Configuration de TLSv1.3 pour Secure Email Web Manager

Table des matières

Introduction

Ce document décrit la configuration du protocole TLS v1.3 pour Cisco Secure Email and Web Manager (EWM)

Conditions préalables

Une connaissance générale des paramètres et de la configuration du module SEWM est souhaitée.

Composants utilisés

- Cisco Secure Email Web Manager (SEWM) AsyncOS 15.5.1 et versions ultérieures.
- Paramètres de configuration SSL.

"Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est actif, assurez-vous de comprendre l'impact potentiel de toute commande. »

Aperçu

Le module SEWM a intégré le protocole TLS v1.3 pour chiffrer les communications pour les services associés au protocole HTTPS ; Interface utilisateur classique, interface NGUI et API de repos.

Le protocole TLS v1.3 offre des communications plus sécurisées et des négociations plus rapides, car l'industrie s'efforce d'en faire la norme.

Le SEWM utilise la méthode de configuration SSL existante dans le SEGWebUIor CLI de SSL avec quelques paramètres notables à mettre en évidence.

- Conseils de prudence lors de la configuration des protocoles autorisés.
- Impossible de manipuler les chiffrements TLS v1.3.
- TLS v1.3 peut uniquement être configuré pour HTTPS de l'interface utilisateur graphique.
- Les options de sélection de la case à cocher du protocole TLS entre TLS v1.0 et TLS v1.3 utilisent un modèle illustré plus en détail dans l'article.

Configurer

Le module SEWM a intégré le protocole TLS v1.3 pour HTTPS dans AsycOS 15.5.

Il est recommandé de faire preuve de prudence lors du choix des paramètres de protocole pour éviter une défaillance HTTPS.

La prise en charge du navigateur Web pour TLS v1.3 est courante, bien que certains environnements nécessitent des ajustements pour accéder au module SEWM.

L'implémentation Cisco SEWM du protocole TLS v1.3 prend en charge 3 chiffrements par défaut qui ne peuvent pas être modifiés ou exclus dans le SEWM.

Chiffres TLS 1.3 :

TLS_AES_256_GCM_SHA384

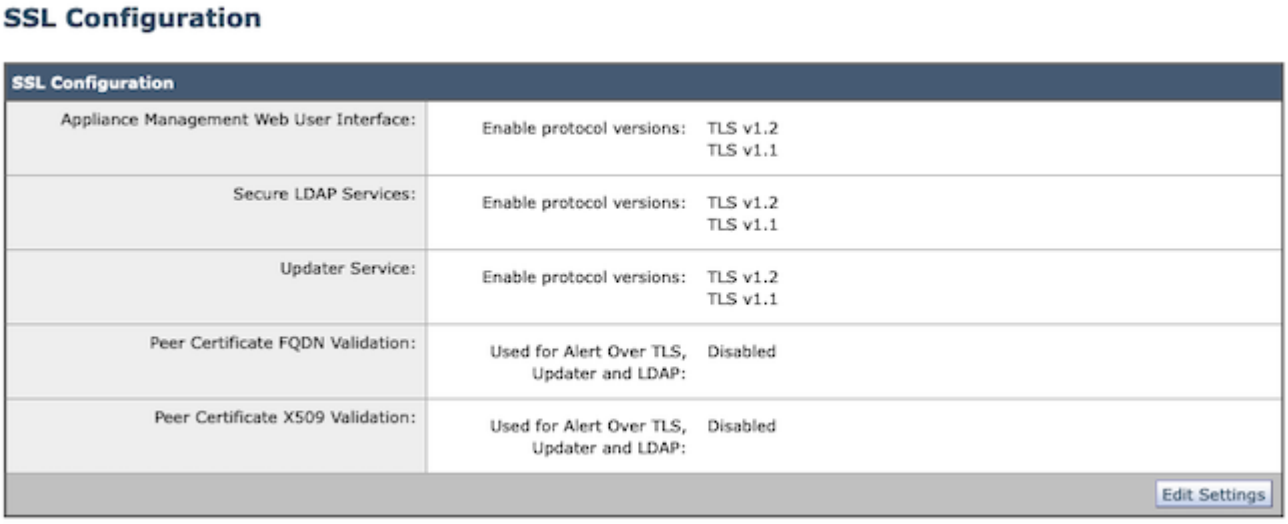
TLS_CHACHA20_POLY1305_SHA256

TLS_AES_128_GCM_SHA256

Configuration à partir de WebUI

Accédez à **>** Administration système **>** Configuration SSL

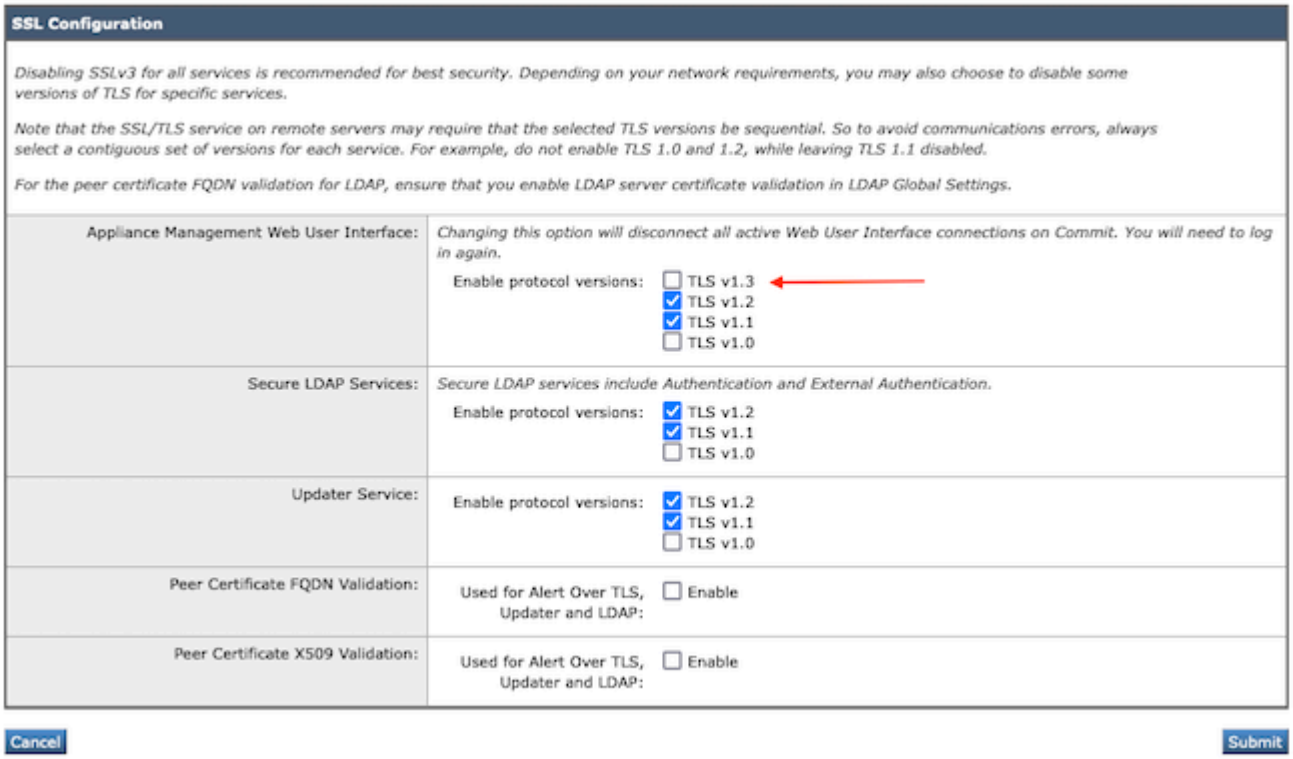
- La sélection du protocole TLS par défaut après la mise à niveau vers 15.5 AsyncOS HTTPS inclut TLS v1.1 et TLS v1.2 uniquement.
- Les deux services supplémentaires répertoriés, Secure LDAP Services et Updater Services, ne prennent pas en charge TLS v1.3.



Sélectionnez « Modifier les paramètres » pour présenter les options de configuration.

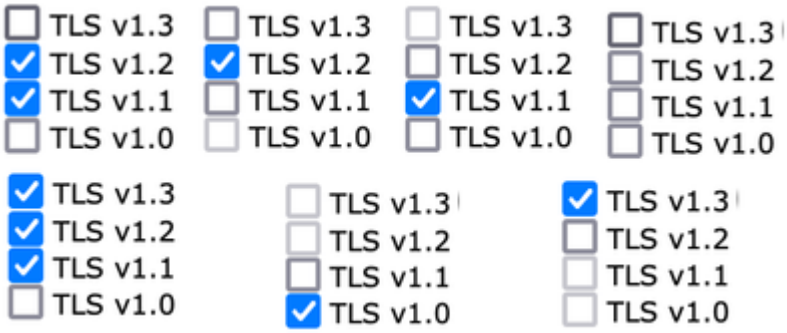
Les options de sélection du protocole TLS pour « Interface utilisateur Web » incluent TLS v1.0, TLS v1.1, TLS v1.2 et TLS v1.3.

- Après la mise à niveau vers AsyncOS 15.5, seuls les protocoles TLS 1.1 et TLS 1.2 sont sélectionnés par défaut.

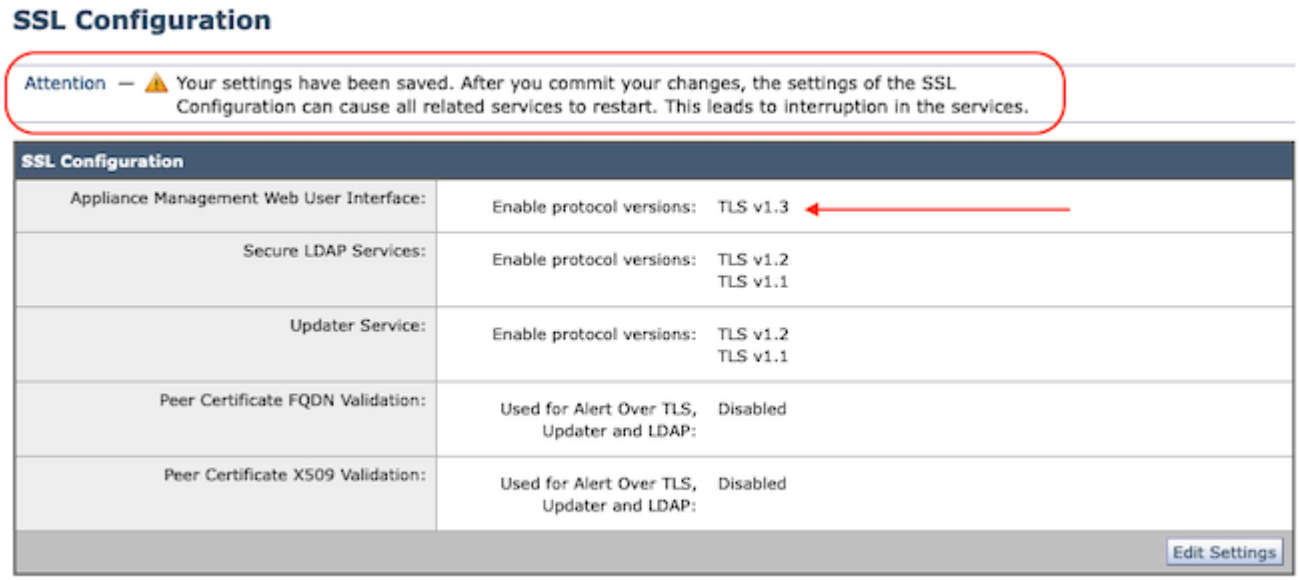


Remarque : TLS1.0 est déconseillé et donc désactivé par défaut. TLS v1.0 est toujours disponible si le propriétaire choisit de l'activer.

- Les cases à cocher s'affichent avec des cases en gras présentant les protocoles disponibles et les cases grisées pour les options non compatibles.
- Les exemples d'options de l'image illustrent les options de case à cocher de l'interface utilisateur Web.



Remarque : Les modifications apportées à la configuration SSL peuvent entraîner le redémarrage des services associés. elle provoque une brève interruption du service WebUI.



Configuration à partir de CLI

Le module EWM autorise TLS v1.3 sur un service : interface utilisateur Web

sma1.exemple.com> sslconfig

La désactivation de SSLv3 est recommandée pour une sécurité optimale.

Notez que le service SSL/TLS sur les serveurs distants nécessite que les versions TLS sélectionnées soient séquentielles. Pour éviter les erreurs de communication, sélectionnez toujours un
ensemble de versions pour chaque service. Par exemple, n'activez pas TLS 1.0 et 1.2, tout en laissant TLS 1.1 désactivé.

Sélectionnez l'opération que vous souhaitez effectuer :
- VERSIONS - Activer ou désactiver les versions SSL/TLS
- PEER_CERT_FQDN - Validez la conformité FQDN du certificat homologue pour Alert Over TLS, Updater et LDAP.
- PEER_CERT_X509 - Validez la conformité du certificat homologue X509 pour Alert Over TLS, Updater et LDAP.
[]> versions

Activez ou désactivez la version SSL/TLS pour les services :

Updater - Service de mise à jour
WebUI - Interface utilisateur Web de gestion des appareils
LDAPS - Services LDAP sécurisés (y compris l'authentification et l'authentification externe)

Notez que TLSv1.3 n'est pas disponible pour Updater et LDAPS, seul WebUI peut être configuré avec TLSv1.3.

Versions SSL/TLS actuellement activées par service : (O: Activé, N : Désactivé)

Mise à jour WebUI LDAPS
TLSv1.0 N N N
TLSv1.1 Y N Y
TLSv1.2 Y Y Y
TLSv1.3 S/O S/O

Sélectionnez le service pour lequel activer/désactiver les versions SSL/TLS :

1. Mise à jour
2. Interface utilisateur Web
3. PADL
4. Tous les services
[]> 2

Les protocoles actuellement activés pour WebUI sont TLSv1.2.

Pour modifier le paramètre d'un protocole spécifique, sélectionnez une option ci-dessous :

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

La prise en charge de TLSv1.3 pour l'interface utilisateur Web de gestion du matériel est actuellement désactivée. Voulez-vous l'activer ? [N]> o

Les protocoles actuellement activés pour WebUI sont TLSv1.3 et TLSv1.2.

Sélectionnez l'opération que vous souhaitez effectuer :
- VERSIONS - Activer ou désactiver les versions SSL/TLS
- PEER_CERT_FQDN - Valide la conformité FQDN du certificat homologue pour Alert Over TLS, Updater et LDAP.
- PEER_CERT_X509 - Validez la conformité du certificat homologue X509 pour Alert Over TLS, Updater et LDAP.
[]>

sma1.exemple.com> commit

Avertissement : Les modifications apportées à la configuration SSL entraînent
ces processus doivent redémarrer après Commit - gui, euq_webui.
Cela entraîne une brève interruption des opérations SMA.

Veuillez saisir des commentaires décrivant vos modifications :
[]> activer tls v1.3

Modifications validées : Dim Jan 28 23:55:40 2024 HNE
Redémarrage de l'interface graphique...
gui redémarré
Redémarrage de euq_webui...
euq_webui redémarré

Patientez quelques instants et vérifiez que l'interface Web est accessible.

Remarque : Pour sélectionner plusieurs versions de TLS pour un service, l'utilisateur doit sélectionner un service et une version de protocole, puis répéter la sélection d'un service et d'un protocole jusqu'à ce que tous les paramètres aient été modifiés.

Vérifier

Cette section inclut quelques scénarios de test de base et les erreurs qui se présentent en raison de versions incompatibles ou d'erreurs de syntaxe.

Vérifiez le fonctionnement du navigateur en ouvrant une session de navigateur Web sur l'interface utilisateur Web EWM ou l'interface utilisateur de nouvelle génération configurée avec TLSv1.3.

Tous les navigateurs Web que nous avons testés sont déjà configurés pour accepter TLS v1.3.

- Exemple de définition du paramètre de navigateur sur Firefox pour désactiver la prise en charge TLS v1.3 produit des erreurs sur l'interface ClassicUI et l'interface NGUI de l'appliance.

- Interface utilisateur classique utilisant Firefox configurée pour exclure TLS v1.3, comme test.
- NGUI reçoit la même erreur, à la seule exception du numéro de port 4431 (par défaut) dans l'URL.



Échec de TLS v1.3 Webui

- Pour garantir la communication, vérifiez les paramètres du navigateur pour vous assurer que TLSv1.3 est inclus. (Cet exemple provient de Firefox)



- Un exemple de commande openssl utilisant une valeur de chiffrement mal tapée donnerait cette sortie d'erreur : exemple d'échec du test de connexion openssl dû à un chiffrement non valide : Erreur avec la commande : "-ciphersuites TLS_AES_256_GCM_SHA386"

2226823168:ERROR:1426E089:SSL routines:ciphersuite_cb:no cipher match:ssl/ssl_ciph.c:1299:

- L'exemple de commande curl exécutée sur l'interface ng-ui lorsque TLS v1.3 est désactivé génère cette erreur.

courbure : (35) CURL_SSLVERSION_MAX incompatible avec CURL_SSLVERSION

Informations connexes

- Appliance de gestion de la sécurité du contenu Cisco - Notes de version
- Cisco Content Security Management Appliance - Guides d'utilisation

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.