

# دليل ميلستلا دنع TLS ضوافت يف مكحتلا ESA

## المحتويات

[المقدمة](#)

[تمكين TLS عند التسليم](#)

[تعريفات إعدادات TLS](#)

[تمكين TLS على واجهة المستخدم الرسومية](#)

[تمكين TLS على واجهة سطر الأوامر](#)

## المقدمة

يوضح هذا المستند كيفية التحكم في تفاوض أمان طبقة النقل (TLS) عند التسليم على جهاز أمان البريد الإلكتروني (ESA).

وكما هو محدد في RFC 3207، فإن "TLS هو ملحق لخدمة SMTP يسمح لخادم SMTP والعميل باستخدام أمان طبقة النقل لتوفير اتصال خاص ومصادق عبر الإنترنت. TLS هي آلية شائعة لتحسين إتصالات TCP باستخدام الخصوصية والمصادقة.

## تمكين TLS عند التسليم

يمكنك طلب STARTTLS لتسليم البريد الإلكتروني إلى مجالات معينة باستخدام أي من الطريقتين الموضحتين في هذا المستند:

• استخدام الأمر `CLI destinationConfig`.

• من واجهة المستخدم الرسومية (GUI) أختار سياسات البريد < عناصر التحكم في الوجهة.

يسمح لك الأمر `destination control` (عناصر تحكم الوجهة) بتحديد خمسة إعدادات مختلفة لـ TLS لمجال محدد عند تضمين مجال ما. بالإضافة إلى ذلك، يمكنك تحديد ما إذا كان التحقق من صحة المجال ضروريا أم لا.

## تعريفات إعدادات TLS

إعدادات TLS

معنى

الإعداد

الافتراضي لـ

TLS الذي يتم

تعيينه عند

إستخدام صفحة

عناصر تحكم

الوجهة أو الأمر

`destinationCo`

`nfig` - الفرعي

الافتراضي

المستخدم

للاتصالات

الصادرة من

المنصت إلى

افتراضي

عامل نقل  
الرسائل (MTA)  
للمجال. يتم  
تعيين القيمة  
"الافتراضي" إذا  
قمت بالإجابة  
على لا على  
السؤال: "هل  
ترغب في تطبيق  
إعداد TLS  
محدد لهذا  
المجال؟"  
لا يتم التفاوض  
على TLS  
للاتصالات  
الصادرة من  
الواجهة إلى  
MTA للمجال.  
يتم التفاوض  
على TLS من  
واجهة ESA إلى  
MTA (MTA  
للمجال. ومع  
ذلك، إذا فشل  
تفاوض TLS  
(قبل تلقي  
إستجابة 220)،  
تستمر معاملة  
SMTP "في  
الخفاء" (غير  
المشفرة). لا  
توجد محاولة  
للتحقق مما إذا  
كانت الشهادة قد  
نشأت من مرجع  
مصدق موثوق  
به. إذا حدث خطأ  
بعد تلقي  
إستجابة 220،  
فلن تعود معاملة  
SMTP إلى  
مسح النص.  
يتم التفاوض  
على TLS من  
واجهة ESA إلى  
MTA (آت)  
للمجال. لم يتم  
إجراء أية محاولة  
للتحقق من  
شهادة المجال.  
إذا فشل  
التفاوض، فلن  
يتم إرسال أي

1 - لا

2 - مفضل

3. مطلوب

بريد إلكتروني  
من خلال  
الاتصال. إذا نجح  
التفاوض، يتم  
تسليم البريد عبر  
جلسة عمل  
مشفرة.  
يتم التفاوض  
على TLS من  
MTA إلى ESA  
(MTA) للمجال.  
يحاول الجهاز  
التحقق من  
شهادة  
المجال. يمكن  
تحقيق ثلاث  
نتائج:

- يتم  
التفاوض  
على TLS  
ويتم  
التحقق من  
الشهادة.  
يتم تسليم  
البريد عبر  
جلسة عمل  
مشفرة.

- يتم  
التفاوض  
على TLS،  
ولكن لم  
يتم التحقق  
من  
الشهادة.  
يتم تسليم  
البريد عبر  
جلسة عمل  
مشفرة.

- لم يتم  
إجراء  
اتصال  
TLS،  
وبالتالي لم  
يتم التحقق  
من  
الشهادة.  
يتم تسليم  
رسالة البريد  
الإلكتروني  
بنص عادي.

4. مفضل (تحقق)

يتم التفاوض  
على TLS من  
MTA إلى ESA  
(MTA) للمجال.  
يلزم التحقق من  
شهادة المجال.  
وهناك ثلاث  
نتائج محتملة:

• يتم

التفاوض  
على اتصال  
TLS ويتم  
التحقق من  
الشهادة.  
يتم تسليم  
رسالة البريد  
الإلكتروني  
عبر جلسة  
مشفرة.

• يتم

التفاوض  
على اتصال  
TLS، ولكن  
لم يتم  
التحقق من  
الشهادة من  
قبل مرجع  
ثقة (CA).

لم يتم

تسليم

البريد.

• لا يتم

التفاوض  
على اتصال  
TLS. لم  
يتم تسليم  
البريد.

الفرق بين TLS

مطلوب - التحقق

و TLS مطلوب -

التحقق من

وجود خيارات

المجال

المستضاف في

عملية التحقق

من الهوية.

الطريقة التي تتم

بها معالجة الهوية

المقدمة ونوع

المعرفات

5. مطلوب (تحقق)

6. مطلوب - التحقق من المجالات المستضافة

المرجعية  
المسموح  
باستخدامها،  
تصنع فرقا حول  
النتيجة النهائية.  
يتم اشتقاق  
الهوية المقدمة  
أولا من ملحق  
subjectAltNa  
me من النوع  
dNSName. إذا  
لم يكن هناك  
تطابق بين  
dNSName  
وأحد الهويات  
المرجعية  
المقبولة (-REF  
(ID)، يفشل  
التحقق بغض  
النظر عن وجود  
CN في حقل  
الموضوع ويمكن  
أن يمر بالمزيد  
من التحقق من  
الهوية. يتم  
التحقق من  
صحة CN  
المستمد من  
حقل الموضوع  
فقط عندما لا  
تحتوي الشهادة  
على أي من  
ملحق  
subjectAltNa  
me من النوع  
.dNSName  
يرجى مراجعة  
[عملية التحقق](#)  
[من TLS لأمان](#)  
[البريد الإلكتروني](#)  
[من Cisco](#)  
للحصول على  
مزيد من  
المعلومات.

## تمكين TLS على واجهة المستخدم الرسومية

1. اختر Montior < عناصر تحكم الواجهة.
2. طقطقة يضيف غاية.
3. قم بإضافة مجال الواجهة في حقل الواجهة.
4. حدد أسلوب دعم TLS من القائمة المنسدلة دعم TLS.
5. انقر فوق إرسال لإرسال التغييرات.

Destination Controls	
Destination:	example.com
IP Address Preference:	Default (IPv6 Preferred)
Limits:	Concurrent Connections: <input checked="" type="radio"/> Use Default (500) <input type="radio"/> Maximum of <input type="text" value="500"/> (between 1 and 1,000)
	Maximum Messages Per Connection: <input checked="" type="radio"/> Use Default (50) <input type="radio"/> Maximum of <input type="text" value="50"/> (between 1 and 1,000)
	Recipients: <input checked="" type="radio"/> Use Default (No Limit) <input type="radio"/> Maximum of <input type="text" value="0"/> per <input type="text" value="60"/> minutes <i>Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60</i>
	Apply limits: Per Destination: <input checked="" type="radio"/> Entire Domain <input type="radio"/> Each Mail Exchanger (MX Record) IP address  Per ESA hostname: <input checked="" type="radio"/> System Wide <input type="radio"/> Each Virtual Gateway <i>(recommended if Virtual Gateways are in use)</i>
TLS Support:	Required
<i>A security certificate/key has not yet been configured. Enabling TLS will automatically enable the "Demo" certificate/key. (To configure a different certificate/key, start the CLI and use the certconfig command.)</i>	
Bounce Verification:	Perform address tagging: <input checked="" type="radio"/> Default (No) <input type="radio"/> No <input type="radio"/> Yes  <i>Applies only if bounce verification address tagging is in use. See Mail Policies &gt; Bounce Verification.</i>
Bounce Profile:	Default <i>Bounce Profile can be configured at Network &gt; Bounce Profiles.</i>

Cancel

Submit

## تمكين TLS على واجهة سطر الأوامر

يستخدم هذا المثال الأمر `destinationConfig` لطلب إتصالات TLS والمحادثات المشفرة للمجال `example.com`. لاحظ أن هذا المثال يوضح أن TLS مطلوب لمجال يستخدم شهادة العرض التوضيحي المثبتة مسبقاً على الجهاز. يمكنك تمكين TLS باستخدام شهادة الإيضاح لأغراض الاختبار، ولكنه غير آمن ولا يوصى به للاستخدام العام.

يتم تعيين القيمة "الافتراضي" إذا قمت بالإجابة على لا على السؤال: "هل ترغب في تطبيق إعداد TLS محدد لهذا المجال؟" إذا أجبت بنعم، أختار لا، مفضلأو مطلوب.

ESA> `destconfig`

```
:Choose the operation you want to perform
.SETUP - Change global settings -
.NEW - Create a new entry -
.EDIT - Modify an entry -
.DELETE - Remove an entry -
.DEFAULT - Change the default -
.LIST - Display a summary list of all entries -
.DETAIL - Display details for one destination or all entries -
.CLEAR - Remove all entries -
.IMPORT - Import tables from a file -
.EXPORT - Export tables to a file -
new <[]
```

```
.Enter the domain you wish to configure
example.com <[]
```

```
:Choose the operation you want to perform
.SETUP - Change global settings -
```

```

        .NEW - Create a new entry -
        .EDIT - Modify an entry -
        .DELETE - Remove an entry -
        .DEFAULT - Change the default -
        .LIST - Display a summary list of all entries -
        .DETAIL - Display details for one destination or all entries -
        .CLEAR - Remove all entries -
        .IMPORT - Import tables from a file -
        .EXPORT - Export tables to a file -
        new <[]

```

```

        .Enter the domain you wish to configure
        example.com <[]

```

Do you wish to configure a concurrency limit for example.com? [Y]> **N**

Do you wish to apply a messages-per-connection limit to this domain? [N]> **N**

Do you wish to apply a recipient limit to this domain? [N]> **N**

Do you wish to apply a specific TLS setting for this domain? [N]> **Y**

```

        ?Do you want to use TLS support
        No .1
        Preferred .2
        Required .3
        Preferred - Verify .4
        Required - Verify .5
        Required - Verify Hosted Domains .6
        3 <[1]

```

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

Do you wish to apply a specific bounce verification address tagging setting for this domain? [N]> **N**

Do you wish to apply a specific bounce profile to this domain? [N]> **N**

Do you wish to apply a specific IP sort preference to this domain? [N]> **N**

.There are currently 3 entries configured

```

        :Choose the operation you want to perform
        .SETUP - Change global settings -
        .NEW - Create a new entry -
        .EDIT - Modify an entry -
        .DELETE - Remove an entry -
        .DEFAULT - Change the default -
        .LIST - Display a summary list of all entries -
        .DETAIL - Display details for one destination or all entries -
        .CLEAR - Remove all entries -
        .IMPORT - Import tables from a file -
        .EXPORT - Export tables to a file -
        list <[]

```

Rate Domain	Bounce Limiting	Bounce TLS	Bounce Verification	IP Version Profile	Preference
example.com	Default	On	Default	Default	Default
Default)	On	Off	Off	(Default)	Prefer IPv6)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت  
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبلاو  
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل مهتغب  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه  
ىلإ أمئاد عوچرلاب ي صؤتو تامچرتل هذه ةقدنع اهتيلوئسم Cisco  
Systems (رفوتم طبارلا) ي لصلأل يزي لچنل دن تسمل