تكوين تكامل آمن لحدث FTD من خلال التحكم في سحابة الأمان عبر موصل حدث آمن

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين Cisco Secure FTD لإرسال أحداث الأمان إلى "التحكم في سحابة الأمان" (SCC) باستخدام "موصل حدث الأمان" (SEC).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- الدفاع الآمن عن تهديد جدار الحماية (FTD) من Cisco
- واجهة سطر أوامر Linux (CLI)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

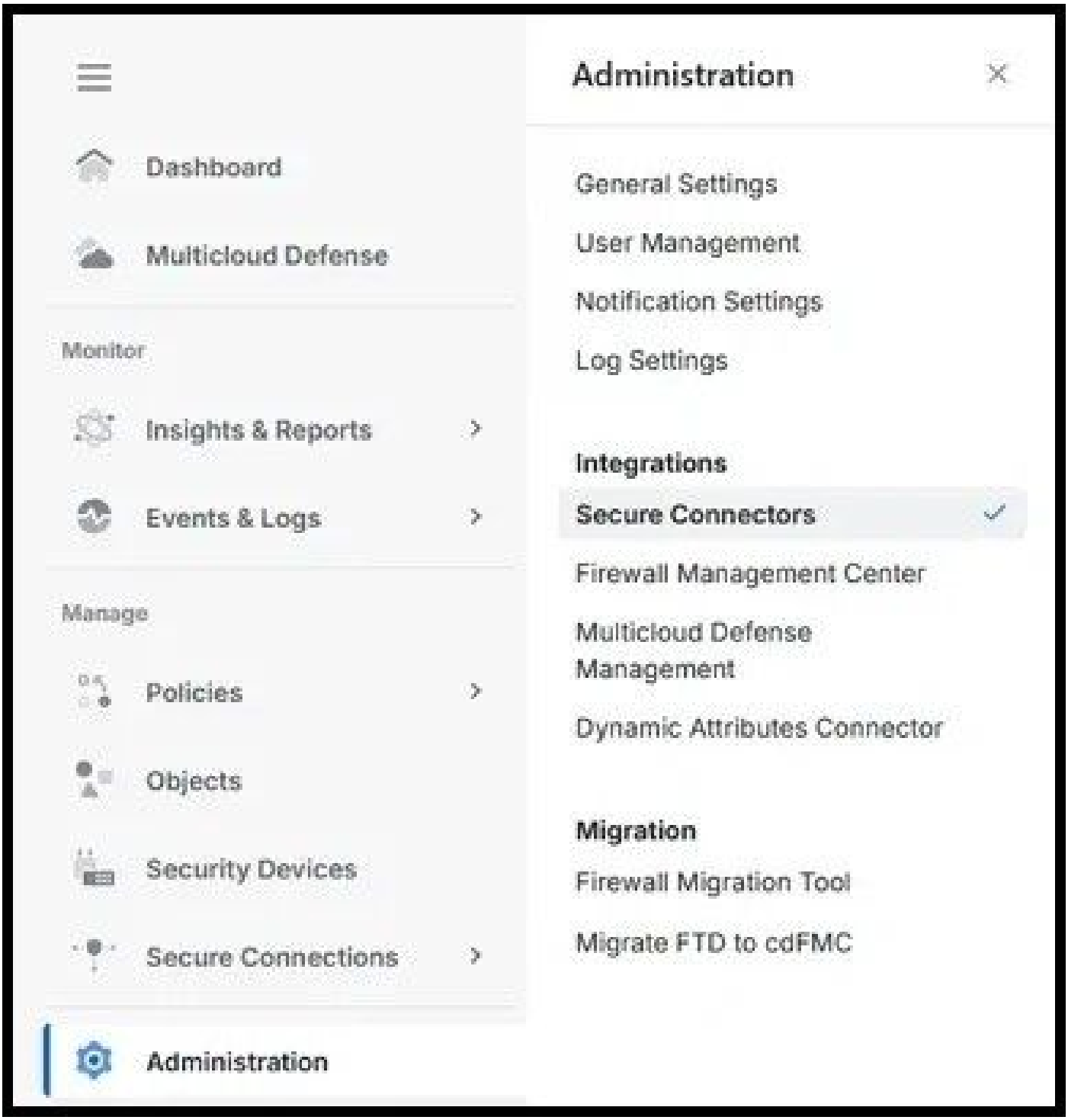
- Cisco Secure FTD، الإصدار 7.6
- Ubuntu لدان لصيغة 24.04

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.

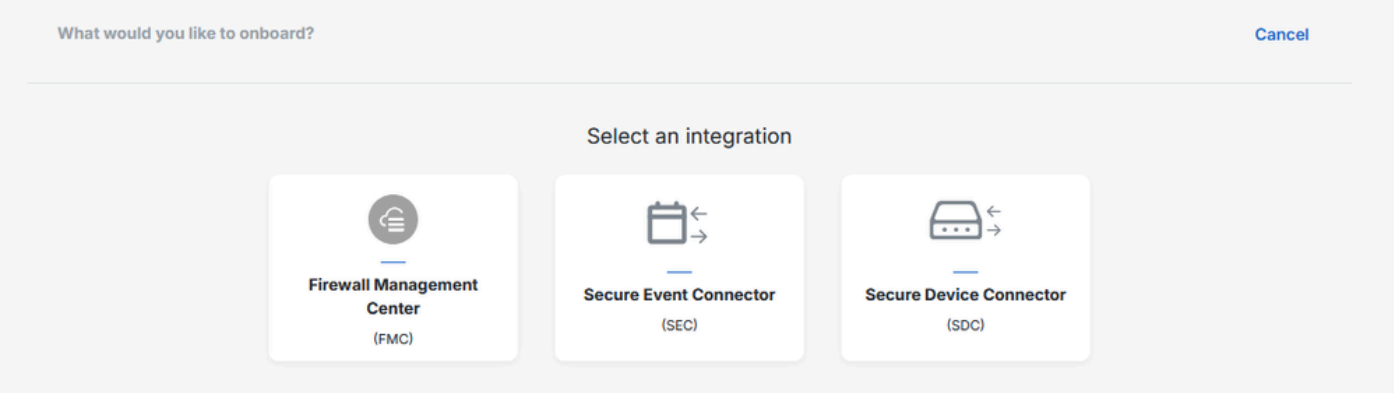
التكوين

الخطوة 1. تسجيل الدخول إلى بوابة مجموعة SCC:

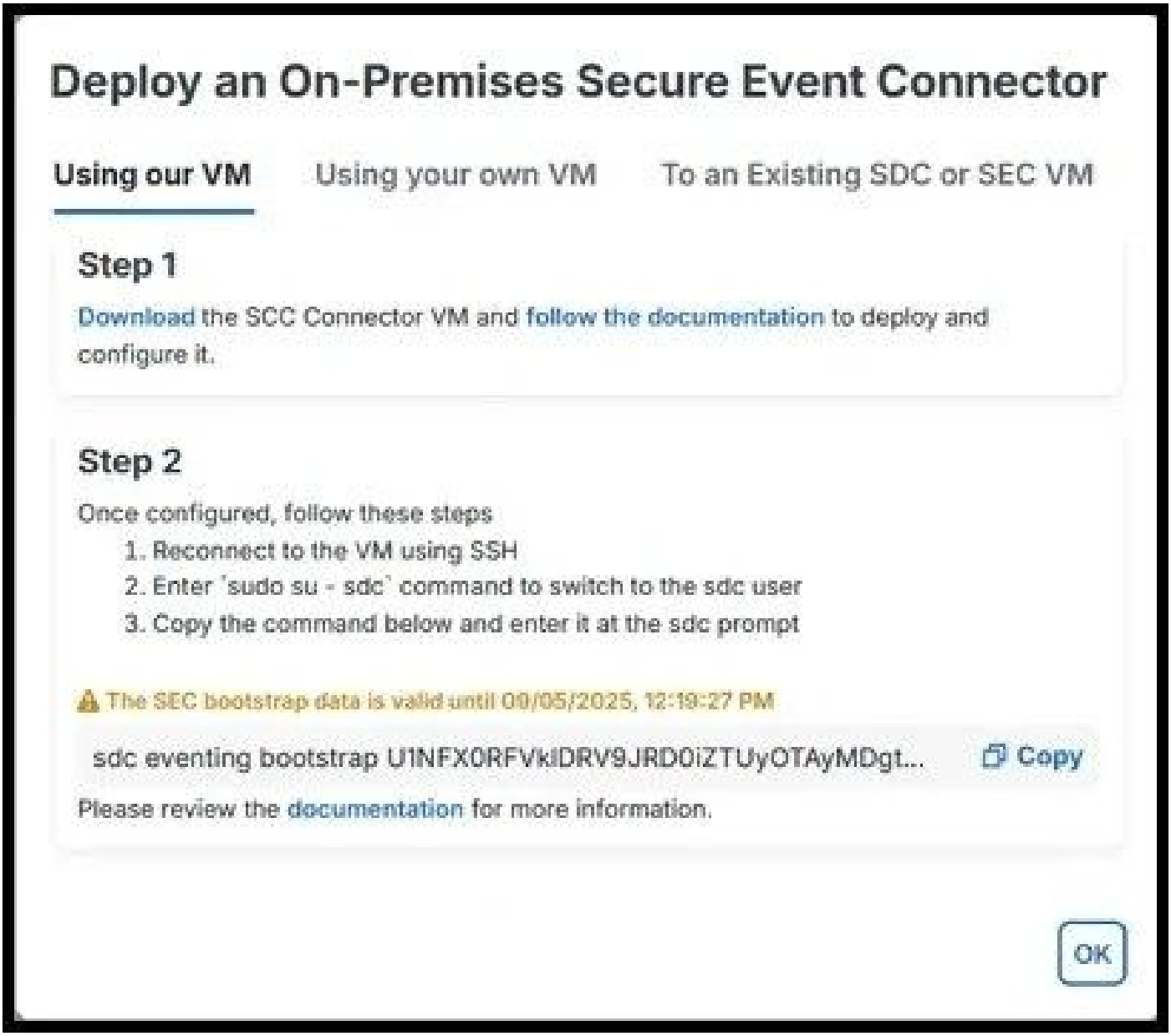
الخطوة 2. من قائمة الجانب الأيسر، أختر الإدارة والموصلات الآمنة:



الخطوة 3. على الجانب الأيمن العلوي، انقر فوق رمز زائد لضم موصل جديد واختر موصل حدث آمن:



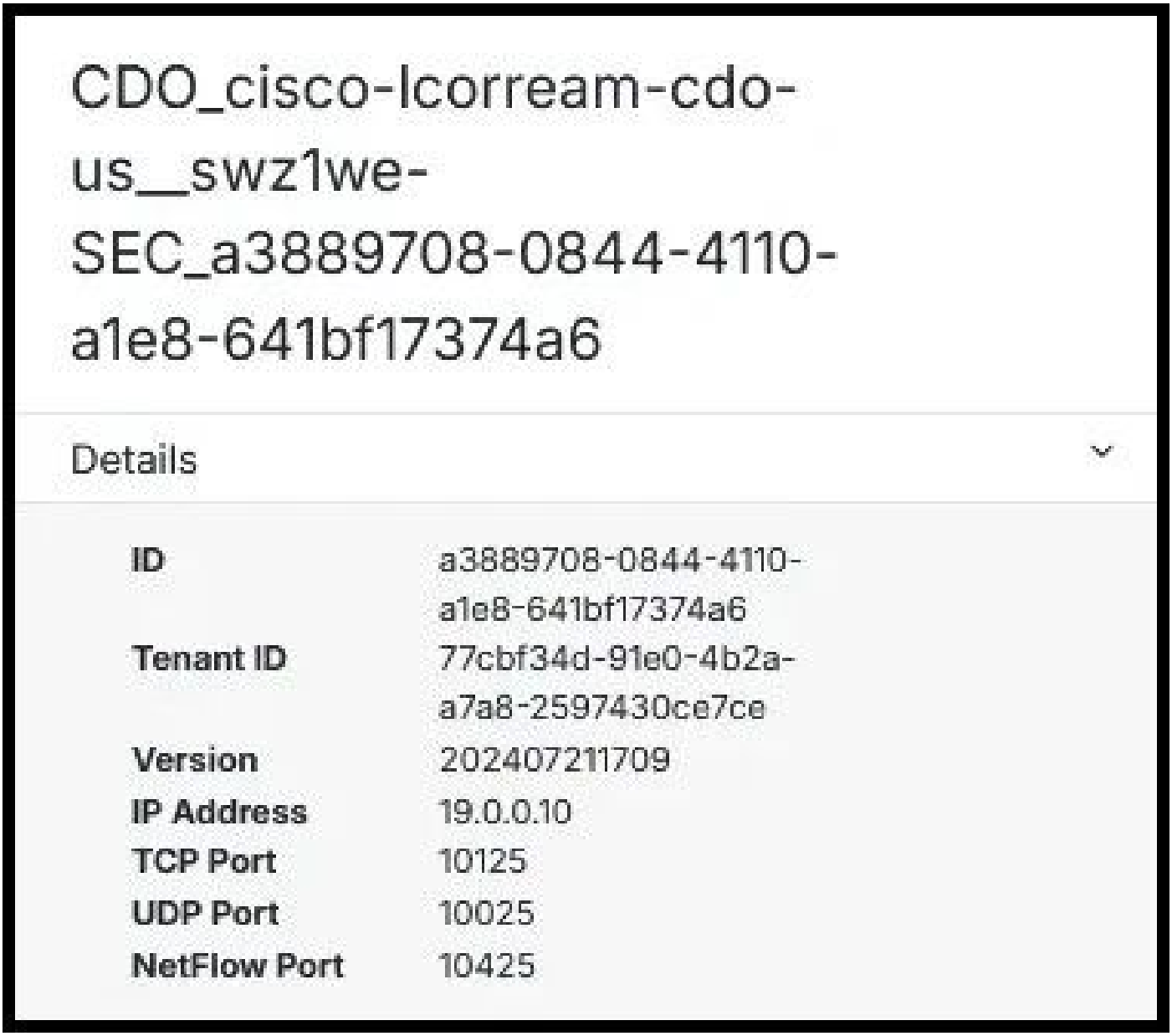
الخطوة 4. أستخدم الخطوات لتثبيت الموصل وتمهيد تشغيله استنادا إلى الخيار المطلوب بين "إستخدام الجهاز الظاهري (VM) الخاص بك" أو "إلى SDC أو SEC VM موجود":



الخطوة 5. تظهر رسالة مماثلة عندما يتم تنفيذ بروتوكول نظام تمهيد تشغيل الكمبيوتر بنجاح:

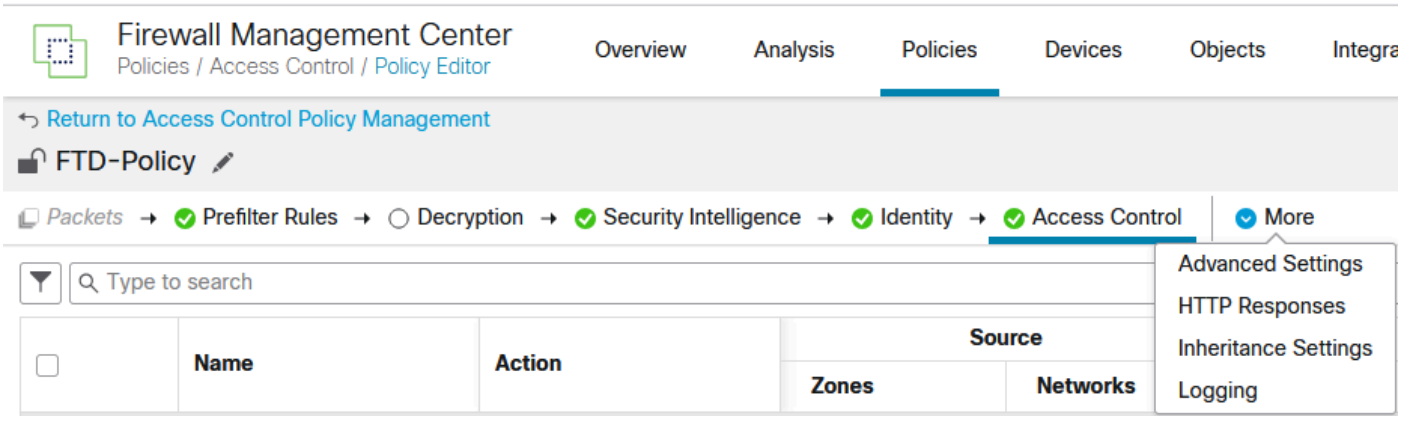
```
2025-06-09 05:41:56 [INFO] Bootstrap package processed successfully
2025-06-09 05:41:56 [INFO] Default AWS Region is us-west-2
2025-06-09 05:42:00 [INFO] Scanning for next available TCP port starting with 10125
2025-06-09 05:42:00 [INFO] TCP port found and set to 10125
2025-06-09 05:42:00 [INFO] Scanning for next available UDP port starting with 10025
2025-06-09 05:42:00 [INFO] UDP port found and set to 10025
2025-06-09 05:42:00 [INFO] Scanning for next available Netflow port starting with 10425
2025-06-09 05:42:00 [INFO] Netflow port found and set to 10425

WARNING! Your credentials are stored unencrypted in '/var/lib/sdc/.docker/config.json'.
Configure a credential helper to remove this warning. See
https://docs.docker.com/go/credential-store/

5a99d0351c1ae91cd790dcf18ee1d0594d37fcfaf5a1725473eeed042342a567
2025-06-09 05:42:06 [INFO] The SEC is up and running - You should be all set to go
2025-06-09 05:42:08 [INFO] Your SEC has been successfully bootstrapped! Please verify that everything is working within
the SCC UI, and thank you for being a customer
sdc@lcorream-sdc:~$
```

الخطوة 6. بمجرد نشر الموصل وتجهيزه، تظهر معلومات المنفذ في مدخل SCC:

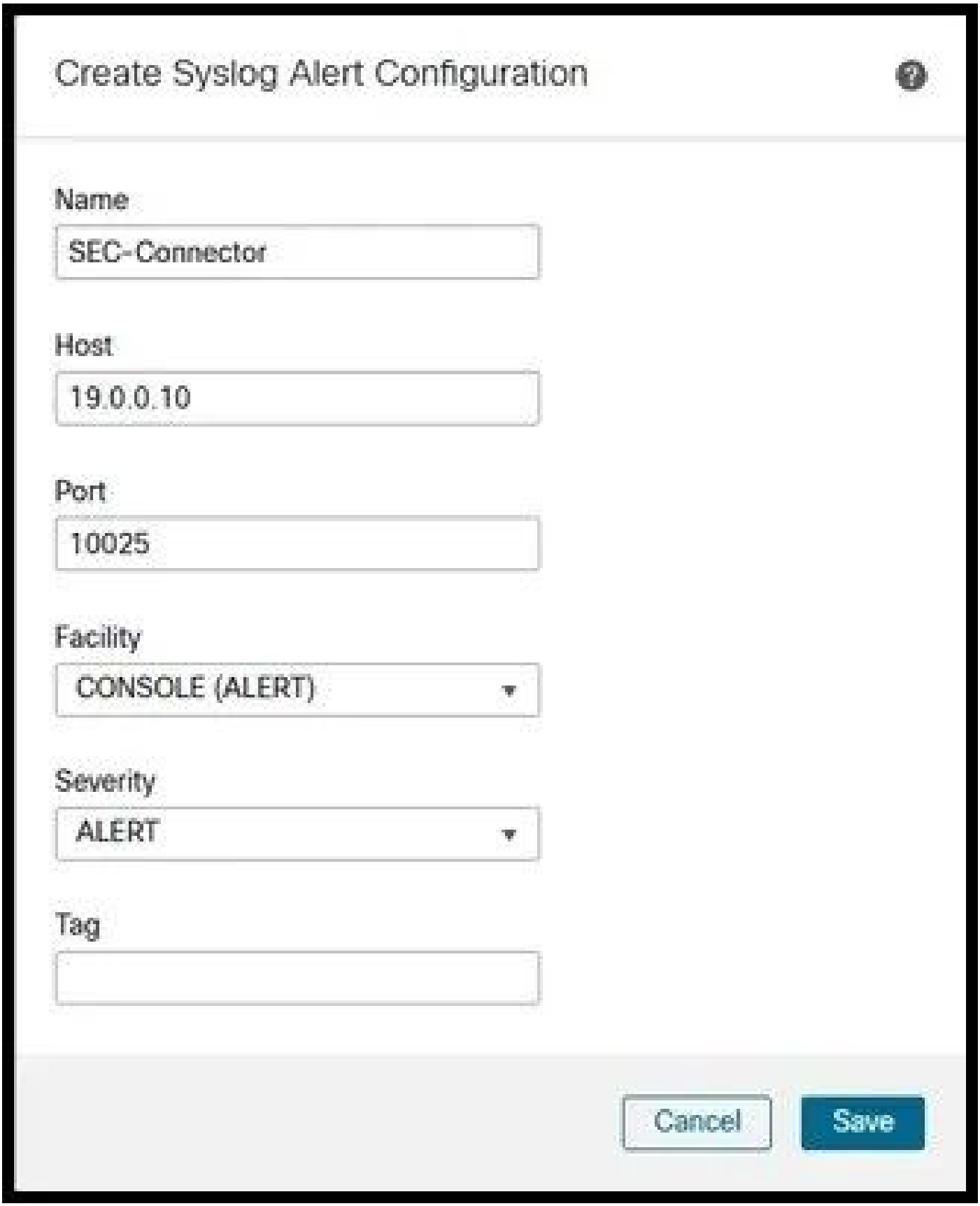


الخطوة 7. في مركز إدارة جدار الحماية الآمن (FMC) من Cisco، انتقل إلى السياسات ثم إلى التحكم في الوصول. أختر النهج المتوافق مع الجهاز (الأجهزة) الذي يتم تحميله.

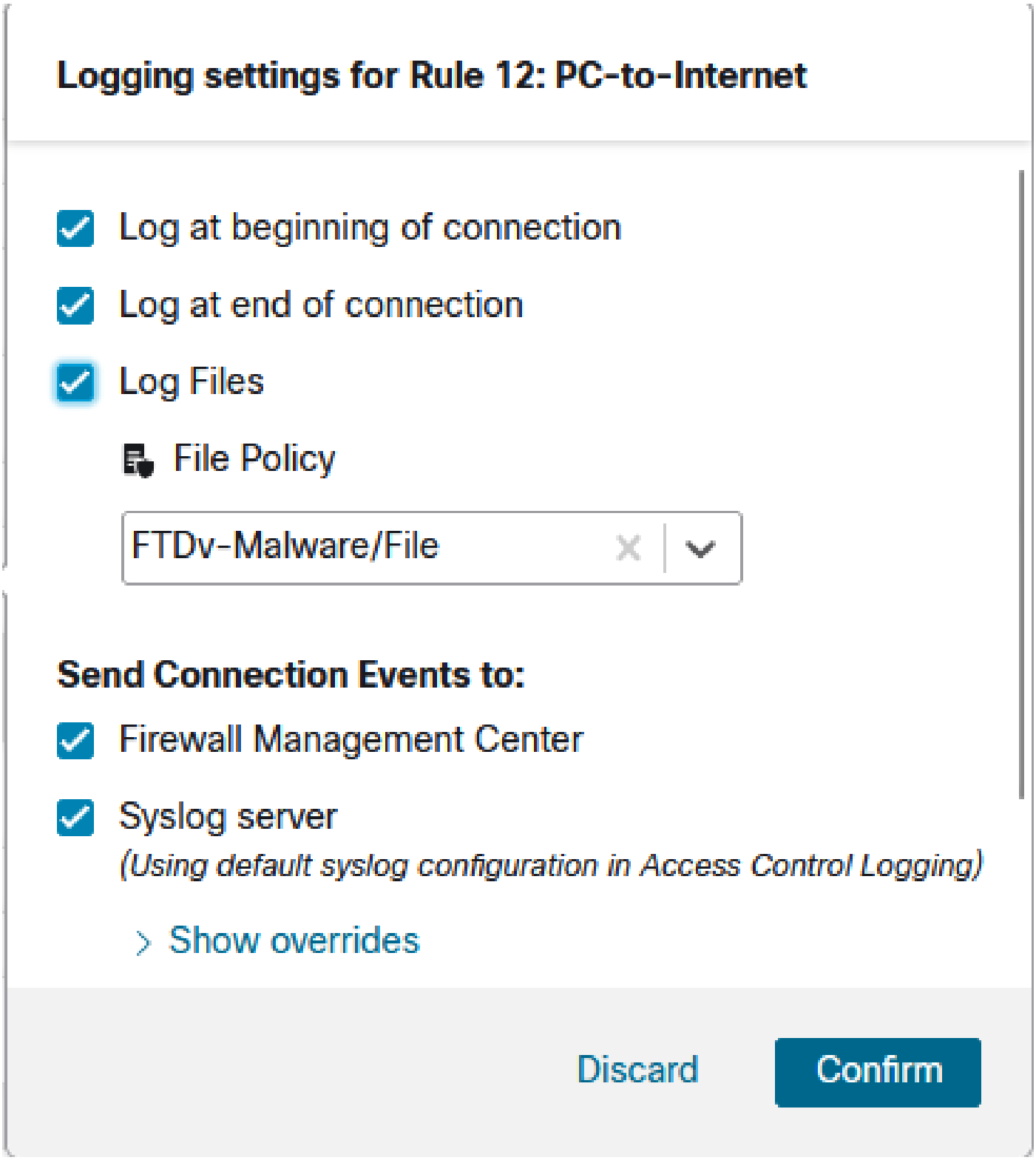
الخطوة 8. أختر المزيد ثم التسجيل:



الخطوة 9. قم بتمكين الإرسال باستخدام خيار تنبيه syslog محدد وأضفت تنبيه syslog جديد. أستخدم عنوان بروتوكول الإنترنت (IP) ومعلومات المنفذ التي تم الحصول عليها من موصل SEC في مدخل SCC:



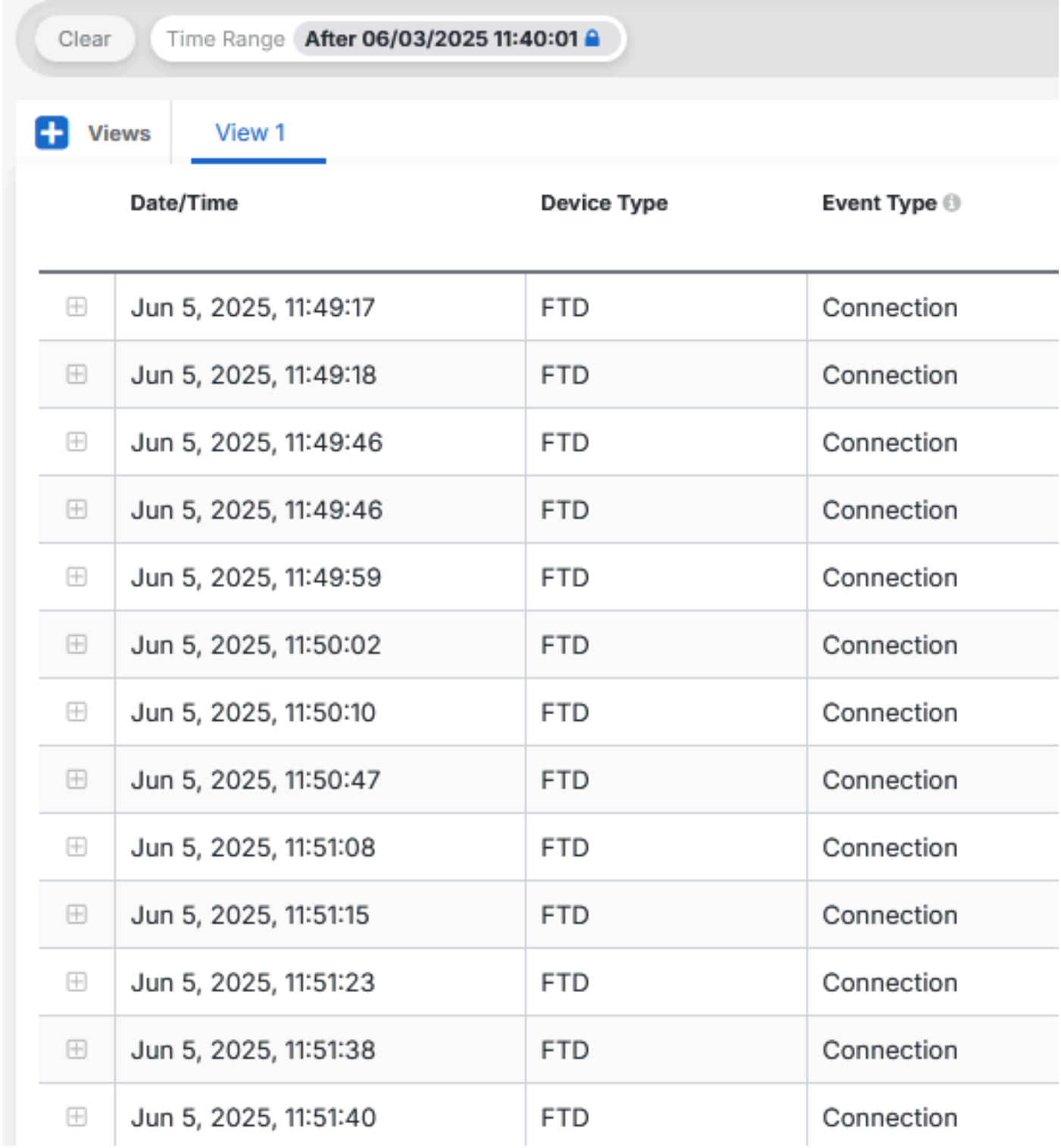
الخطوة 10. العودة إلى نهج التحكم في الوصول، قم بتعديل القواعد الفردية لإرسال الأحداث إلى خادم syslog:



الخطوة 11. قم بنشر التغييرات التي تم إجراؤها على FTD للسماح لجدار الحماية ببدء تسجيل الأحداث.

التحقق من الصحة

للتحقق من تنفيذ التغييرات بنجاح وإجراء تسجيل الأحداث، انتقل إلى الأحداث والسجلات وتسجيل الأحداث في بوابة SCC وتأكد من رؤية الأحداث:



استكشاف الأخطاء وإصلاحها

في FTD، قم بتشغيل التقاط حزمة على الجهاز باستخدام واجهة الإدارة التي تطابق حركة مرور البيانات التي تنتقل إلى SEC من أجل التقاط حركة مرور syslog:

```
> capture-traffic

Please choose domain to capture traffic from:
  0 - eth0
```

```
  1 - Global

Selection? 0

Warning: Blanket capture may cause high CPU usage and reduced throughput, use selective filtering to re
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: host 19.0.0.10 port 10025
Starting traffic capture, press ctrl + c to exit (Maximum 1,000,000 packets will be captured)
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: can't parse filter expression: syntax error
Exiting.

> capture-traffic

Please choose domain to capture traffic from:
  0 - eth0
  1 - Global

Selection? 0

Warning: Blanket capture may cause high CPU usage and reduced throughput, use selective filtering to re
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: host 19.0.0.10 and port 10025
Starting traffic capture, press ctrl + c to exit (Maximum 1,000,000 packets will be captured)
HS_PACKET_BUFFER_SIZE is set to 4.
10:43:00.191655 IP firepower.56533 > 19.0.0.10.10025: UDP, length 876
10:43:01.195318 IP firepower.56533 > 19.0.0.10.10025: UDP, length 1192
10:43:03.206738 IP firepower.56533 > 19.0.0.10.10025: UDP, length 809
10:43:08.242948 IP firepower.56533 > 19.0.0.10.10025: UDP, length 1170
```

من الجهاز الظاهري ل SEC، تأكد من توفر اتصال بالإنترنت على الجهاز الظاهري. قم بتشغيل الأمر sdc troubleshooting، إنشاء حزمة أستكشاف الأخطاء وإصلاحها يمكن إستخدامها للتحقق من ملف lar.log للحصول على مزيد من التشخيص.

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).