

اطخأ فاش ك تسال TLSVERIFY مادختسإ اهال صإو TLS مئلسل

المحتويات

[المقدمة](#)

[معلومات ذات صلة](#)

المقدمة

يوضح هذا المستند كيفية استخدام TLSVERIFY لاستكشاف أخطاء تسليم TLS وإصلاحها.

فيما يتعلق بمعالجة البريد على جهاز أمان البريد الإلكتروني من Cisco (ESA)، قد ترى أن TLS لا يقوم بتسليم أو إرجاع خطأ أو تنبيه.

من ال CLI على الأداة، استعملت **tlsverify** أن يختبر TLS إتصال من جهازك إلى المجال الخارجي.

```
mail3.example.com> tlsverify
```

```
:Enter the TLS domain to verify against  
example.com <[
```

```
Enter the destination host to connect to. Append the port  
(example.com:26) if you are not connecting on port 25)  
example.com]> mx.example.com:25]
```

```
.Connecting to 1.1.1.1 on port 25  
.Connected to 1.1.1.1 from interface 10.10.10.10  
.Checking TLS connection  
.TLS connection established: protocol TLSv1, cipher RC4-SHA  
.Verifying peer certificate  
.Verifying certificate common name mx.example.com  
TLS certificate match mx.example.com  
.TLS certificate verified  
.TLS connection to 1.1.1.1 succeeded
```

```
.TLS successfully connected to mx.example.com  
.TLS verification completed
```

يظهر الأمر الإخراج أعلاه من **tlsverify** التحقق من صحة TLS من هذا الجهاز إلى الوجهة باستخدام عنوان IP 1.1.1.1

معلومات ذات صلة

- [جهاز أمان البريد الإلكتروني من Cisco - أدلة المستخدم النهائي](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةلخت. فرتمة مچرت مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءن إل دن تسمل