تكوين سجل النظام على سلسلة موجهات RV325 VPN و RV320

الهدف

سجلات النظام هي سجلات لأحداث الشبكة. السجلات هي أداة مهمة يتم إستخدامها لفهم كيفية عمل الشبكة. حيث أنها مفيدة لإدارة الشبكة واستكشاف أخطاء الشبكة وإصلاحها.

تشرح هذه المقالة كيفية تكوين أنواع السجالت المراد تسجيلها، وكيفية عرض السجالت على سلسلة موجه VPN RV32x، وكيفية إرسال السجالت إلى المستلم عبر SMS، أو إلى خادم سجل النظام، أو إلى مستلم عبر البريد الإلكتروني.

الأجهزة القابلة للتطبيق

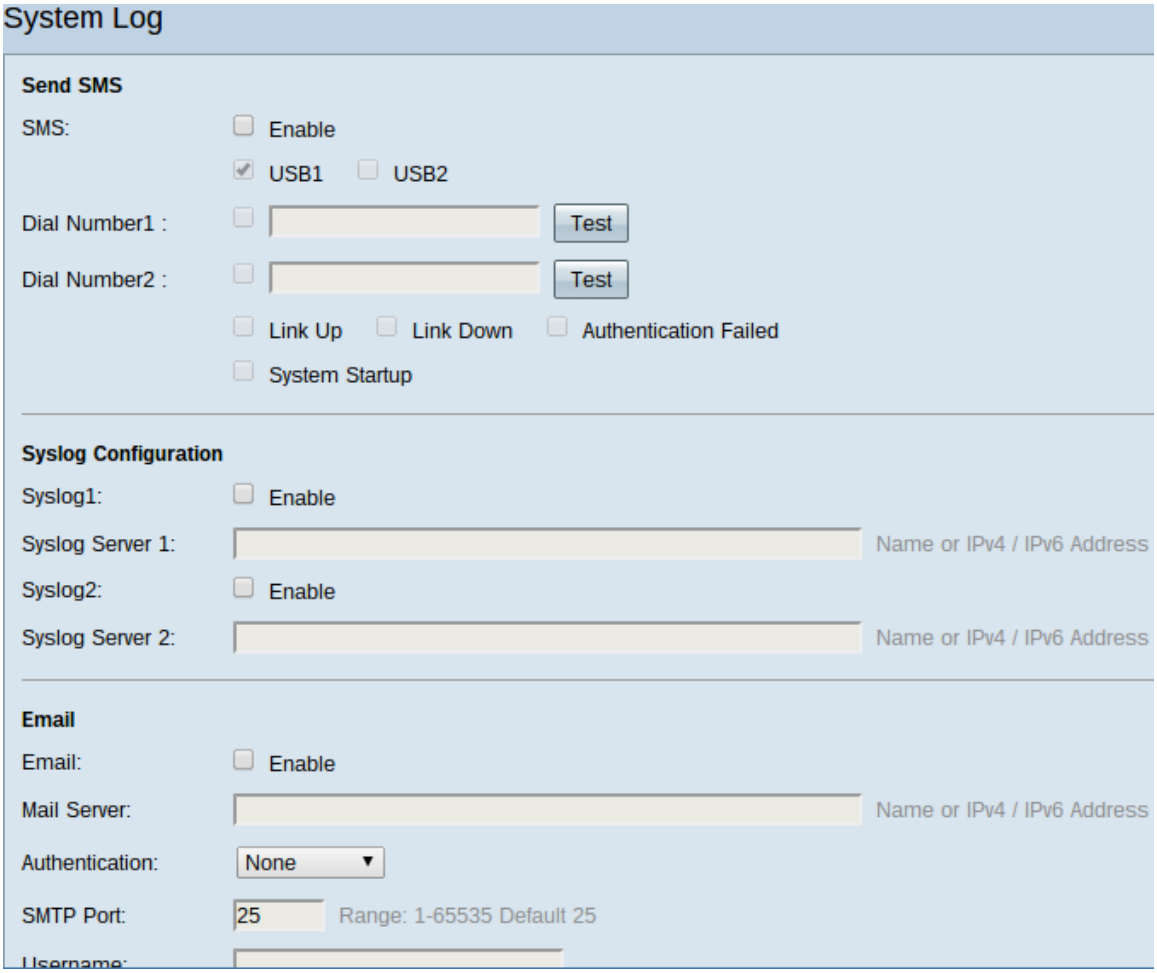
·موجه VPN RV320 بشبكة WAN مزدوجة
· الموجه RV325 Gigabit WAN VPN Router

إصدار البرامج

·v1.1.0.09

تكوين سجل النظام

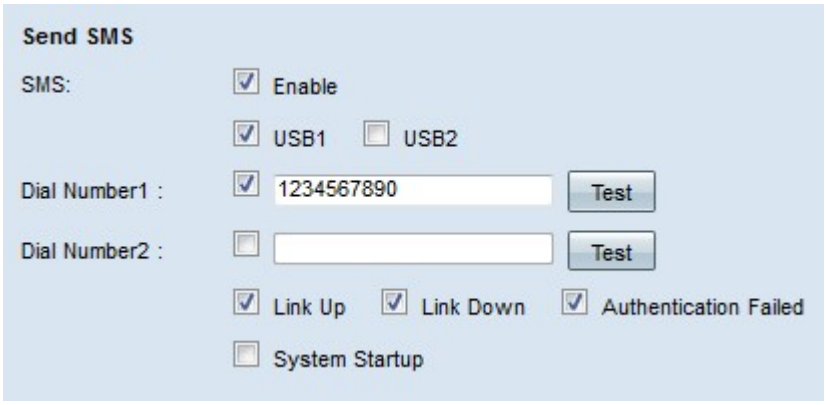
الخطوة 1. قم بتسجيل الدخول إلى الأداة المساعدة لتكوين الويب واختر **تسجيل الدخول > سجل النظام**. تظهر صفحة *سجل النظام*:



راجع الأقسام التالية للحصول على معلومات حول صفحة *سجل النظام*.

- [سجلات النظام بواسطة SMS](#) — كيفية إرسال سجلات النظام إلى هاتف عبر SMS.
- [سجلات النظام على خوادم سجل النظام](#) — كيفية إرسال سجلات النظام إلى خادم سجل النظام.
- [إرسال سجلات النظام بالبريد الإلكتروني](#) — كيفية إرسال سجلات النظام إلى عنوان بريد إلكتروني.
- [إعدادات السجل](#) — كيفية تكوين نوع الرسائل التي يتم حفظها في السجل.
- [عرض سجل النظام](#) — كيفية عرض سجلات النظام على الجهاز.
- [عرض جدول السجل الصادر](#) — كيفية عرض سجلات النظام التي ترتبط فقط بالحزم الصادرة.
- [عرض جدول السجلات الواردة](#) — كيفية عرض سجلات النظام التي تتعلق فقط بالحزم الواردة.

سجلات النظام بواسطة SMS



الخطوة 1. تحقق من **تمكين** في حقل SMS لإرسال سجلات النظام إلى عميل من خلال رسائل خدمة الرسائل القصيرة (SMS).

الخطوة 2. حدد خانات الاختيار الخاصة بمنافذ USB التي يتصل بها مودم USB من الجيل الثالث.

الخطوة 3. حدد خانة الاختيار في حقل "رقم الطلب 1" وأدخل رقم الهاتف الذي يتم إرسال الرسائل إليه.

ملاحظة: انقر على **اختبار** لاختبار الاتصال بالطلب رقم 1. إذا لم يستلم الرقم الذي تم تكوينه رسالة الاختبار، فتأكد من إدخال رقم الهاتف بشكل صحيح في حقل "رقم الطلب 1".

الخطوة 4. (إختياري) حدد خانة الاختيار في حقل "رقم الطلب 2" وأدخل رقم الهاتف الذي يتم إرسال الرسائل إليه.

ملاحظة: انقر على **اختبار** لاختبار الاتصال بالطلب رقم 2. إذا لم يستلم الرقم الذي تم تكوينه رسالة الاختبار، فتأكد من إدخال رقم الهاتف بشكل صحيح في حقل "رقم الطلب 2".

الخطوة 5. حدد خانات الاختيار الخاصة بالأحداث التي ستؤدي إلى تشغيل سجل ليتم إرساله.

·الارتباط — تم إنشاء اتصال ب RV320.

·الارتباط معطل — تم قطع الاتصال ب RV320.

·فشلت المصادقة — فشلت المصادقة.

·بدء تشغيل النظام — تم تمهيد الموجه.

الخطوة 6. طقطقة **حفظ**. تم تكوين سجلات النظام عبر SMS.

سجلات النظام على خوادم سجل النظام

الخطوة 1. تحقق من **تمكين** في حقل syslog1 لإرسال سجلات النظام إلى خادم سجل النظام.

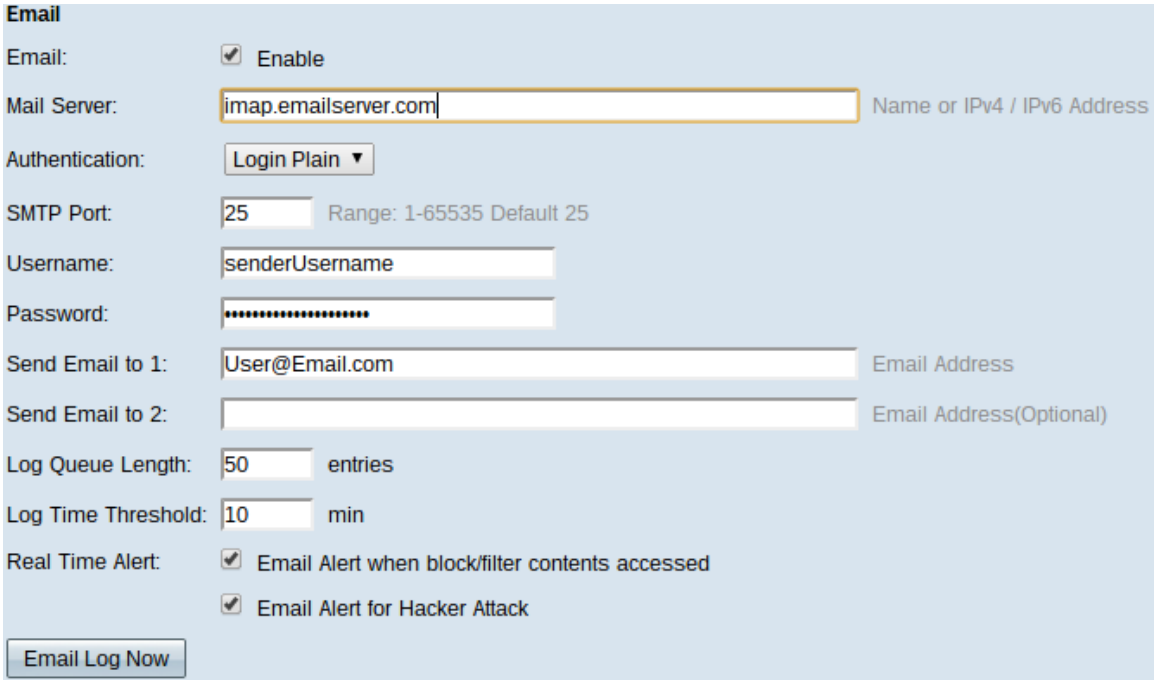
الخطوة 2. أدخل اسم المضيف أو عنوان IP الخاص بخادم سجل النظام في حقل Syslog Server 1.

الخطوة 3. (إختياري) لإرسال السجلات إلى خادم سجل نظام آخر، حدد **تمكين** في حقل syslog2.

الخطوة 4. إذا تم تحديد خانة الاختيار في حقل syslog2، فأدخل اسم المضيف أو عنوان IP الخاص بخادم سجل النظام في حقل Syslog Server 2.

الخطوة 5. طقطقة **حفظ**. تم تكوين سجلات النظام من خلال خوادم سجل النظام.

سجلات نظام البريد الإلكتروني



الخطوة 1. حدد **تمكين** في حقل البريد الإلكتروني لإرسال سجلات النظام إلى مستلم عبر البريد الإلكتروني.

الخطوة 2. أدخل اسم المجال أو عنوان IP لخادم البريد في حقل خادم البريد.

الخطوة 3. أختر نوع المصادقة الذي يستخدمه خادم البريد في حقل المصادقة.

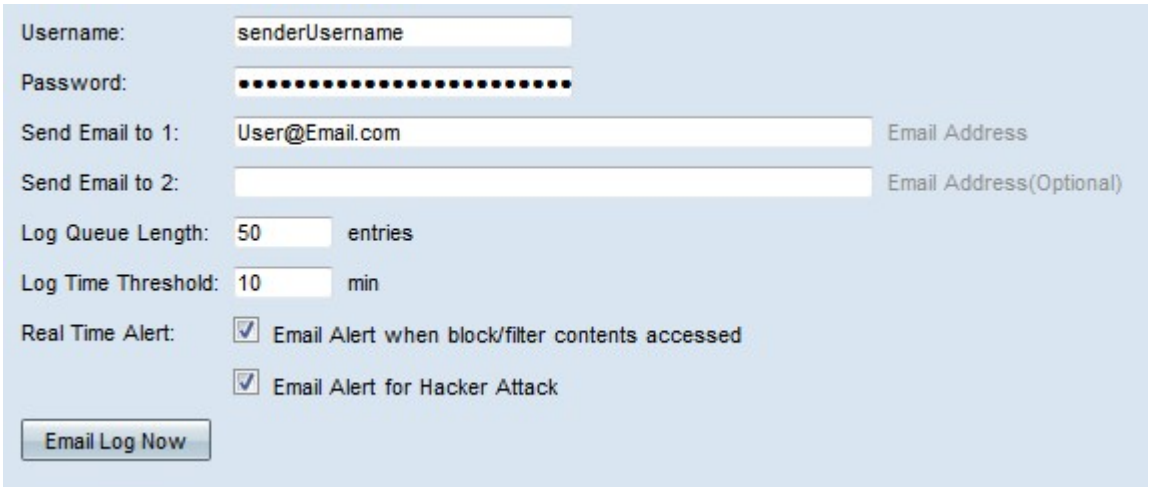
·بلا — لا يستخدم خادم البريد أية مصادقة.

·عادي لتسجيل الدخول — يستخدم خادم البريد المصادقة بتنسيق نص عادي.

·TLS — يستخدم خادم البريد تأمين طبقة النقل (TLS) للسماح للعميل والخادم بتبادل معلومات المصادقة بشكل آمن.

·SSL — يستخدم خادم البريد طبقة مآخذ التوصيل الآمنة (SSL) للسماح للعميل والخادم بتبادل معلومات المصادقة بشكل آمن.

الخطوة 4. أدخل منفذ بروتوكول نقل البريد البسيط (SMTP) الذي يستخدمه خادم البريد في حقل منفذ SMTP. SMTP هو بروتوكول يسمح بإرسال رسائل البريد الإلكتروني عبر شبكات IP.



الخطوة 5. أدخل اسم مستخدم مرسل البريد الإلكتروني في حقل اسم المستخدم.

الخطوة 6. أدخل كلمة مرور مرسل البريد الإلكتروني في حقل كلمة المرور.

الخطوة 7. أدخل عنوان البريد الإلكتروني لمستلم البريد الإلكتروني في الحقل إرسال بريد إلكتروني إلى 1.

الخطوة 8. (إختياري) أدخل عنوان بريد إلكتروني إضافي لإرسال رسائل البريد الإلكتروني الخاصة بالسجل إلى الحقل إرسال بريد إلكتروني إلى 2.

الخطوة 9. أدخل عدد إدخالات السجل التي يجب إجراؤها قبل إرسال السجل إلى مستلم البريد الإلكتروني في حقل طول قائمة انتظار السجل.

الخطوة 10. أدخل الفاصل الزمني الذي يرسل فيه الجهاز السجل إلى البريد الإلكتروني في حقل حد وقت السجل.

الخطوة 11. حدد خانة الاختيار الأولى لحقل تنبيه الوقت الفعلي لإرسال بريد إلكتروني على الفور عندما يحاول شخص ما، تم حظره أو تصفيته، الوصول إلى الموجه.

الخطوة 12. حدد خانة الاختيار الثانية لحقل تنبيه الوقت الفعلي لإرسال بريد إلكتروني على الفور عندما يحاول أحد المخترقين الوصول إلى الموجه من خلال هجوم رفض الخدمة (DOS).

ملاحظة: انقر فوق **سجل البريد الإلكتروني الآن** لإرسال السجل على الفور.

الخطوة 13. طقطقة **حفظ**. تم تكوين سجلات النظام عبر البريد الإلكتروني.

إعدادات السجل

الخطوة 1. حدد خانات الاختيار للأحداث التي ستقوم بتشغيل إدخال سجل.

·سجل التنبيه — يتم إنشاء هذه السجلات عند حدوث هجوم أو محاولة هجوم.

- Syn Flooding — يتم تلقي طلب SYN بسرعة أكبر من قدرة الموجه على معالجتها.

- انتحال IP — تلقى RV320 حزم IP بعناوين IP مزورة للمصدر.

- محاولة تسجيل الدخول غير المصرح بها — فشلت محاولة تم رفضها لتسجيل الدخول إلى الشبكة.

- إختبار اتصال الموت — تم إرسال إختبار اتصال بحجم غير طبيعي إلى واجهة في محاولة لتحطيم الجهاز المستهدف.

- Win Nuke — تم إرسال هجوم رفض الخدمة الموزع عن بعد (DDOS) المعروف باسم WinNuke، إلى واجهة في محاولة لتحطيم الجهاز الهدف.

·سجل عام — يتم إنشاء هذه السجلات عند حدوث إجراءات شبكة عامة.

- رفض السياسات — تم رفض الوصول إلى مستخدم استنادا إلى السياسات التي تم تكوينها للموجه.

- تسجيل الدخول المعتمد — تم تخويل المستخدم للوصول إلى الشبكة.

- رسائل خطأ النظام — حدث خطأ في النظام.

- السماح بالسياسات — تم منح حق الوصول لمستخدم استنادا إلى السياسات التي تم تكوينها للموجه.

- Kernel — تضمين جميع رسائل kernel في السجل. النواة هي الجزء الأول من نظام التشغيل الذي يتم تحميله في الذاكرة عند بدء التشغيل. رسائل Kernel هي سجلات مقترنة بالنواة.

- تغييرات التكوين — تم تعديل تكوين الموجه.

- IPSec و PPTP VPN — حدث تفاوض IPsec و PPTP VPN أو اتصال أو قطع اتصال.

- SSL VPN — حدث تفاوض SSL VPN أو اتصال أو قطع اتصال.

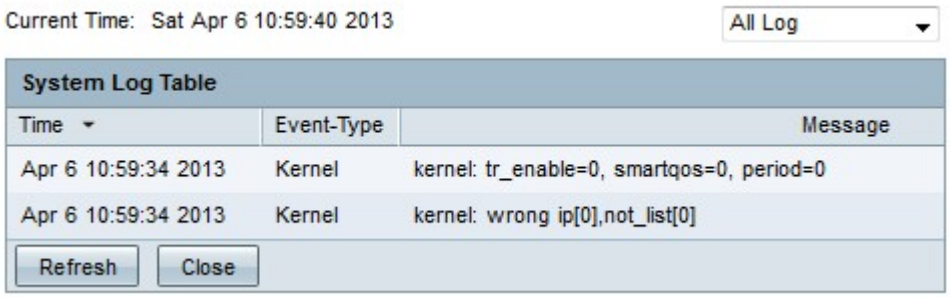
- الشبكة — تم إجراء اتصال فعلي أو فقدانه على واجهات WAN أو DMZ.

الخطوة 2. طقطقة **حفظ**. تم تكوين إعدادات السجل.

ملاحظة: انقر على **مسح السجل** لمسح السجل الحالي.

عرض سجل النظام

الخطوة 1. انقر فوق **عرض سجل النظام** لعرض جدول سجل النظام. تظهر نافذة *جدول سجل النظام*.



الخطوة 2. (إختياري) من القائمة المنسدلة أختر نوع السجلات التي تريد عرضها.

·جميع السجلات — تتضمن جميع رسائل السجل.

·سجل النظام — يتضمن رسائل خطأ النظام فقط.

·سجل أعمال جدار الحماية/DoS — يتضمن سجلات التنبيه فقط.

·سجل VPN — يتضمن سجلات IPSec و PPTP VPN و SSL VPN فقط.

·سجل الشبكة — ال يتضمن إلا سجلات الشبكة.

·سجل Kernel — يتضمن رسائل Kernel فقط.

·سجل المستخدم — يتضمن سياسات الرفض فقط، ويسمح بالسياسات، وسجل الدخول المعتمد، وسجلات تغيير التكوين

·سجل SSL — يتضمن سجلات SSL VPN فقط.

يعرض جدول سجل النظام المعلومات التالية.

·الوقت — وقت إنشاء السجل.

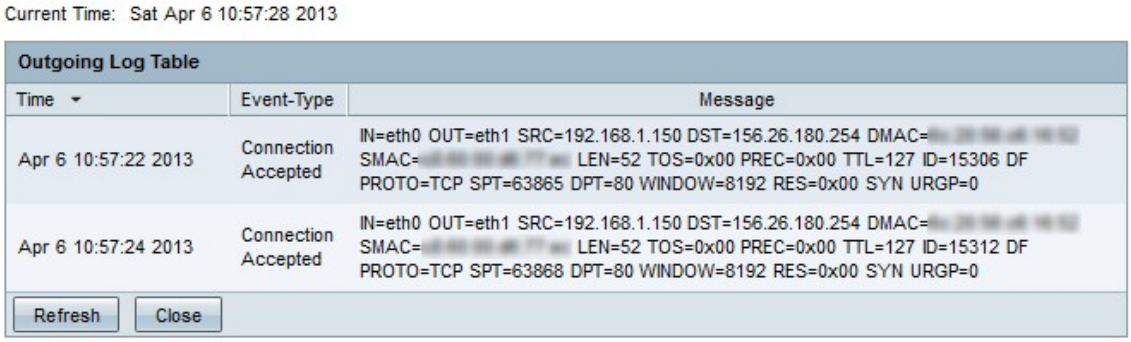
·نوع الحدث — نوع السجل.

·الرسالة — المعلومات المطابقة للسجل. وهذا يتضمن نوع النهج وعنوان IP المصدر وعنوان MAC المصدر.

ملاحظة: انقر فوق **تحديث** لتحديث جدول السجلات.

عرض جدول السجل الصادر

الخطوة 1. انقر فوق **جدول السجل الصادر** لعرض جدول السجل الذي يتعلق فقط بالحزم الصادرة. تظهر نافذة *جدول السجل الصادر*.



يعرض جدول السجل الصادر المعلومات التالية.

·الوقت — وقت إنشاء السجل.

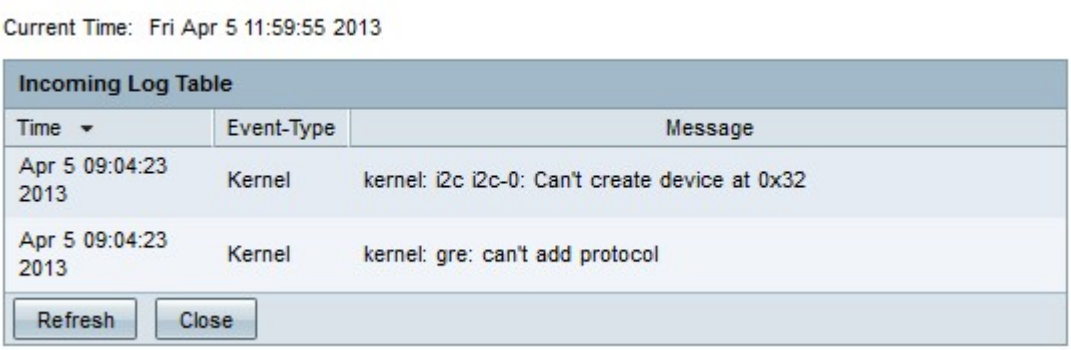
·نوع الحدث — نوع السجل.

·الرسالة — المعلومات المطابقة للسجل. وهذا يتضمن نوع النهج وعنوان IP المصدر وعنوان MAC المصدر.

ملاحظة: انقر فوق **تحديث** لتحديث جدول السجلات.

عرض جدول السجلات الواردة

الخطوة 1. انقر فوق **جدول السجل الوارد** لعرض جدول السجل الذي يتعلق فقط بالحزم الواردة. تظهر نافذة *جدول السجل الوارد*.



يعرض جدول السجلات الوارد المعلومات التالية.

·الوقت — وقت إنشاء السجل.

·نوع الحدث — نوع السجل.

·الرسالة — المعلومات المطابقة للسجل. وهذا يتضمن نوع النهج وعنوان IP المصدر وعنوان MAC المصدر.

ملاحظة: انقر فوق **تحديث** لتحديث جدول السجلات.

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).