تكوين TLSv1.3 لعبارة البريد الإلكتروني الآمنة

المحتويات

المقدمة

يصف هذا المستند تكوين بروتوكول TLS v1.3 لعبارة البريد الإلكتروني الآمنة (SEG) من Cisco.

المتطلبات الأساسية

هناك حاجة إلى معرفة عامة حول إعدادات SEG والتكوين.

المكونات المستخدمة

- تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:
  - Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 والإصدارات الأحدث.
- إعدادات تكوين SEG SSL.

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

نظرة عامة

وقد أدمج SEG بروتوكول TLS v1.3 لتشفير الاتصالات للخدمات ذات الصلة SMTP و HTTPS؛ واجهة مستخدم كلاسيكية و NGUI و REST API.

يتميز بروتوكول TLS v1.3 باتصال أكثر أمانا وتفاوض أسرع حيث تعمل الصناعة على جعله المعيار.

يستخدم SEG طريقة تكوين SSL الموجودة ضمن SEG WebUI أو CLI ل SSL مع بعض الإعدادات الإبرازة إلى الابرازه.

- نصائح وقائية عند تكوين البروتوكولات المسموح بها.
- لا يمكن التلاعب بالشفرات.
- يمكن تكوين TLS v1.3 ل GUI HTTPS، والبريد الوارد، والبريد الصادر.
- تستخدم خيارات تحديد خانة الاختيار لبروتوكول TLS بين TLS v1.0 إلى TLS v1.3 نطم موضح بمزيد من التفاصيل داخل المقالة.

التكوين

وتدمج مجموعة الخدمات الخاصة بروتوكول TLS v1.3 ل HTTPS و SMTP ضمن نظام التشغيل AsycOS 15.5. يوصى بالحذر عند إختيار إعدادات البروتوكول لمنع حالات فشل تسليم/تلقي البريد الإلكتروني و HTTPS.

الإصدارات السابقة من دعم TLS v1.2 من Cisco SEG في الطرف العالي مع مزودي البريد الإلكتروني الآخرين مثل MS O365 التي تدعم TLS v1.2 في وقت كتابة المقالة.

يدعم تنفيذ Cisco SEG لبروتوكول TLS v1.3 3 تشفير افتراضي لا يمكن تغييره أو إستبعاده ضمن إعدادات تكوين تشفير SEG كما تسمح البروتوكولات الأخرى.

لا تزال إعدادات تكوين SEG SSL الموجودة تسمح بمعالجة TLS v1.0، v1.1، v1.2 لمجموعات التشفير.

تشفير TLS 1.3:

TLS_AES_256_GCM_SHA384

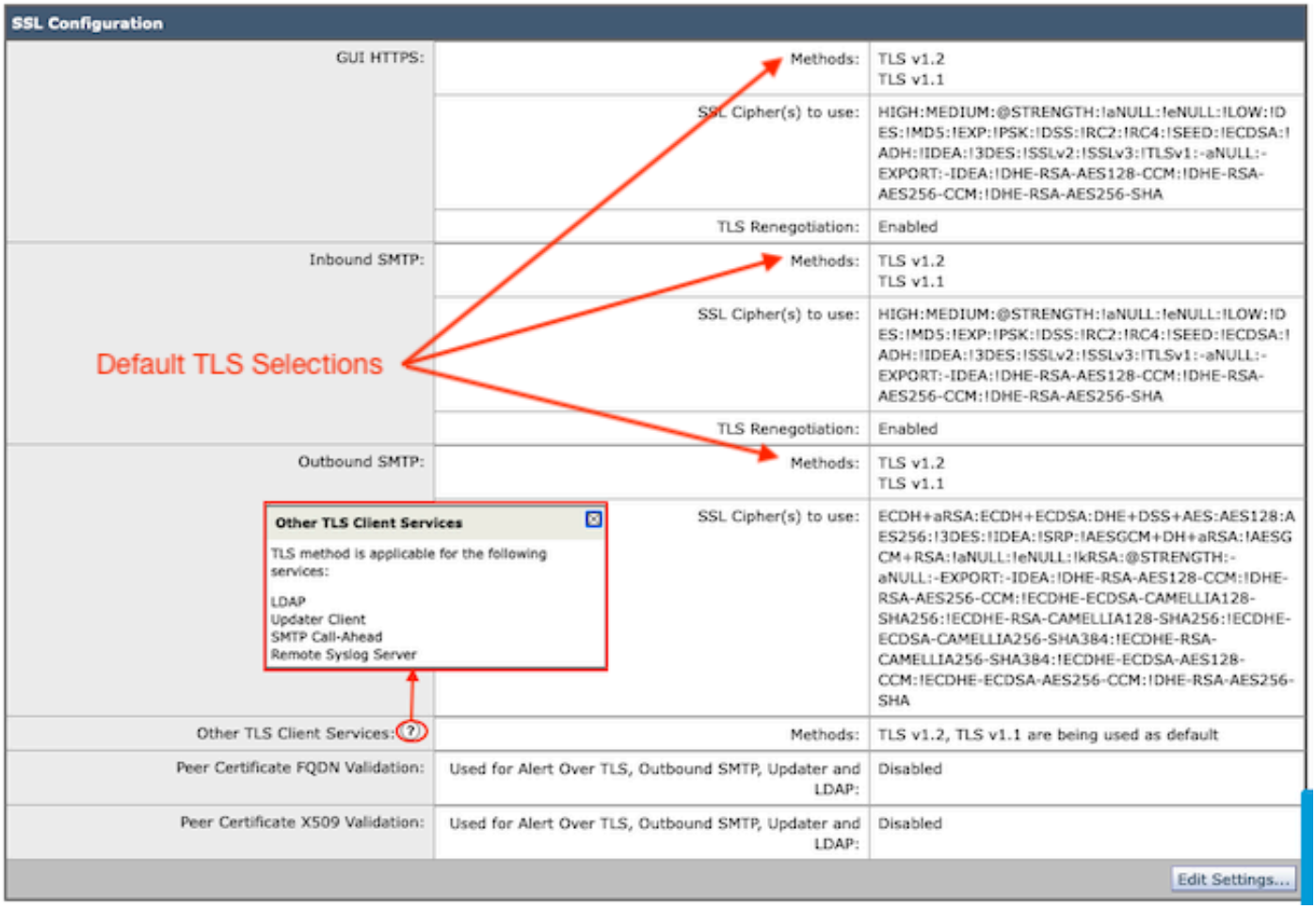
TLS_CHACHA20_POLY1305_SHA256

TLS_AES_128_GCM_SHA256

التكوين من WebUI

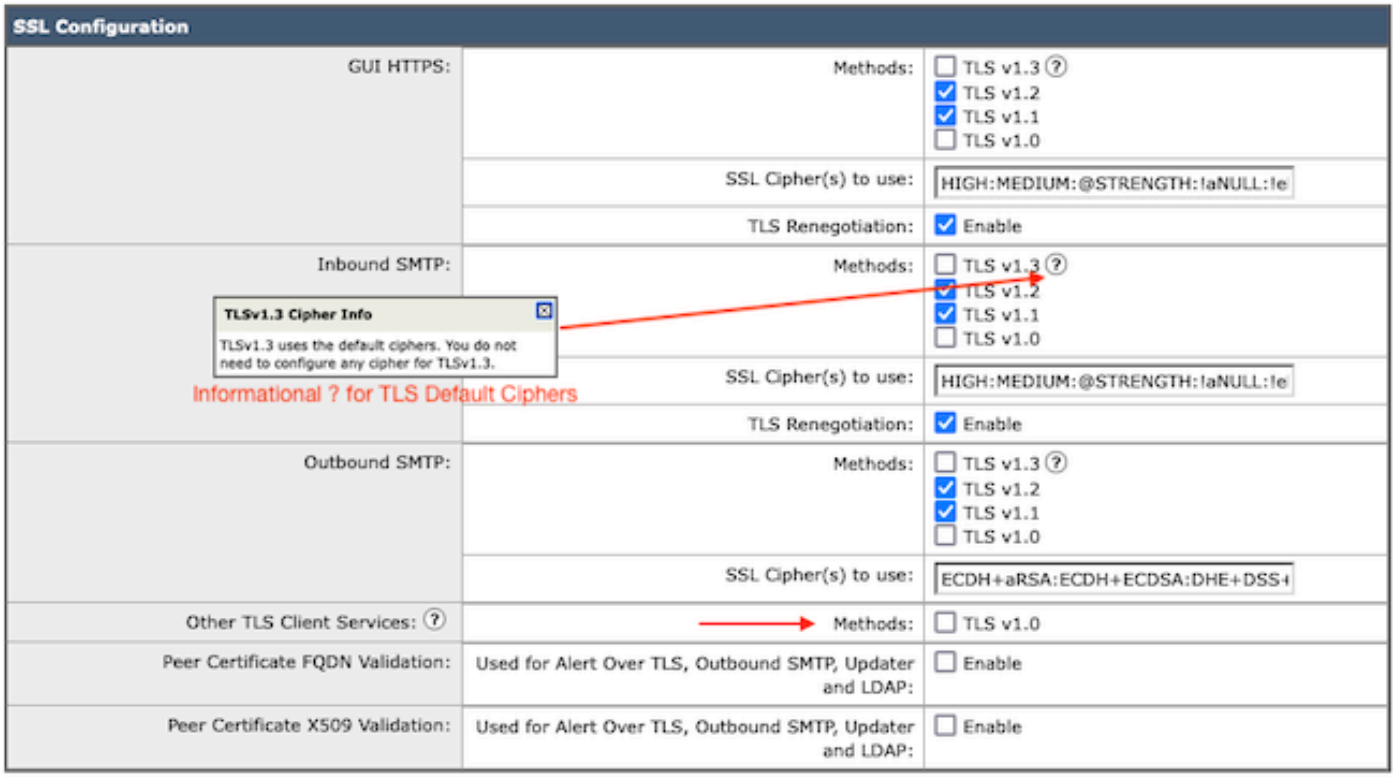
انتقل إلى > إدارة النظام > تكوين SSL

- تتضمن ترقية منشور تحديد بروتوكول TLS الافتراضي إلى 15.5 AsyncOS TLS v1.1 و TLS v1.2 فقط.
- يستخدم إعداد "خدمات عميل TLS الأخرى" TLS v1.2 مع خيار التحديد، أستخدم TLS v1.1 فقط TLS v1.0.



حدد "تحرير الإعدادات" لتقديم خيارات التكوين.

- يتم تحديد TLS v1.1 و TLS v1.2 باستخدام المربعات النشطة لتحديد البروتوكولات الأخرى.
- التالي ؟ جوار كل TLS v1.3 وه تكرار لخيارات التشفير الثابت.
- يعرض "خدمات عميل TLS الأخرى:" الآن خيار إستخدام TLS v1.0 فقط في حالة تحديده.



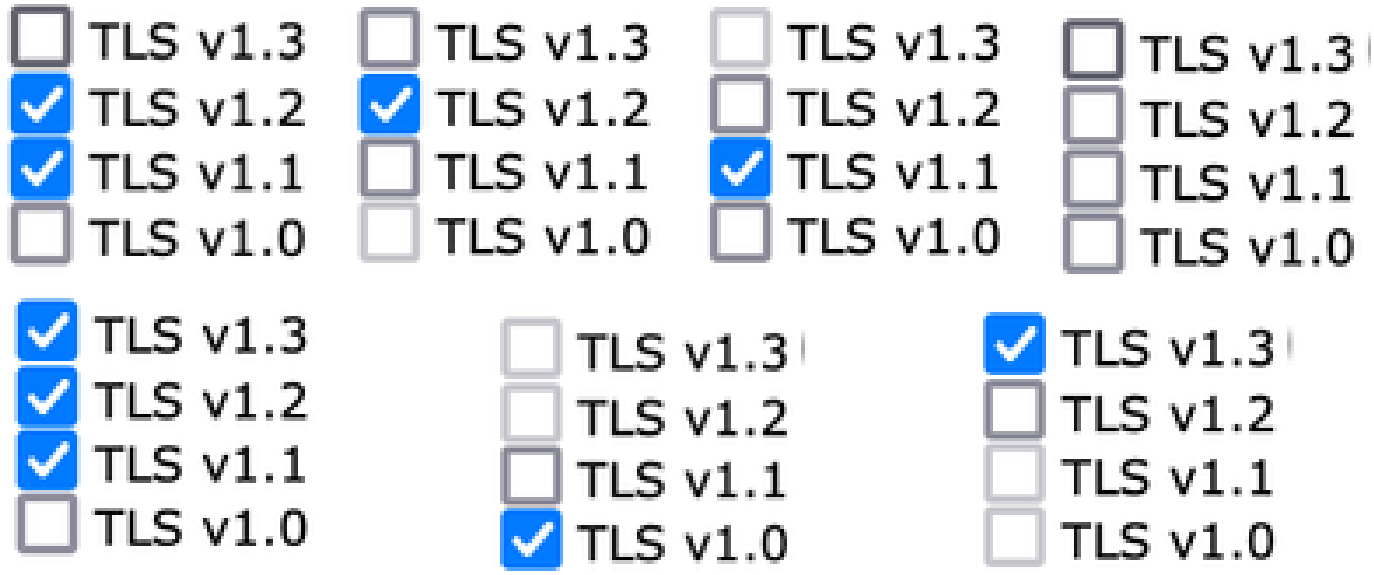
Note:
TLS protocols can be enabled only in sequence.
The configured SSL Cipher(s) do not apply to TLS 1.3. The TLS 1.3 protocol uses default ciphers.

تتضمن خيارات تحديد بروتوكول TLS TLS V1.0 و TLS v1.1 و TLS v1.2 و TLS v1.3.

- يتم تحديد ترقية مادة النشر إلى بروتوكولات AsyncOS 15.5، ويتم تحديد بروتوكولات TLS v1.1 و TLS v1.2 بشكل افتراضي.

ملاحظة: TLS1.0 مهمل وبالتالي معطل بشكل افتراضي. لا يزال TLS v1.0 متوفرا إذا اختار المالك تمكينه.

- تضئ خيارات خانة الاختيار باستخدام مربعات ذات مزالج تعرض البروتوكولات المتاحة ومربعات ذات علامات خارجية للخيارات غير المتوافقة.
- توضح خيارات العينة في الصورة خيارات خانة الاختيار.



ترجيل طريقة عرض نموذج الالتزام لبروتوكولات TLS المحددة.

SSL Configuration		
GUI HTTPS:	Methods:	TLS v1.3 TLS v1.2
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:-aNULL:-EXPORT:-IDEA:!DHE-RSA-AES256-SHA:!DHE-RSA-AES128-CCM:!DHE-RSA-AES256-CCM
	TLS Renegotiation:	Enabled
Inbound SMTP:	Methods:	TLS v1.3 TLS v1.2 TLS v1.1 TLS v1.0
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:-aNULL:-EXPORT:-IDEA:!DHE-RSA-AES256-SHA:!DHE-RSA-AES128-CCM:!DHE-RSA-AES256-CCM
	TLS Renegotiation:	Enabled
Outbound SMTP:	Methods:	TLS v1.3 TLS v1.2 TLS v1.1
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:-aNULL:-EXPORT:-IDEA:!DHE-RSA-AES256-SHA:!DHE-RSA-AES128-CCM:!DHE-RSA-AES256-CCM:!ECDHE-ECDSA-CAMELLIA128-SHA256:!ECDHE-RSA-CAMELLIA128-SHA256:!ECDHE-ECDSA-CAMELLIA256-SHA384:!ECDHE-RSA-CAMELLIA256-SHA384:!ECDHE-ECDSA-AES128-CCM:!ECDHE-ECDSA-AES256-CCM
Other TLS Client Services:	Methods:	TLS v1.2, TLS v1.1 are being used as default
Peer Certificate FQDN Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	Disabled
Peer Certificate X509 Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	Disabled
		Edit Settings...

ملاحظة: تتسبب التعديلات التي تم إجراؤها على بروتوكول HTTPS TLS لواجهة المستخدم الرسومية (GUI) في قطع اتصال قصير بواجهة مستخدم الويب بسبب إعادة تعيين خدمة HTTPS.

CLI تشكيل:

يسمح SEG باستخدام TLS v1.3 على 3 خدمات:

- GUI HTTPS
- SMTP الوارد
- SMTP الصادر

عند تنفيذ الأمر > sslconfig، يتم إخراج البروتوكولات والشفرات التي تم تكوينها حاليا ل GUI HTTPS، و SMTP الوارد، و SMTP الصادر

- أسلوب GUI HTTPS: tlsv1_0tlsv1_1tlsv1_2tlsv1_3
- أسلوب SMTP الوارد: tlsv1_0tlsv1_1tlsv1_2tlsv1_3
- أسلوب SMTP الصادر: tlsv1_1tlsv1_2tlsv1_3

أختر العملية التي تريد تنفيذها:

- GUI - تحرير إعدادات HTTPS SSL لواجهة المستخدم الرسومية.
- الوارد - تحرير إعدادات SMTP الواردة ssl.
- الصادر - تحرير إعدادات SMTP الصادرة ssl.

[]> الوارد

أدخل أسلوب SMTP SSL الوارد الذي تريد إستخدامه.

1. TLS v1.3
2. TLS v1.2
3. TLS v1.1
4. TLS v1.0

[2-4]> 1-3

ملاحظة: يمكن أن تتضمن عملية تحديد SEG رقم قائمة واحد مثل 2، نطاق من أرقام القوائم مثل 1-4، أو أرقام قوائم مفصولة بفواصل 1،2،3.

تقبل المطالبات التالية ل CLI sslconfig القيمة الموجودة بالضغط على "enter" أو تعديل الإعداد حسب الرغبة.

قم بإكمال التغيير باستخدام الأمر > التزام << أدخل تعليقا إختياريا إذا كنت تريد >> اضغط "إدخال" لإكمال التغييرات.

التحقق من الصحة

يتضمن هذا القسم بعض سيناريوهات الاختبار الأساسية والأخطاء التي يمكن أن تظهر بسبب إصدارات بروتوكول TLS غير المتطابقة أو أخطاء بناء الجملة.

نموذج إدخال السجل لمفاوضات SMTP الصادرة من SEG التي تؤدي إلى رفض بسبب الوجهة غير المدعومة TLS v1.3:

```
Wed Jan 17 20:41:18 2024 Info: DCID 485171 TLS deferring: (336151598, 'error:1409442E:SSL routines:ssl3
```

نموذج إدخال السجل لخادم مرسلة يستقبل TLS v1.3 تم التفاوض عليه بنجاح:

```
Wed Jan 17 21:09:12 2024 Info: DCID 485206 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384
```

نموذج إدخال سجل لخادم مستلم دون تمكين TLS v1.3.

```
Wed Jan 17 20:11:06 2024 Info: ICID 1020004 TLS failed: (337678594, 'error:14209102:SSL routines:tls_ea
```

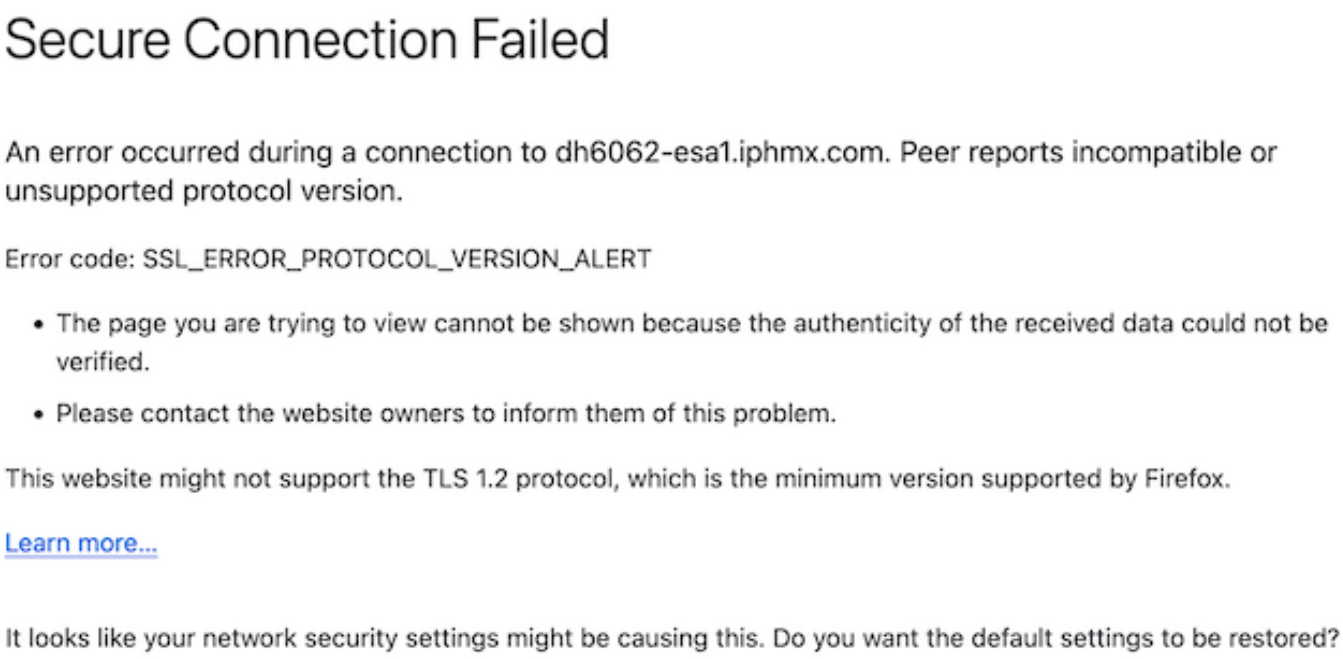
إستقبال TLS المدعومة من SEG الإصدار 1.3

```
Wed Jan 17 21:09:12 2024 Info: ICID 1020089 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384
```

للتحقق من وظيفة المستعرض، ما عليك سوى فتح جلسة مستعرض ويب ل SEG WebUI أو NGUI التي تم تكوينها باستخدام TLSv1.3.

ملاحظة: تم تكوين كافة مستعرضات الويب التي قمنا باختبارها بالفعل لقبول TLS v1.3.

- الاختبار: ينتج عن تكوين إعداد المستعرض على دعم TLS v1.3 لتعطيل Firefox أخطاء على كل من ClassicUI و NGUI الخاص بالجهاز.
- واجهة مستخدم (UI) كلاسيكية باستخدام Firefox تم تكوينها لاستبعاد TLS v1.3، كإختبار.
- ستتلقى NGUI الخطأ نفسه مع الاستثناء الوحيد وهو رقم المنفذ 4431(الافتراضي) داخل عنوان URL.



- لضمان الاتصال، تحقق من إعدادات المستعرض للتأكد من تضمين TLSv1.3. (هذه العينة من Firefox وتستخدم الأرقام من 1 إلى 4

security.tls.version.fallback-limit	4
security.tls.version.max	4
security.tls.version.min	3

معلومات ذات صلة

- بوابة البريد الإلكتروني الآمنة من Cisco - دليل الإعداد
- صفحة بدء تشغيل عبارة البريد الإلكتروني الآمن من Cisco لدعم الأدلة
- عبارة البريد الإلكتروني الآمنة من Cisco - ملاحظات الإصدار

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).