# تكوين TLS لتشفير الاتصال الوارد على منصت ESA

## المحتويات


المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
معلومات أساسية
التكوين
تمكين TLS على نهج تدفق بريد HAT لمستمع عبر واجهة المستخدم الرسومية
تمكين TLS على نهج تدفق بريد HAT لمستمع عبر CLI (واجهة سطر الأوامر)
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
معلومات ذات صلة


## المقدمة

يوضح هذا المستند كيفية تمكين أمان طبقة النقل (TLS) على موزع رسائل على جهاز أمان البريد الإلكتروني (ESA).

## المتطلبات الأساسية

### المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

### المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى ESA مع أي إصدار من AsyncOS.

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

## معلومات أساسية

يجب تمكين TLS لأي مستمعين حيث تتطلب التشفير للاتصالات الواردة. قد ترغب في تمكين TLS على المستمعين الذين يواجهون الإنترنت (المستمعون العامون)، ولكن ليس للمستمعين للأنظمة الداخلية (المستمعون الخاصون). أو قد ترغب في تمكين التشفير لكافة المستمعين. وبشكل افتراضي، لا يسمح مستمعو TLS سواء من القطاع الخاص أو العام باتصالات TLS. يجب تمكين TLS في جدول الوصول إلى المضيف (HAT) الخاص بمستمع لتمكين TLS للبريد الإلكتروني الوارد (الاستلام) أو الصادر (الإرسال). بالإضافة إلى ذلك، تم إيقاف تشغيل إعدادات نهج تدفق البريد الخاصة بمستمعي TLS الخاص والعام بشكل افتراضي.

## التكوين

يمكنك تحديد ثلاثة إعدادات مختلفة ل TLS على منصت:

| ضبط | معنى |
| --- | --- |
| لا | غير مس<br>ب LS<br>للاتصا<br>الوارد<br>تتطلب<br>الاتصا<br>بموصل<br>الرسائ<br>محادث<br>مشفر<br>بروتوك<br>نقل ال<br>البسيط<br>(MTP<br>هذا ه<br>الإعدا<br>الافترا<br>لكافة<br>المست<br>الذين<br>بتكوينه<br>على ا<br>يسمح<br>للاتصا<br>الوارد<br>المصغ<br>عملاء<br>الرسائ<br>(TAs<br>يسمح<br>للاتصا<br>الوارد<br>المست<br>MTAs<br>وإلى أ<br>تلقي أ<br>RTTL<br>S، يس<br>ESA |
| آثرتن | |
| إستوجبتا | |

## تمكين TLS على نهج تدفق بريد HAT لمستمع عبر واجهة المستخدم الرسومية

أكمل الخطوات التالية:

1. من صفحة "سياسات تدفق البريد"، أختر مصغيا تريد تعديل سياساته ثم انقر فوق الارتباط الخاص باسم النهج المراد تحريره. (يمكنك أيضا تحرير معلمات النهج الافتراضية.) يتم عرض صفحة تحرير سياسات تدفق البريد.
2. في قسم "التشفير والمصادقة"، في حقل "إستخدام TLS:"، أختر مستوى TLS الذي تريده للمصغي.
3. انقر على **إرسال**.
4. انقر فوق **تنفيذ التغييرات**، وقم بإضافة تعليق إختياري عند الضرورة، ثم انقر فوق **تنفيذ التغييرات** لحفظ التغييرات.

**ملاحظة**: يمكنك تعيين شهادة محددة لاتصالات TLS إلى مستمعين عامين فرديين عند إنشاء مستمع.

## تمكين TLS على نهج تدفق بريد HAT لمستمع عبر CLI (واجهة سطر الأوامر)

1. أستخدم الأمر **listEnergyConfig > edit** لاختيار وحدة إصغاء تريد تكوينها.
2. أستخدم الأمر **hostaccess > default** لتحرير إعدادات HAT الافتراضية الخاصة بالمستمع.
3. أدخل أحد هذه الخيارات لتغيير إعداد TLS عند مطالبتك:

```
?Do you want to allow encrypted TLS connections

No .1
Preferred .2
Required .3
3<[1]
```

```
You have chosen to enable TLS. Please use the 'certconfig' command to
.ensure that there is a valid certificate configured
```

لاحظ أن هذا المثال يطلب منك إستخدام الأمر **certconfig** لضمان وجود شهادة صالحة يمكن إستخدامها مع المنصت. إذا لم تقم بإنشاء أي شهادات، يستخدم المنصت شهادة العرض التوضيحي المثبتة مسبقا على الجهاز. يمكنك تمكين TLS باستخدام شهادة الإيضاح لأغراض الاختبار، ولكنه غير آمن ولا يوصى به للاستخدام العام. أستخدم الأمر **listActiveConfig > Edit > Certificate** لتعيين شهادة إلى المصغي.بمجرد تكوين TLS، يتم عرض الإعداد في ملخص موزع المصغي في واجهة سطر الأوامر:

```
Name: Inboundmail
Type: Public
Interface: PublicNet (192.168.2.1/24) TCP Port 25
Protocol: SMTP
:Default Domain
(Max Concurrency: 1000 (TCP Queue: 50
Domain map: disabled
TLS: Required
```

4. أدخل الأمر **commit** لتمكين التغيير.

## التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

- أستخدم ملف سجل البريد النصي وانظر هذا المستند: حدد ما إذا كان ESA يستخدم TLS للتسليم أو التلقي
- إستخدام تعقب الرسائل: GUI: مراقبة > تعقب الرسائل
- إستخدام التقارير: واجهة المستخدم الرسومية (GUI): مراقبة > إتصالات TLS
- أستخدم موقع ويب لجهة خارجية مثل checktls.com

## استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

يمكنك تحديد ما إذا كان ESA يرسل تنبيها إذا فشل تفاوض TLS عند تسليم الرسائل إلى مجال يتطلب اتصال TLS. تحتوي رسالة التنبيه على اسم المجال الوجهة لمفاوضات TLS الفاشلة. يرسل ESA رسالة التنبيه إلى كافة المستلمين الذين تم تعيينهم لتلقي تنبيهات مستوى خطورة التحذير لأنواع تنبيه النظام. يمكنك إدارة مستلمي التنبيهات عبر إدارة النظام > صفحة التنبيهات في واجهة المستخدم الرسومية (أو من خلال الأمر **alertconfig** في واجهة سطر الأوامر).

## معلومات ذات صلة

- أدلة المستخدم النهائي AsyncOS للبريد الإلكتروني
- 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).