نشر وحدة التحكم في إدارة اللوحة الأساسية (FMC) التي يتم تسليمها عبر السحابة في Cisco Defense Orchestrator (CDO)

المحتويات

المقدمة

يصف هذا المستند عميلة النشر والعملية المدمجة لوحدة التحكم في إدارة اللوحة الأساسية (FMC) التي يتم تسليمها عبر الشبكة السحابية على النظام الأساسي لـ CDO.

المتطلبات الأساسية

المتطلبات

توصي Cisco بمعرفة المواضيع التالية:

- مركز إدارة FirePOWER (CDfmc) الذي يتم توفيره عبر السحابة
- Cisco Defense Orchestrator (CDO)
- الدفاع الظاهري ضد تهديد Firepower (FTDv)

الحد الأدنى لإصدار FTD 7.0.3

المكونات المستخدمة

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

- cdFMC
- FTDv 7.2.0

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة.

بأدب جميع الأجهزة المُستخدمة في هذا المستند بتكوين مجمع (افتراضي). اذا كانت
شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

الذي (CDfmc) مركز إدارة جدار الحماية (CDO) هو النظام الأساسي لمركز إدارة جدار الحماية Cisco Defense Orchestrator (CDO)
يتم تسليمه عبر السحابة. يُعد مركز إدارة جدار الحماية الذي تم تسليمه عبر السحابة. يتم تسليمه عبر أحد
منتجات البرامج كخدمة (SAAs) التي تقوم بإدارة أجهزة ضد دفاع الآمن من
فهو يوفر العديد من الوظائف نفسها التي يوفرها برنامج دفاع الآمن عن جدار جديد
الحماية (Secure Firewall) ويستيتم بنفس مظهر وسلوك مركز إدارة جدار الحماية الآمن
المحلي FMC (API). تطبيقات تجمة برمجة واجهة نفس سلوك مستخدم ويحلي
المحلي.

تم تصميم هذا المنتج للترحيل من مراكز إدارة جدار الحماية الآمن المحلية إلى إصدار SAAs
لمركز إدارة جدار الحماية الآمن.

التكوين

نشر مركز إدارة FirePOWER الذي توفره الشبكة السحابية على CDO.

تظهر هذه الصور عملية الإعداد الأولية واللازمة لنشر وحدة تحكم في مركز إدارة الأساسية (FMC)
تم تسليمها عبر السحابة على CDO.

من قائمة CDO، انتقل إلى **Tools & Services > Firewall Management Center > Onboard**.
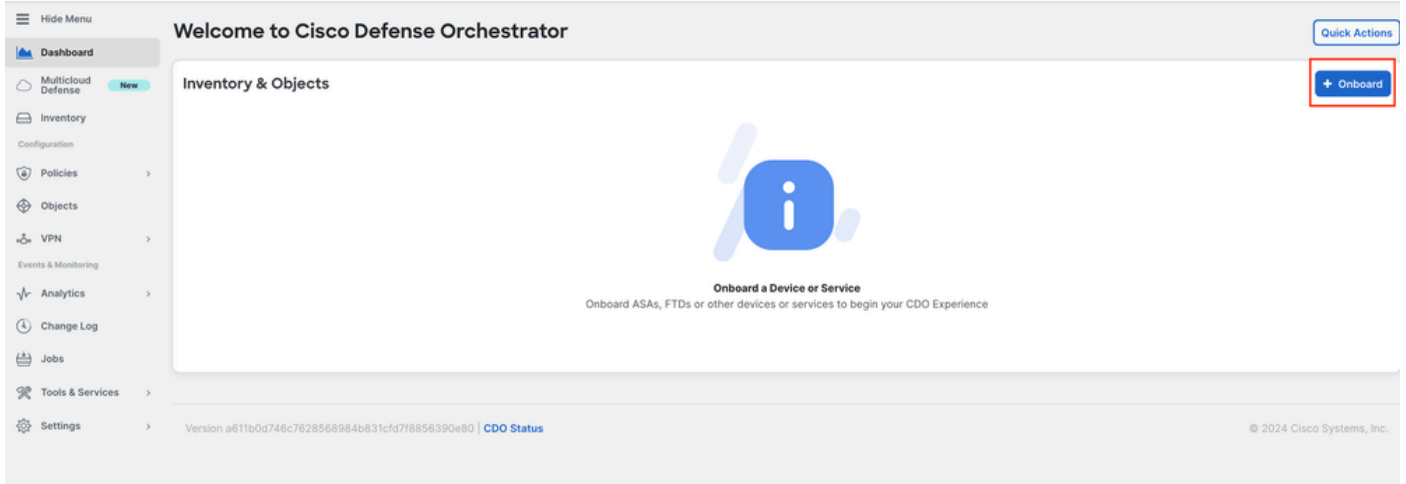
تحديد Enable Cloud-Delivered FMC.

تخمن CDO مثيل مركز إدارة جدار الحماية الذي تم تسليمه عبر السحابة في الخلفية، وعادة ما يستغرق ذلك من 15 إلى 30 دقيقة حتى يكتمل. يمكنك تعقب تقدم الإعداد على عمود الحالة الخاص ب FMC التي تم تسليمها عبر السحابة.

بعد اكتمال التوفير، تتغير الحالة إلى Active. وبالإضافة إلى ذلك، يمكنك الوصول على إعلام من جهاز مركز إدارة جدار الحماية الذي تم تسليمه عبر السحابة على لوحة إعلامات CDO.
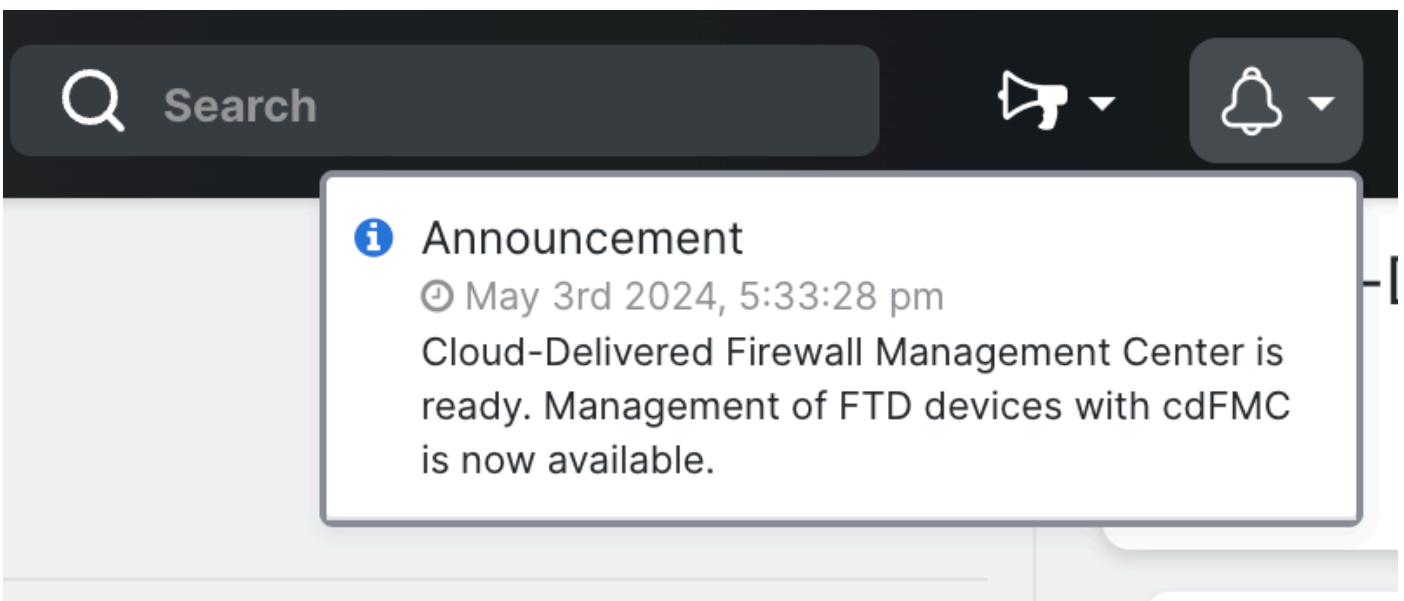
.اهترادإو ةكبشلا يذلا ةيامحلا رادج ةرادإ زكرم ىلإ ديدهتلا نع عافدلا ةزهجأ ليمحت ذئدنع كنكمي

لقتنا ىلإ **Menu > Tools & Services > Firewall Management Center**.
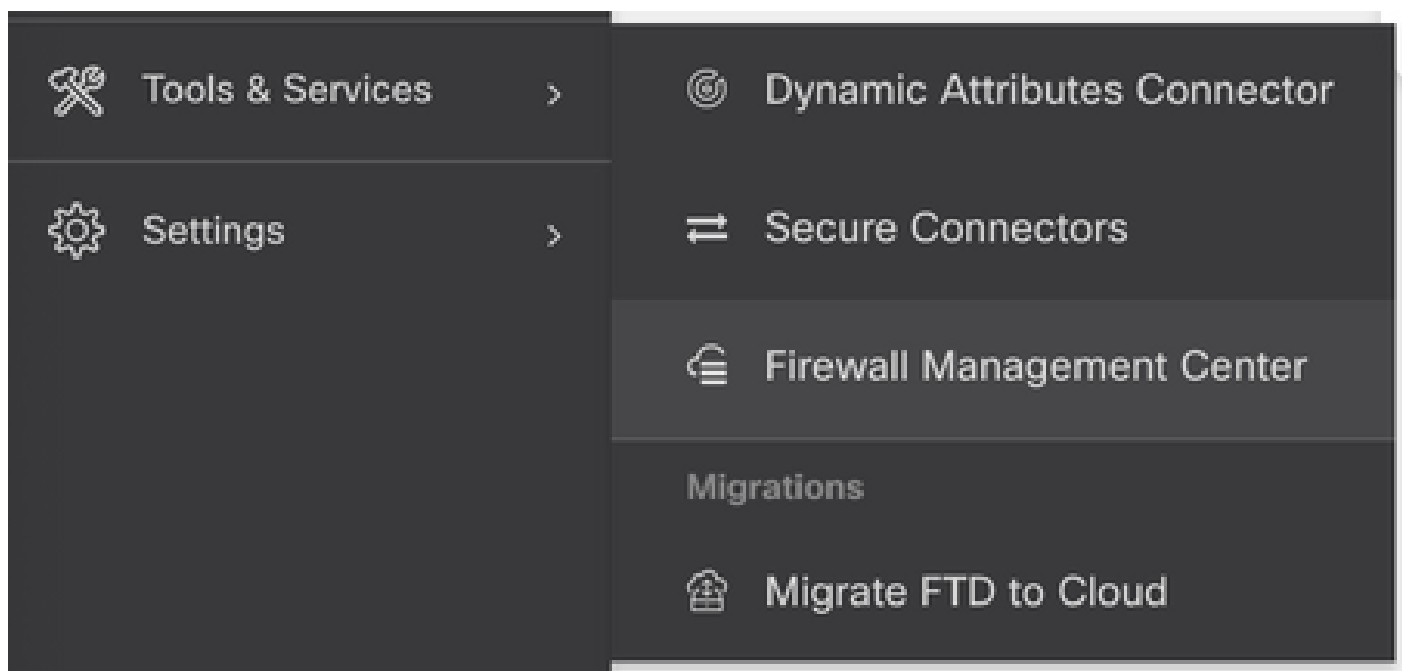
ةصاخلا (GUI) ةيموسرلا مدختسملا ةهجاو ىلإ لوصوللو CDfmc ،CDfmc ةناوطسألا تامولعم ضرعل CDfmc ةناوطسألا ددح
.نميألا بناجلا ىلع ةحاتملا تارايخلا نم يأ ددح ،FMC ةناوطسألاب

يمكنك الآن مشاهدة واجهة مستخدم (GUI) لوحدة التحكم الخاصة بـ CDfmc. وجهة المستخدم الرسومية (GUI) لوحدة التحكم

على اللوحة FTD على FMC يتم تسليمها عبر السحابة

تظهر هذه الصور كيفية تركيب FTD حتى يتم تسجيله على قرص cdFMC باستخدام مفتاح تسجيل واجهة سطر الأوامر (CLI).

أولاً، حدد Onboard an FTD في الصفحة الرئيسية لـ CDO.

ثم حدد الخيار **Use CLI Registration Key**.

قم بالمتابعة لإدخال معلومات FTDv المطلوبة.

وأخيرًا، تقوم وحدة التحكم في إدارة إدارة السحابة النمطية CDfmc بإنشاء **CLI Key** وحدة خاصة بالجهاز.

انسخ **CLI Key** إلى CLI من جهاز كمازك المدار.

يقوم القرص المضغوط بالضغط عدب FMC مهمة تسجيل.

✎ **ملاحظة:** تأكد من أن جهاز FTD لديه اتصال عبر المنافذ 8305 (SFTUNNEL) و 443 المستأجر من CDO لأجل إكمال عملية التسجيل. راجع [متطلبات الشبكة](#) بالكامل.

✎ **ملاحظة:** إذا تعذر عليك الاتصال بالمضيف، فيمكنك تصحيح تكوين DNS في FTD-CLI باستخدام هذا الأمر: **تكوين** DNS **<address>** للشبكة.

للمراقبة عملية التسجيل، انتقل إلى **Device Actions > Workflows.**.

قم بتوسيع الحالة **Active** للوصول إلى معلومات إضافية، تظهر هذه الصور كيفية تسجيل FTDv بنجاح.

أخيراً، انتقل إلى **Device Overview** > **Device Management** للوصول إلى cdFMC ومراجعة حالة نظرة عامة على FTDv.

معلومات ذات صلة

- [**الدعم التقني والمستندات - Cisco Systems**](#)

- [إدارة أجهزة الدفاع عن تهديد جدار الحماية الآمن من Cisco باستخدام مركز إدارة جدار الحماية الذي يتم تشغيله عبر السحابة](#)

حول هذه الترجمة

ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية
والبشرية لتقديم 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 مسؤوليتها عن دقة هذه الترجمات وتوصي بالرجوع دائمًا إلى
المستند الإنجليزي الأصلي (الرابط متوفر).