستخدم.



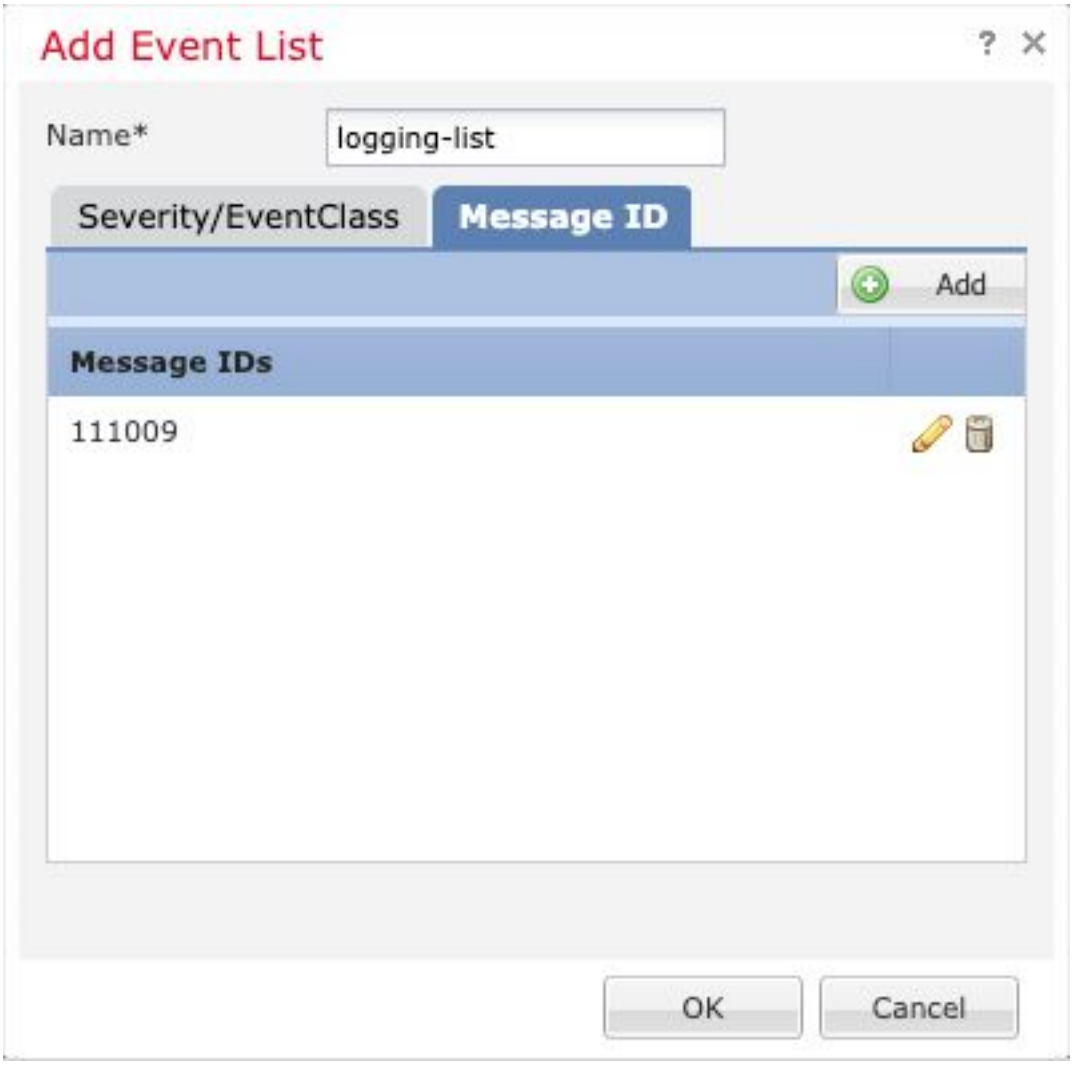
الخطوة 4. حدد **إضافة** في علامة التبويب **البيانات المضيفة**. قم بتعبئة المعلومات المتعلقة بخادم SNMP. إذا كنت تستخدم واجهة بدلا من منطقة، فتأكد من إضافة اسم الواجهة يدويا في قسم الركن الأيمن. حدد "موافق" بمجرد تضمين جميع المعلومات الضرورية.



الخطوة 5. حدد علامة التبويب **مدائمات SNMP** وحدد مربع **syslog**. تأكد من إزالة جميع علامات إختيار المدائمات الأخرى إذا لم تكن مطلوبة.



الخطوة 6. انتقل إلى **syslog** وحدد علامة التبويب **قوائم الأحداث**. حدد الزر **إضافة**. قم بإضافة اسم والرسائل التي سيتم تضمينها في القائمة. حدد **موافق** للمتابعة.

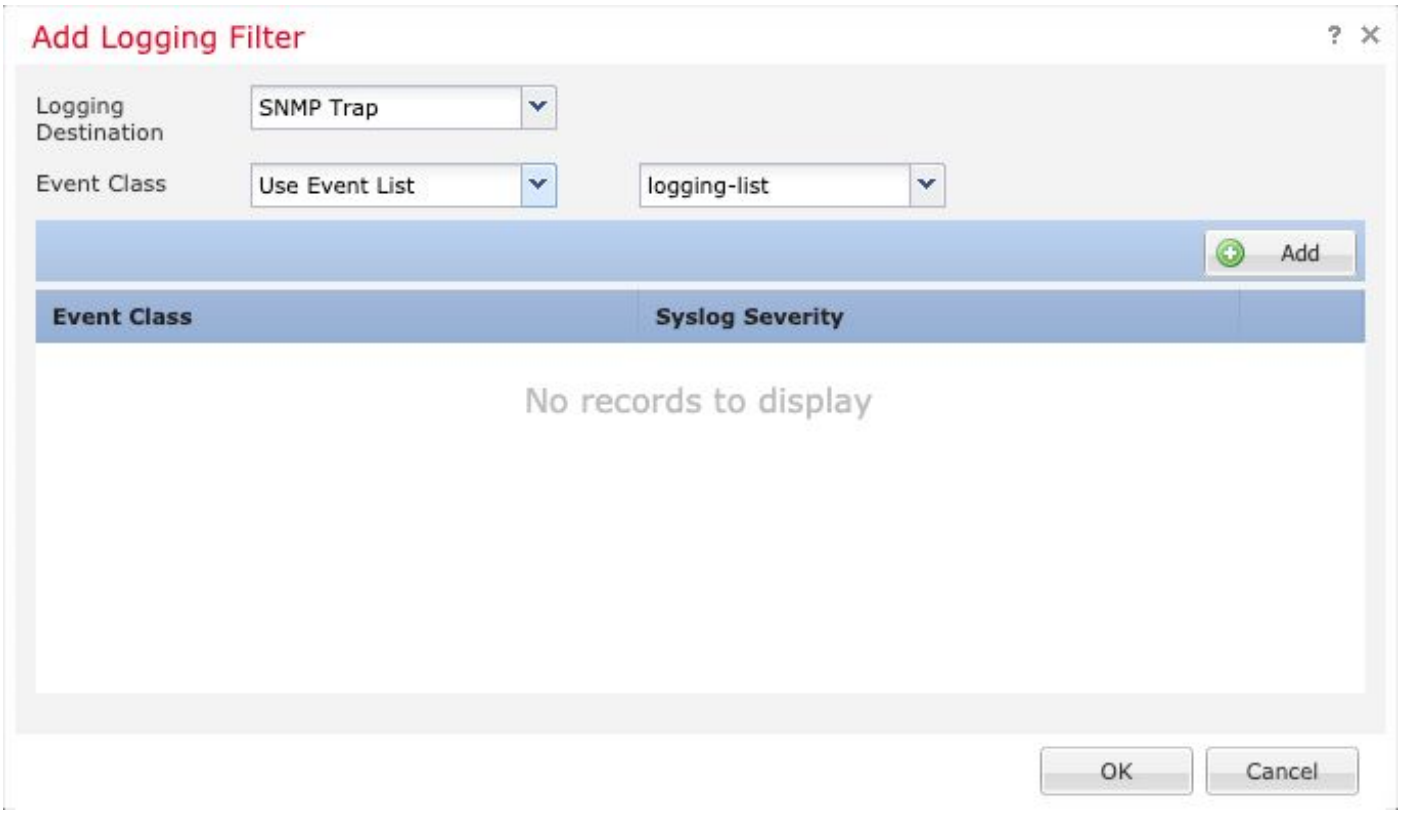


الخطوة 7. حدد علامة التبويب **وجهات التسجيل** وحدد الزر **إضافة**.

تغيير وجهة التسجيل إلى **مكالمة SNMP**.

حدد **قائمة أحداث المستخدم** واختر قائمة الأحداث التي تم إنشاؤها في الخطوة 6 المجاورة لها.

حدد **موافق** لإنهاء تحرير هذا المقطع.



الخطوة 8. حدد الزر **حفظ ونشر** التغييرات على الجهاز الذي تمت إدارته.

التحقق من الصحة

يمكن إستخدام الأوامر أدناه في كل من FTD CLISH و ASA CLI.

إظهار إحصائيات خادم SNMP

يوفر الأمر **"show snmp-server statistics"** معلومات حول عدد المرات التي تم فيها إرسال خ. يمكن أن يتضمن هذا العداد مكالمات أخرى.

```
# 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
```

يشغل معرف الرسالة المستخدم في هذا المثال لكل مرة يقوم فيها المستخدم بتنفيذ أمر. في كل مرة يتم إصدار أمر "show"، تتم زيادة العداد.

إظهار إعداد التسجيل

يوفر "show logging setting" معلومات حول الرسائل التي يتم إرسالها بواسطة كل وجهة. يشير تسجيل المحفوظات إلى عدادات إخبارات SNMP. ترتبط إحصائيات تسجيل المذاكرة بعدادات مضيفات 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
```

قم بإصدار الأمر "show logging queue" لضمان عدم إسقاط أية رسائل.

```
# 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
```

معلومات ذات صلة

- رسائل Cisco ASA Series Syslog
- CLI Book 1: دليل تكوين واجهة سطر الأوامر لعمليات Cisco ASA Series العامة، 9.12
- تكوين SNMP على أجهزة FirePOWER NGFW

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).