إنشاء طلب توقيع شهادة على ESA

المحتويات

المقدمة

يوضح هذا المستند كيفية إنشاء طلب توقيع شهادة (CSR) على جهاز أمان البريد الإلكتروني (ESA).

إنشاء CSR على ESA

اعتبارا من AsyncOS 7.1.1، يمكن ل ESA إنشاء شهادة موقعة ذاتيا للاستخدام الخاص بك وإنشاء CSR للإرسال إلى مرجع مصدق والحصول على الشهادة العامة. تقوم هيئة الترخيص بإرجاع شهادة عامة موثوق بها موقعة بواسطة مفتاح خاص. أستخدم صفحة **الشبكة > الشهادات** في واجهة المستخدم الرسومية أو الأمر **certconfig** في واجهة سطر الأوامر لإنشاء الشهادة الموقعة ذاتيا، وإنشاء CSR، وتثبيت الشهادة العامة الموثوق بها.

إذا حصلت على شهادة أو قمت بإنشائها لأول مرة، ابحث في الإنترنت عن "شهادات خادم SSL لخدمات المرجع المصدق" واختر الخدمة التي تلبي إحتياجات مؤسستك على أفضل وجه. اتبع تعليمات الخدمة للحصول على الشهادة.

خطوات التكوين على واجهة المستخدم الرسومية (GUI)

1. طقطقت in order to خلقت مستقل توقيع شهادة، **يضيف شهادة** على الشبكة > شهادة صفحة في ال gui (أو **ال certconfig** أمر في ال CLI). في صفحة إضافة شهادة، أختر **إنشاء شهادة موقعة ذاتيا**.
2. أدخل هذه المعلومات للشهادة الموقعة ذاتيا: الاسم الشائع - اسم المجال المؤهل بالكامل.المنظمة - الاسم القانوني الدقيق للمنظمة.الوحدة التنظيمية - قسم المنظمة.المدينة (المنطقة المحلية) - المدينة التي يوجد فيها مقر المنظمة بصورة قانونية.الولاية (المقاطعة) - الولاية أو المقاطعة أو المنطقة التي يوجد فيها مقر المنظمة بشكل قانوني.البلد - الرسالتان الموجهتان إلى المنظمة الدولية للتوحيد القياسي (ISO) المختصتان عن البلد الذي توجد فيه المنظمة بصورة قانونية.المدة قبل انتهاء الصلاحية - عدد الأيام قبل انتهاء صلاحية الشهادة.حجم المفتاح الخاص - حجم المفتاح الخاص الذي سيتم إنشاؤه ل CSR. يتم دعم 2048 بت و 1024 بت فقط.
3. طقطقت **بعد ذلك** in order to شاهدت الشهادة وتوقيع معلومة.
4. أدخل اسما للشهادة. يقوم AsyncOS بتعيين الاسم الشائع بشكل افتراضي.
5. إذا كنت تريد إرسال CSR للشهادة الموقعة ذاتيا إلى مرجع مصدق، انقر فوق **تنزيل طلب توقيع الشهادة** لحفظ CSR في تنسيق البريد المحسن للخصوصية (PEM) إلى جهاز محلي أو جهاز شبكة.
6. انقر على **إرسال** لحفظ الشهادة وتنفيذ التغييرات. إذا تركت التغييرات غير ملتزمة، فسيفقد المفتاح الخاص ولا يمكن تثبيت الشهادة الموقعة.

عندما يرجع المرجع المصدق الشهادة العامة الموثوقة الموقعة بمفتاح خاص، انقر على اسم الشهادة في صفحة الشهادات وأدخل المسار إلى الملف على جهازك المحلي أو شبكتك لتحميل الشهادة. تأكد من أن الترخيص العام

الموثوق به الذي تتلقاه بتنسيق PEM أو تنسيق يمكنك تحويله إلى PEM قبل تحميله إلى الجهاز. يتم تضمين أدوات إكمال هذا باستخدام برنامج OpenSSL، وهو برنامج مجاني متوفر على http://www.openssl.org.

إذا قمت بتحميل الشهادة من المرجع المصدق، فسيتم الكتابة فوق الشهادة الموجودة. يمكنك أيضا تحميل شهادة وسيطة متعلقة بالشهادة الموقعة ذاتيا. يمكنك إستخدام الشهادة مع موزع رسائل عام أو خاص أو خدمات HTTPS لواجهة IP أو واجهة بروتوكول الوصول إلى الدليل خفيف الوزن (LDAP) أو جميع إتصالات أمان طبقة النقل الصادرة (TLS) إلى مجالات الوجهة.

معلومات ذات صلة

- دليل الإعداد الشامل لقوائم التحكم في الوصول إلى النقل (TLS) على ESA
- الدعم التقني والمستندات - Cisco Systems

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).