TLSv1.3 configureren voor Secure Email Web Manager

Inhoud

Inleiding

Dit document beschrijft de configuratie van het TLS v1.3-protocol voor Cisco Secure Email and Web Manager (EWM)

Voorwaarden

Algemene kennis van de SEWM instellingen en configuratie is gewenst.

Gebruikte componenten

- Cisco Secure Email Web Manager (SEWM) AsyncOS 15.5.1 en nieuwer.
- SSL-configuratie-instellingen.

"De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, zorg er dan voor dat u de mogelijke impact van elke opdracht begrijpt."

Overzicht

SEWM heeft het TLS v1.3-protocol geïntegreerd om communicatie te versleutelen voor HTTPS-gerelateerde services; Classic UI, NGUI en Rest API.

TLS v1.3 Protocol biedt veiligere communicatie en snellere onderhandeling terwijl de industrie ernaar streeft de standaard te maken.

SEWM gebruikt de bestaande SSL Configuration methode binnen de SEGWebUIof CLI van SSL met een paar opmerkelijke instellingen om te markeren.

- Voorzorgsadvies bij het configureren van de toegestane protocollen.
- De TLS v1.3-algoritmen kunnen niet worden gemanipuleerd.
- TLS v1.3 kan alleen worden geconfigureerd voor GUI HTTPS.
- Met de selectieopties voor het TLS-protocol tussen TLS v1.0 en TLS v1.3 wordt een patroon gebruikt dat in het artikel meer in detail wordt weergegeven.

Configureren

Het SEWM-protocol TLS v1.3 voor HTTPS is geïntegreerd in AsycOS 15.5.

Voorzichtigheid is geboden bij het kiezen van de protocolinstellingen om HTTPS-falen te voorkomen.

Web Browser ondersteuning voor TLS v1.3 is algemeen, hoewel sommige omgevingen aanpassingen vereisen om toegang te krijgen tot het SEWM.

De Cisco SEWM-implementatie van het TLS v1.3 Protocol ondersteunt 3 standaardalgoritmen die niet binnen het SEWM kunnen worden gewijzigd of uitgesloten.

TLS 1.3-algoritmen:

TLS_AES_256_GCM_SHA384

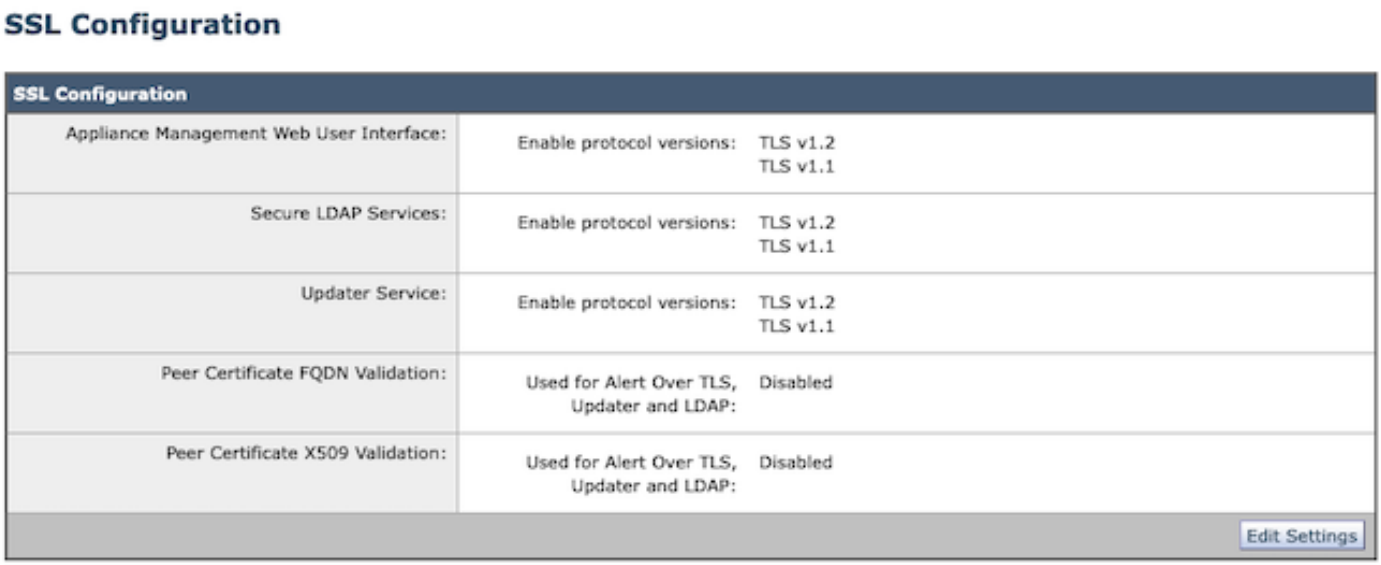
TLS_CHACHA20_POLY1305_SHA256

TLS_AES_128_GCM_SHA256

Configuratie via WebUI

Navigeren naar > Systeembeheer > SSL-configuratie

- De standaard TLS Protocol selectie post upgrade naar 15.5 AsyncOS HTTPS omvat alleen TLS v1.1 en TLS v1.2.
- De twee vermelde extra services, Secure LDAP-services en Updater-services, ondersteunen TLS v1.3 niet.

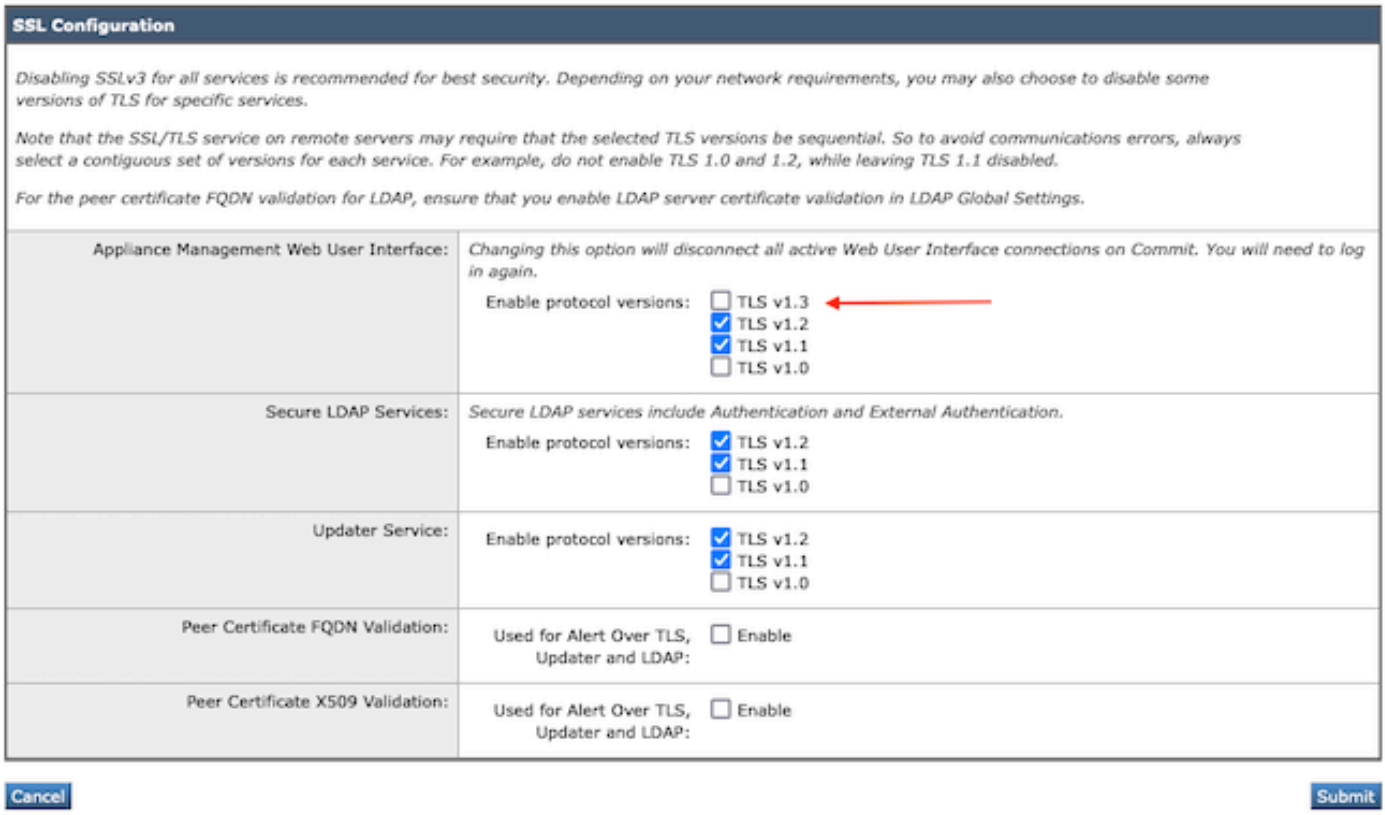


Selecteer "Instellingen bewerken" om de configuratieopties weer te geven.

De opties voor de protocolselectie van TLS voor "Web User Interface," omvatten TLS v1.0, TLS

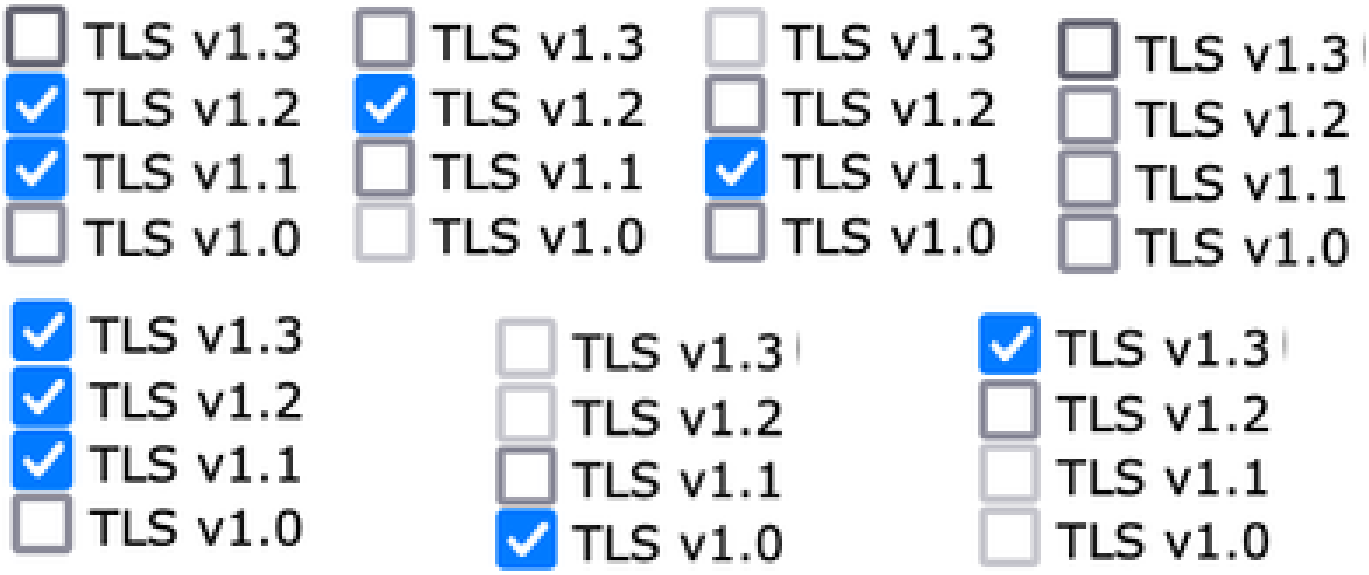
v1.1, TLS v1.2 en TLS v1.3.

- Na de upgrade naar AsyncOS 15.5 worden standaard alleen TLS v1.1- en TLS v1.2-protocollen geselecteerd.

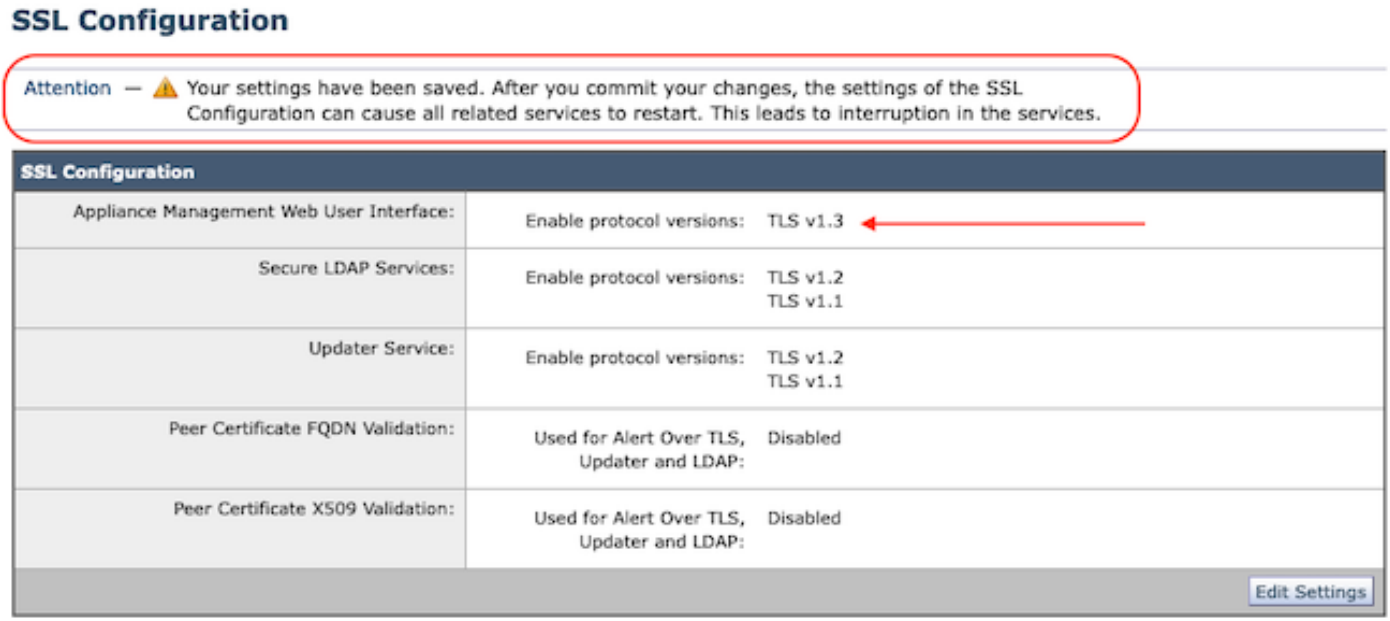


Opmerking: TLS1.0 wordt standaard afgekeurd en uitgeschakeld. TLS v1.0 is nog steeds beschikbaar als de eigenaar ervoor kiest deze in te schakelen.

- De opties voor het aanvinkvakje worden weergegeven met vetgedrukte vakken waarin de beschikbare protocollen en de grijswaarden voor niet-compatibele opties worden weergegeven.
- De voorbeeldopties in de afbeelding illustreren de opties voor het selectievakje van de webgebruikersinterface.



Opmerking: Aanpassingen in de SSL-configuratie kunnen ertoe leiden dat gerelateerde services opnieuw worden gestart. dit veroorzaakt een korte onderbreking van de WebUI-service.



Configuratie vanaf CLI

Het EWM maakt TLS v1.3 op één service mogelijk: WebUI

sma1.example.com> sslconfig

SSLv3 uitschakelen wordt aanbevolen voor de beste beveiliging.

Let op dat de SSL/TLS service op externe servers vereist dat de geselecteerde TLS versies sequentieel zijn. Dus om communicatiefouten te voorkomen, selecteert u altijd een aaneengesloten

reeks versies voor elke dienst. Schakel TLS 1.0 en 1.2 bijvoorbeeld niet in terwijl TLS 1.1 uitgeschakeld blijft.

Kies de bewerking die u wilt uitvoeren:
- VERSIES - SSL/TLS-versies in- of uitschakelen
- PEER_CERT_FQDN - Valideren van peer-certificaat FQDN-naleving voor Alert over TLS, updater en LDAP.
- PEER_CERT_X509 - Valideren peer certificaat X509 compliance voor Alert over TLS, updater en LDAP.
[]> versies

SSL/TLS-versie voor de services in- of uitschakelen:

Updater - updateservice
WebUI - gebruikersinterface voor applicatiebeheer
LDAPS - Beveiligde LDAP-services (inclusief verificatie en externe verificatie)

Merk op dat TLSv1.3 niet beschikbaar is voor Updater en LDAPS, kan alleen WebUI worden geconfigureerd met TLSv1.3.

Huidige SSL/TLS-versies ingeschakeld per service: (Y: ingeschakeld, N: uitgeschakeld)

Updater WebUI LDAPS
TLSv1.0 N N N
TLSv1.1 Y N
TLSv1.2 Y Y
TLSv1.3

Selecteer de service waarvoor SSL/TLS-versies in/uit moeten schakelen:

1. Update
2. WebUI
3. LDAPS
4. Alle diensten
[]> 2

Momenteel ingeschakeld protocol(s) voor WebUI zijn TLSv1.2.

Als u de instelling voor een specifiek protocol wilt wijzigen, selecteert u een van de onderstaande opties:

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

De ondersteuning van TLSv1.3 voor de gebruikersinterface voor Toepassingsbeheer is momenteel uitgeschakeld. Wilt u deze inschakelen? [N]> y

Op dit moment ingeschakelde protocollen voor WebUI zijn TLSv1.3 en TLSv1.2.

Kies de bewerking die u wilt uitvoeren:
- VERSIES - SSL/TLS-versies in- of uitschakelen
- PEER_CERT_FQDN - Valideer de naleving van het peer- certificaat FQDN voor Alert over TLS, updater, en LDAP.
- PEER_CERT_X509 - Valideren peer certificaat X509 naleving voor Alert over TLS, updater, en LDAP.
[]>

sma1.example.com> commit

Waarschuwing: veranderingen in SSL-configuratie veroorzaken de
deze processen opnieuw op gang te brengen na Commit - gui,euq_webui.
Dit veroorzaakt een korte onderbreking in SMA-operaties.

Voer een aantal opmerkingen in waarin uw wijzigingen worden beschreven:
[]> TLS v1.3 inschakelen

Wijzigingen vastgelegd: Sun Jan 28 23:55:40 2024 EST
Kaart bijwerken...
gui opnieuw opgestart
Lijst wordt bijgewerkt...
euq_webui opnieuw opgestart

Wacht een korte tijd en bevestig dat de WebUI toegankelijk is.

Opmerking: voor het selecteren van meerdere versies van TLS voor een service moet de gebruiker een service en een protocolversie selecteren en moet u de selectie van een service en een protocol nogmaals herhalen totdat alle instellingen zijn gewijzigd.

Verifiëren

Deze sectie omvat sommige basistestscenario's en de fouten die toe te schrijven aan slecht gecombineerde versies of syntaxisfouten voorleggen.

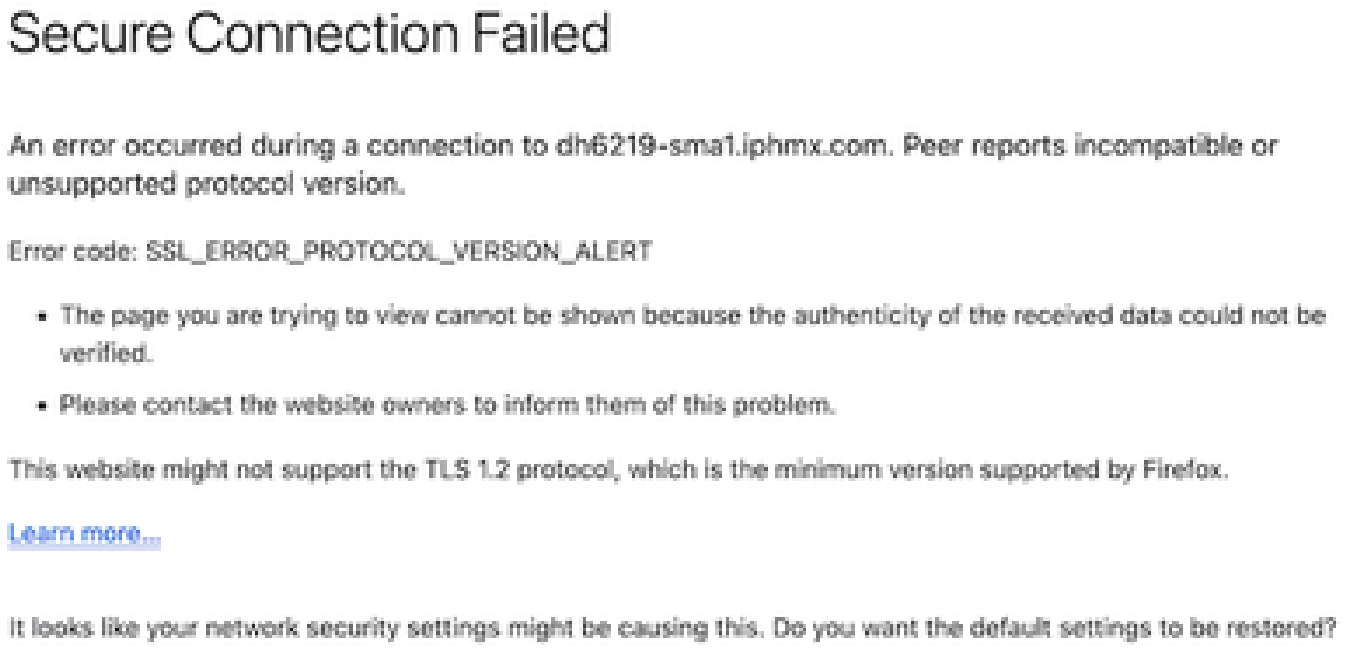
Controleer de functionaliteit van de browser door een webbrowsersessie te openen naar de EWM WebUI of NGUI geconfigureerd met TLSv1.3.

Alle geteste webbrowsers zijn al geconfigureerd om TLS v1.3 te accepteren.

- Steekproefset van de browser instelling op Firefox om TLS v1.3 ondersteuning uit te

schakelen, geeft fouten op zowel de ClassicUI als de NGUI van het apparaat.

- Classic UI met Firefox geconfigureerd om TLS v1.3 uit te sluiten als test.
- NGUI zou dezelfde fout ontvangen met als enige uitzondering het poortnummer 4431 (standaard) binnen de URL.



TLS v1.3 Webex-fout

- Om de communicatie te verzekeren Controleer de instellingen van de browser om te verzekeren dat TLSv1.3 is opgenomen. (Dit voorbeeld komt uit Firefox)

- Voorbeeld openssl opdracht met behulp van een verkeerd getypte algoritme waarde zou deze fout output geven: sample openssl verbinding test fout te wijten aan ongeldige algoritme: Error met commando: "-ciphersuites TLS_AES_256_GCM_SHA386"

2226823168:ERROR:1426E089:SSL-routines:ciphersuite_cb:geen overeenkomend algoritme:ssl/ssl_ciph.c:1299:

- Als deze fout wordt gegenereerd, wordt de voorbeeldopdracht voor krullen uitgevoerd naar de ng-ui als TLS v1.3 is uitgeschakeld.

curl: (35) CURL_SSLVERSIE_MAX niet compatibel met CURL_SSLVERSIE

Gerelateerde informatie

- Cisco Content Security Management-applicatie - Releaseopmerkingen

- Cisco Content Security Management-applicatie - eindgebruikershandleidingen

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.