تكوين TLSv1.3 لمدير ويب البريد الإلكتروني الآمن

المحتويات

المقدمة

يصف هذا المستند تكوين بروتوكول TLS v1.3 لـ Cisco Secure Email and Web Manager (EWM)

المتطلبات الأساسية

معرفة عامة بإعدادات SEWM وتكوينه مطلوبة.

المكونات المستخدمة

- Cisco Secure Email Web Manager (SEWM) AsyncOS 15.5.1 والإصدارات الأحدث.
- إعدادات تكوين 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

قام SEWM بدمج بروتوكول TLS v1.3 لتشفير الاتصالات للخدمات ذات الصلة HTTPS؛ واجهة المستخدم الكلاسيكية، NGUI، و REST API.

ويتميز بروتوكول TLS v1.3 بإمكانية اتصال أكثر أمانا ومفاوضات أسرع بينما تسعى الصناعة جاهدة لجعله المعيار.

يستخدم SEWM طريقة تكوين SSL الموجودة داخل SEGWebUIor CLI الخاص بـ SSL مع بعض الإعدادات البارزة إلى بارزها.

- نصائح وقائية عند تكوين البروتوكولات المسموح بها.
- لا يمكن معالجة شفرات TLS v1.3.
- يمكن تكوين TLS v1.3 لـ GUI HTTPS فقط.
- تستخدم خيارات تحديد خانة الاختيار لبروتوكول TLS بين TLS v1.0 و TLS v1.3 من موضح بمزيد من التفاصيل داخل المقالة.

التكوين

أدمج SEWM بروتوكول TLS v1.3 ل HTTPS ضمن AsycOS 15.5.

يوصى بالحذر عند إختيار إعدادات البروتوكول لمنع فشل HTTPS.

دعم مستعرض الويب ل TLS v1.3 شائع بالرغم من أن بعض البيئات تتطلب عمليات ضبط للوصول إلى SEWM.

يدعم تنفيذ Cisco SEWM لبروتوكول TLS v1.3 3 تشفير افتراضي لا يمكن تغييره أو إستبعاده داخل SEWM.

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 HTTPS 15.5 AsyncOS TLS v1.2 و TLS v1.1 فقط.
- لا تدعم الخدمتان الإضافيتان المدرجتان، وهما خدمات LDAP الآمنة وخدمات التحديث، TLS v1.3.

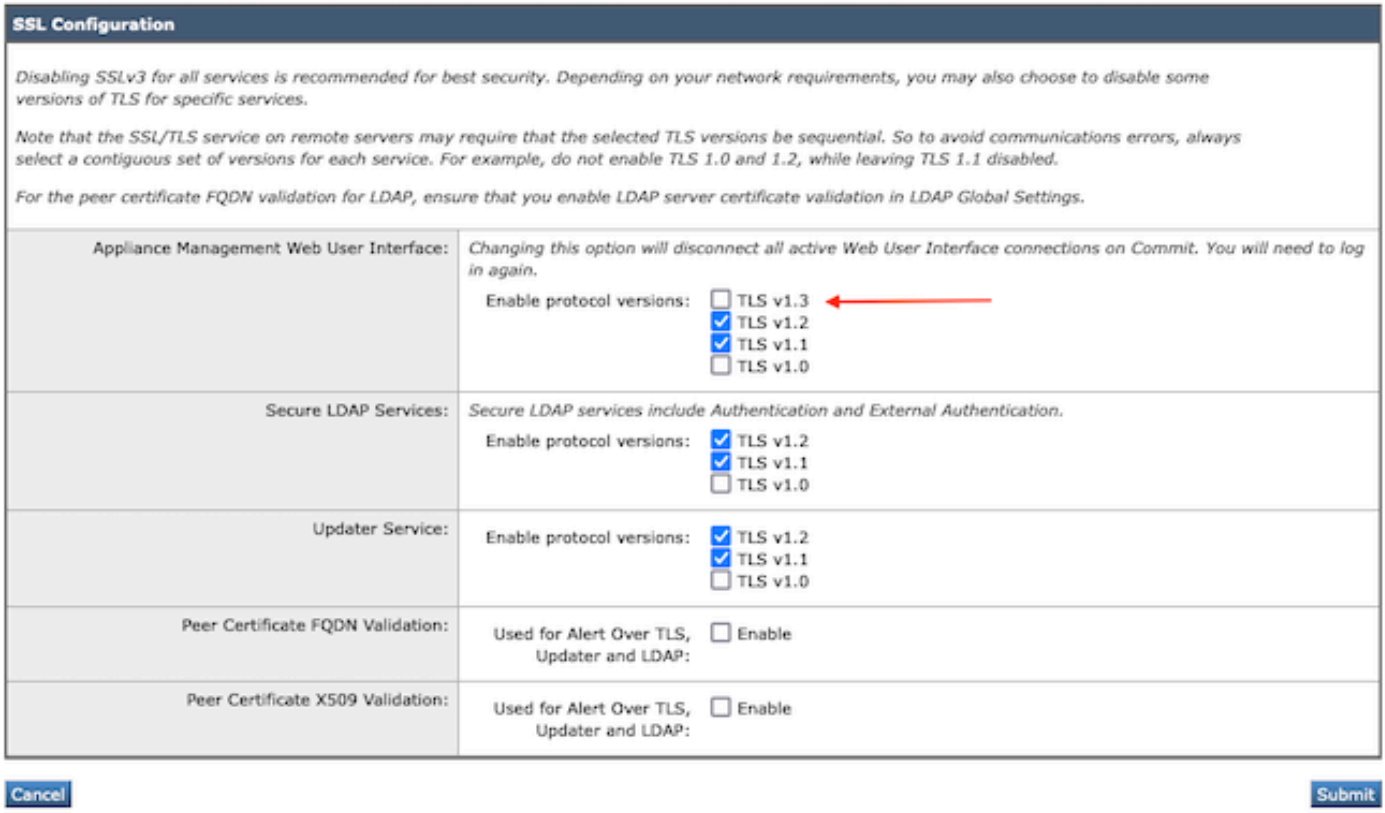
SSL Configuration

SSL Configuration		
Appliance Management Web User Interface:	Enable protocol versions:	TLS v1.2 TLS v1.1
Secure LDAP Services:	Enable protocol versions:	TLS v1.2 TLS v1.1
Updater Service:	Enable protocol versions:	TLS v1.2 TLS v1.1
Peer Certificate FQDN Validation:	Used for Alert Over TLS, Updater and LDAP:	Disabled
Peer Certificate X509 Validation:	Used for Alert Over TLS, Updater and LDAP:	Disabled
		Edit Settings

حدد "تحرير الإعدادات" لتقديم خيارات التكوين.

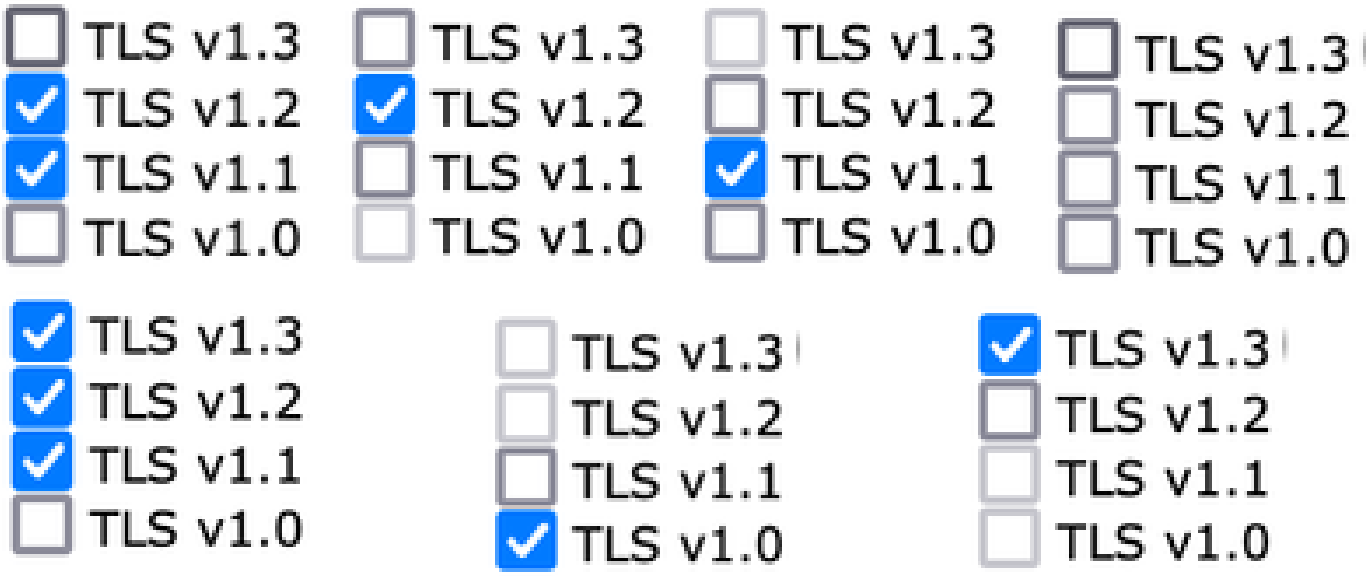
تتضمن خيارات تحديد بروتوكول TLS ل "واجهة مستخدم ويب"، TLS v1.2 و TLS v1.1 و TLS v1.0 و TLS v1.3.

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

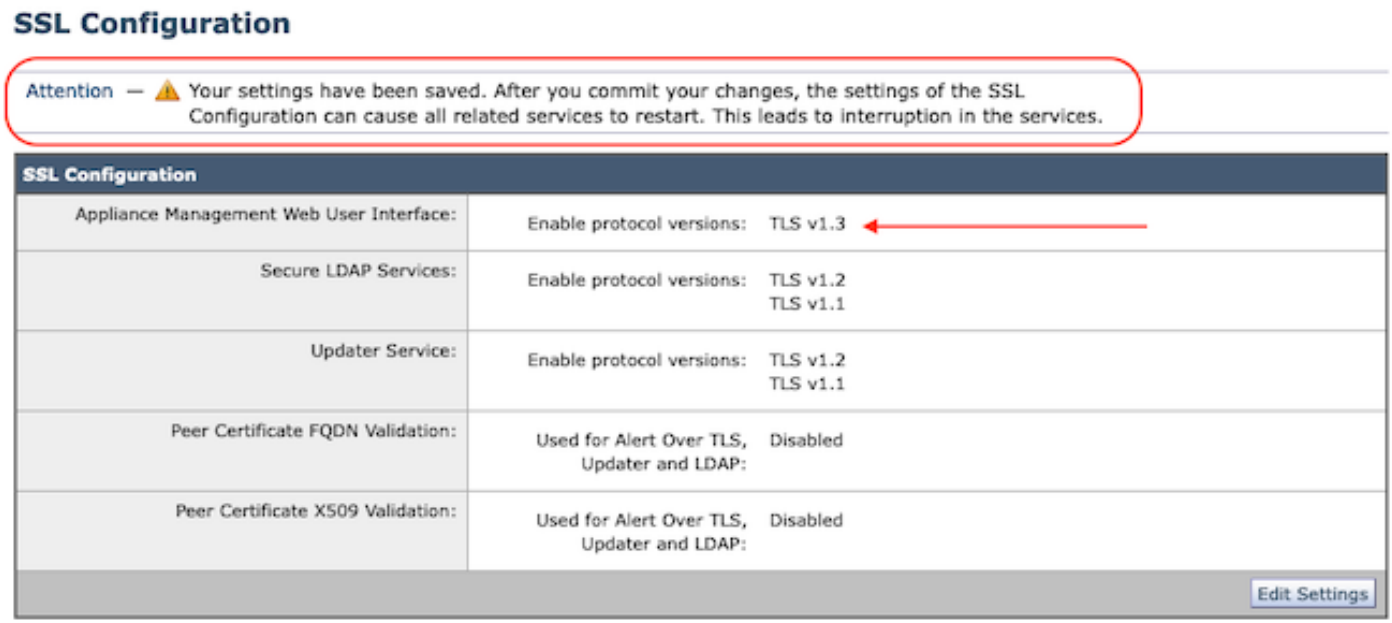


ملاحظة: TLS1.0 مهمل وبالتالي معطل بشكل افتراضي. لا يزال TLS v1.0 متوفرا إذا اختار المالك تمكينه.

- 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 لواجهة مستخدم الويب.



ملاحظة: قد تتسبب التعديلات التي يتم إجراؤها على تكوين SSL في إعادة تشغيل الخدمات ذات الصلة. تتسبب في مقاطعة قصيرة لخدمة WebUI.



التكوين من CLI

يسمح EWM ب TLS v1.3 على خدمة واحدة: WebUI

sma1.example.com> sslconfig

يوصى بتعطيل SSLv3 للحصول على أفضل تأمين.

لاحظ أن خدمة SSL/TLS على الخوادم البعيدة تتطلب أن تكون إصدارات TLS المحددة متتالية. لتجنب أخطاء الاتصال، قم دائما بتحديد ملف متصل
مجموعة من الإصدارات لكل خدمة. على سبيل المثال، لا تقم بتمكين TLS 1.0 و 1.2، مع ترك TLS 1.1 معطلا.

أختر العملية التي تريد تنفيذها:
- الإصدارات - تمكين إصدارات SSL/TLS أو تعطيلها
- peer_cert_fqdn - التحقق من تواقف شهادة النظير مع FQDN للتنبيه عبر TLS والمحدث و LDAP.
- PEER_CERT_X509 - التحقق من تواقف شهادة النظير ل X509 للتنبيه عبر TLS والمحدث و LDAP.
[]> الإصدارات

تمكين أو تعطيل إصدار SSL/TLS للخدمات:

محدث - خدمة تحديث
WebUI - واجهة مستخدم ويب لإدارة الأجهزة
LDAPs - خدمات LDAP الآمنة (بما في ذلك المصادقة والمصادقة الخارجية)

لاحظ أن TLSv1.3 غير متوفر ل Updater و LDAPs، يمكن تكوين WebUI فقط مع TLSv1.3.

إصدارات SSL/TLS الممكنة حاليا حسب الخدمة: (Y : ممكن، N : معطل)

UpdateUI LDAPs

TLSv1.0 N N
TLSv1.1 Y N Y
TLSv1.2 Y Y
TLSv1.3 ال/a ال ينطبق

حدد الخدمة التي سيتم تمكين/تعطيل إصدارات SSL/TLS لها:

1. محدث
2. WebUI
3- أقل البلدان نمواً
4 - جميع الخدمات
[]> 2

البروتوكول (البروتوكولات) الممكنة حاليا ل WebUI هي TLSv1.2.

لتغيير الإعداد لبروتوكول محدد، حدد أحد الخيارات أدناه:

1. TLSv1.0
2. TLSv1.1
3. TLSv1.2
4. TLSv1.3
[]> 4

دعم TLSv1.3 لواجهة مستخدم ويب لإدارة الأجهزة معطل حاليا. هل تريد تمكينها؟ [N]> Y

البروتوكولات الممكنة حاليا ل WebUI هي TLSv1.3 و TLSv1.2.

أختر العملية التي تريد تنفيذها:
- الإصدارات - تمكين إصدارات SSL/TLS أو تعطيلها
- peer_cert_fqdn - التحقق من توافق شهادة النظير مع FQDN للتنبيه عبر TLS والمحدث و LDAP.
- PEER_CERT_X509 - التحقق من توافق شهادة النظير لـ X509 للتنبيه عبر TLS والمحدث و LDAP.
[]>

SMA1.example.com> الالتزام

تحذير: تتسبب التغييرات في تكوين SSL في
ستتم إعادة تشغيل هذه العمليات بعد Commit - gui،euq_webui.
يؤدي ذلك إلى مقاطعة قصيرة لعمليات SMA.

الرجاء إدخال بعض التعليقات التي تصف تغييراتك:
[]> تمكين TLS v1.3

التغييرات التي تم الالتزام بها: Sun Jan 28 23:55:40 2024 EST

إعادة تشغيل واجهة المستخدم الرسومية...
إعادة تشغيل واجهة المستخدم الرسومية
يتم الآن إعادة تشغيل EUQ_WEBUI...
تمت إعادة تشغيل euq_webui

انتظر وقتا قصيرا وتأكد من إمكانية الوصول إلى WebUI.

ملاحظة: يتطلب تحديد إصدارات متعددة من TLS لخدمة ما من المستخدم تحديد خدمة وإصدار بروتوكول، ثم تكرار تحديد خدمة وبروتوكول مرة أخرى حتى يتم تعديل جميع الإعدادات.

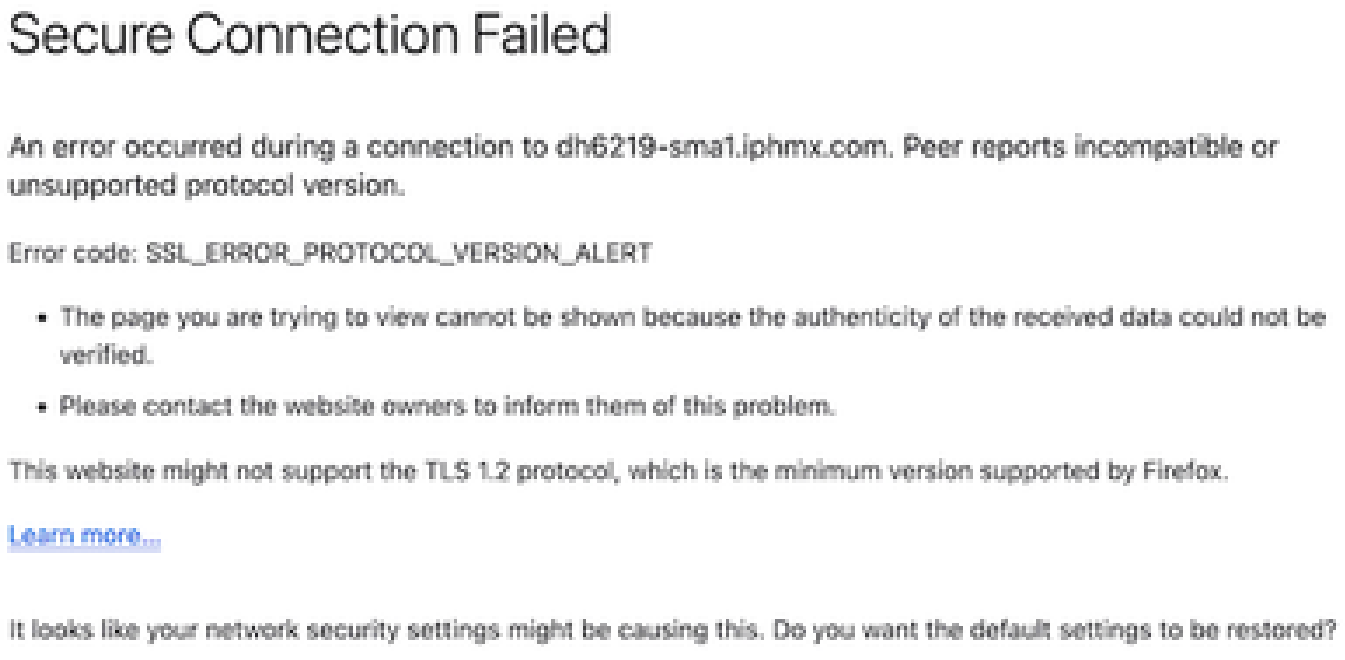
التحقق من الصحة

يتضمن هذا القسم بعض سيناريوهات الاختبار الأساسية والأخطاء التي تظهر بسبب عدم تطابق الإصدارات أو أخطاء بناء الجملة.

تحقق من وظيفة المستعرض من خلال فتح جلسة مستعرض ويب إلى EWM WebUI أو NGUI الذي تم تكوينه باستخدام TLSv1.3.

تم تكوين جميع مستعرضات الويب التي قمنا باختبارها بالفعل لقبول TLS v1.3.

- نموذج تعيين إعداد المستعرض على Firefox لتعطيل دعم TLS v1.3 ينتج عنه 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.



فشل TLS v1.3 Webui

- لضمان الاتصال، تحقق من إعدادات المستعرض للتأكد من تضمين TLSv1.3. (هذه العينة من Firefox)

- نموذج أمر openssl باستخدام قيمة تشفير غير مشفرة سيعطي هذا الخطأ إخراج: فشل إختبار اتصال OpenSSL العينة بسبب تشفير غير صالح: خطأ مع الأمر: "-ciphersuites TLS_AES_256_GCM_SHA386"

226823168:Error:1426E089:SSL routines:ciphersuite_cb:no cipher match:ssl/ssl_ciph.c:1299:

- ينتج أمر إنشاء نموذج إلى NG-ui عند تعطيل TLS v1.3 هذا الخطأ.

curl: (35) curl_sslversion_max غير متوافق مع curl_sslversion

معلومات ذات صلة

- جهاز إدارة أمان المحتوى من Cisco - ملاحظات الإصدار
- جهاز إدارة أمان المحتوى من Cisco - أدلة المستخدم النهائي

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).