Configuración de TLSv1.3 para Secure Email Web Manager

Contenido

Introducción

Este documento describe la configuración del protocolo TLS v1.3 para Cisco Secure Email and Web Manager (EWM)

Prerequisites

Se requiere un conocimiento general de los ajustes y la configuración de SEWM.

Componentes Utilizados

- Cisco Secure Email Web Manager (SEWM) AsyncOS 15.5.1 y versiones posteriores.
- Parámetros de configuración de SSL.

"La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está activa, asegúrese de comprender el impacto potencial de cualquier comando".

Overview

El SEWM ha integrado el protocolo TLS v1.3 para cifrar las comunicaciones de los servicios relacionados con HTTPS: interfaz de usuario clásica, NGUI y API de resto.

El protocolo TLS v1.3 presume de una comunicación más segura y una negociación más rápida a medida que el sector se esfuerza por convertirlo en el estándar.

El SEWM utiliza el método de configuración SSL existente dentro de SEGWebUIo CLI de SSL con algunas configuraciones notables para resaltar.

- Consejos de precaución al configurar los protocolos permitidos.
- Los cifrados TLS v1.3 no se pueden manipular.
- TLS v1.3 se puede configurar solo para HTTPS de la GUI.
- Las opciones de selección de la casilla de verificación del protocolo TLS entre TLS v1.0 y TLS v1.3 utilizan un patrón ilustrado con más detalle en el artículo.

Configurar

El SEWM ha integrado el protocolo TLS v1.3 para HTTPS dentro de AsycOS 15.5.

Se recomienda precaución al elegir la configuración del protocolo para evitar un fallo de HTTPS.

La compatibilidad con el explorador web para TLS v1.3 es común, aunque algunos entornos requieren ajustes para acceder a SEWM.

La implementación de Cisco SEWM del protocolo TLS v1.3 admite 3 cifrados predeterminados que no se pueden cambiar ni excluir dentro del SEWM.

Cifrados TLS 1.3:

TLS_AES_256_GCM_SHA384

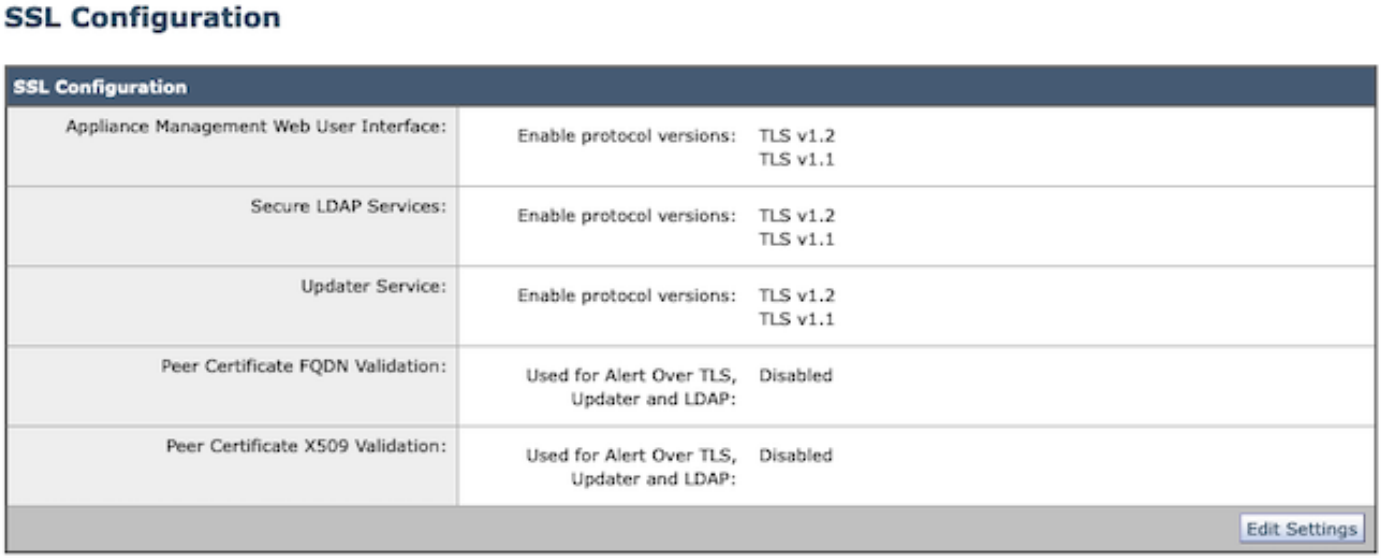
TLS_CHACHA20_POLY1305_SHA256

TLS_AES_128_GCM_SHA256

Configuración desde la interfaz de usuarioWeb

Vaya a > Administración del sistema > Configuración de SSL

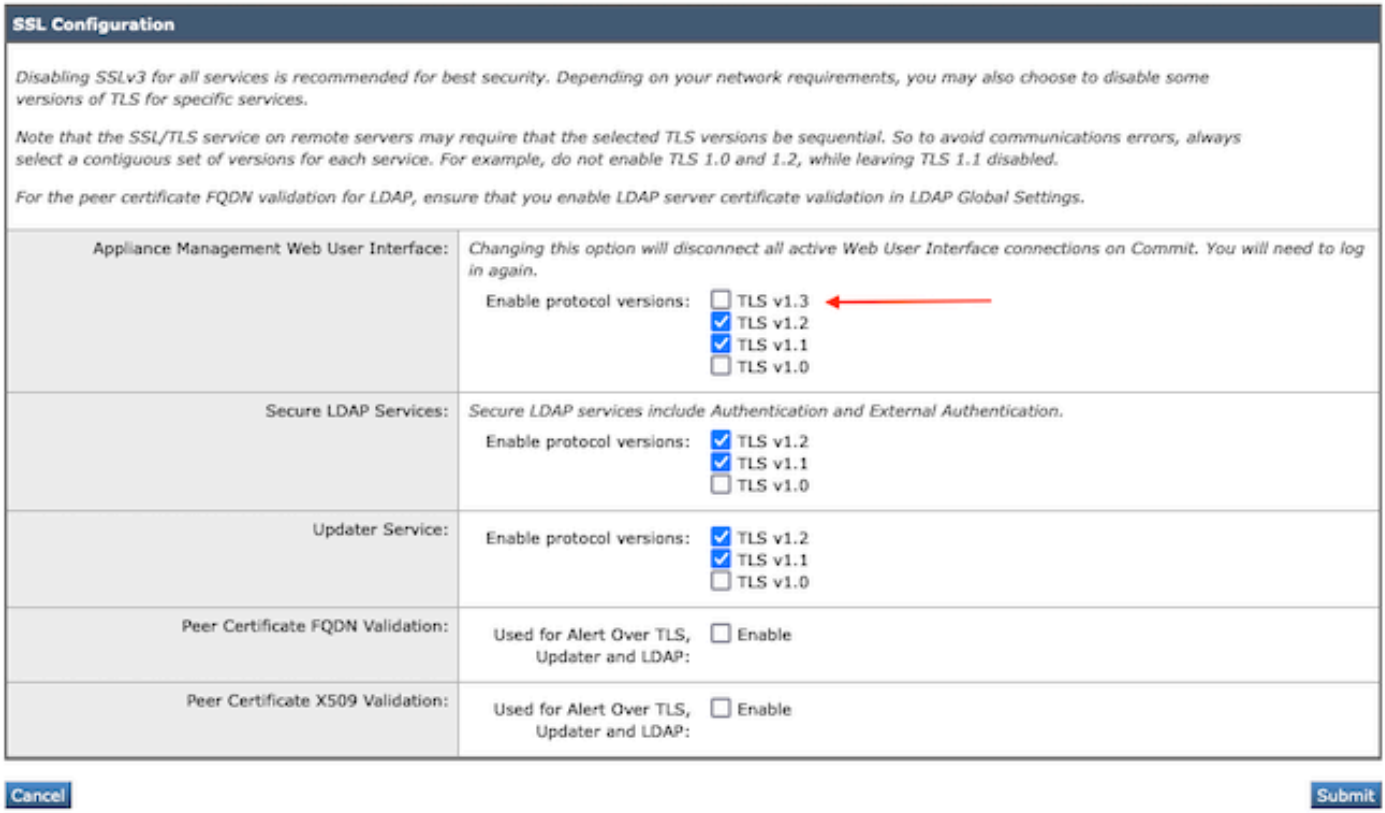
- La selección predeterminada del protocolo TLS después de la actualización a HTTPS de AsyncOS 15.5 incluye solo TLS v1.1 y TLS v1.2.
- Los dos servicios adicionales enumerados, Servicios LDAP seguros y Servicios de actualización, no admiten TLS v1.3.



Seleccione "Editar configuración" para presentar las opciones de configuración.

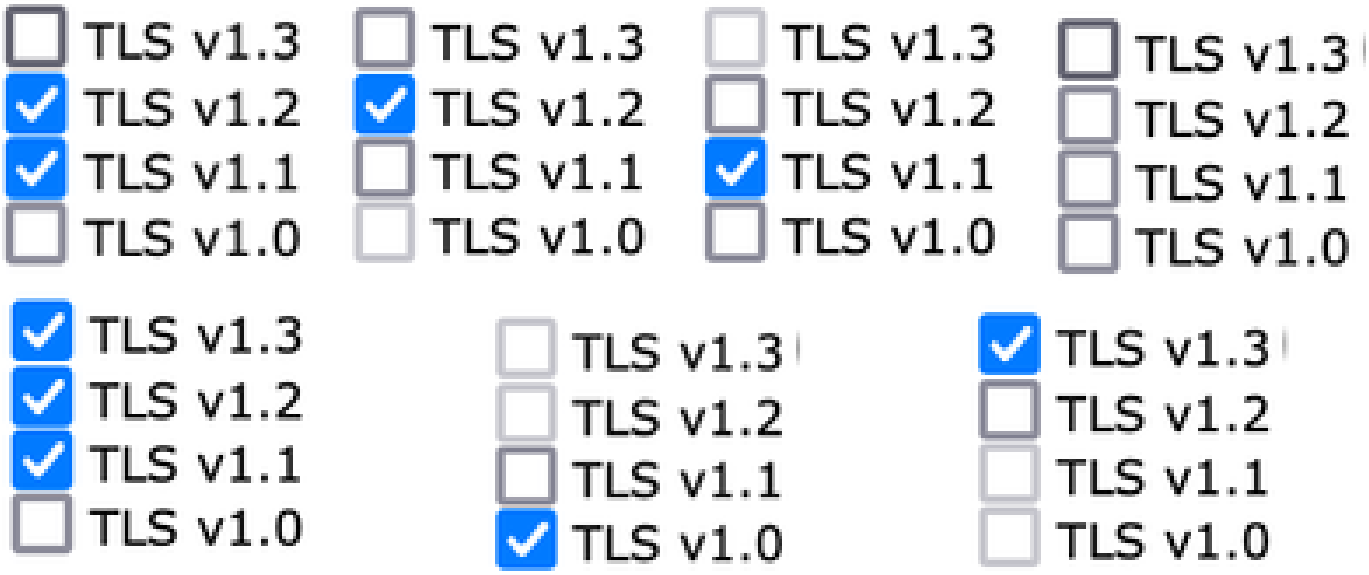
Las opciones de selección del protocolo TLS para "Interfaz de usuario web" incluyen TLS v1.0, TLS v1.1, TLS v1.2 y TLS v1.3.

- Tras la actualización a AsyncOS 15.5, solo los protocolos TLS v1.1 y TLS v1.2 están seleccionados de forma predeterminada.

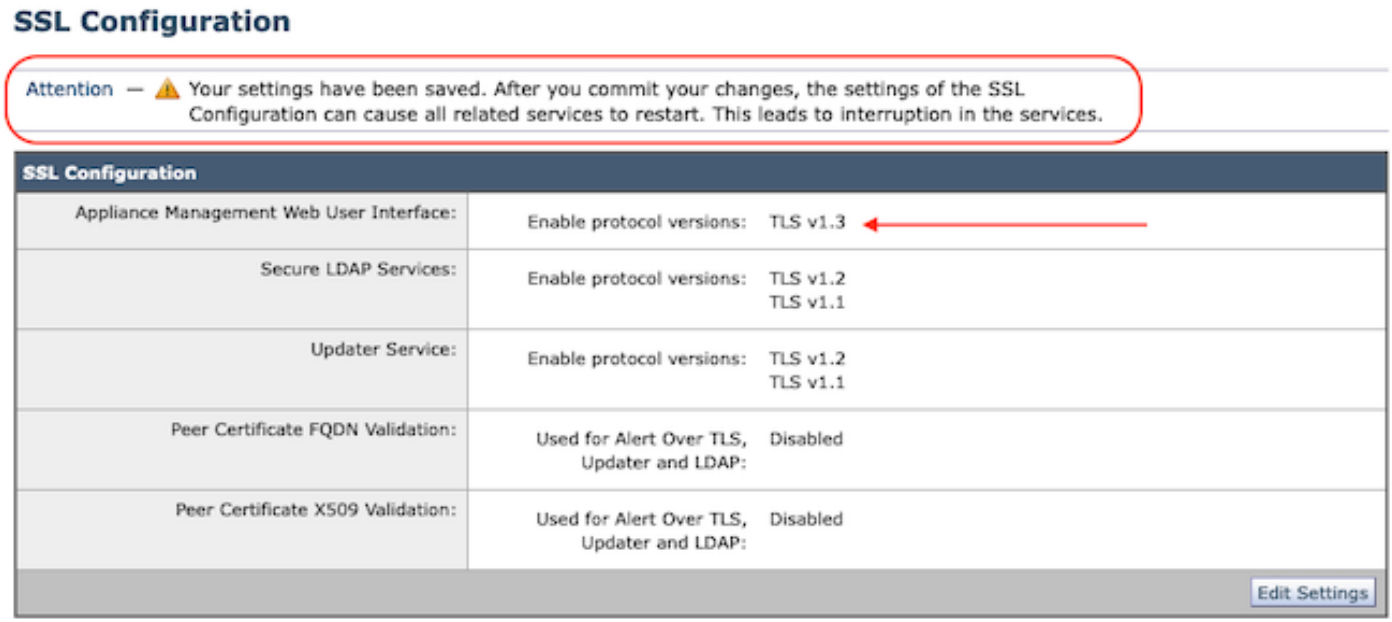


Nota: TLS1.0 está obsoleto y, por lo tanto, está deshabilitado de forma predeterminada. TLS v1.0 sigue estando disponible si el propietario decide activarlo.

- Las opciones de la casilla de verificación se iluminan con cuadros en negrita que presentan los cuadros Protocolos disponibles y Atenuados para las opciones no compatibles.
- Las opciones de ejemplo de la imagen ilustran las opciones de casilla de verificación para la interfaz de usuario Web.



Nota: Las modificaciones en la configuración SSL pueden hacer que se reinicien los servicios relacionados. Esto provoca una breve interrupción del servicio WebUI.



Configuración desde CLI

El EWM permite TLS v1.3 en un servicio: WebUI

sma1.ejemplo.com> sslconfig

Se recomienda desactivar SSLv3 para obtener la mejor seguridad.

Tenga en cuenta que el servicio SSL/TLS de los servidores remotos requiere que las versiones de TLS seleccionadas sean secuenciales. Por lo tanto, para evitar errores de comunicación, seleccione siempre un
conjunto de versiones para cada servicio. Por ejemplo, no habilite TLS 1.0 y 1.2, mientras deja TLS 1.1 inhabilitado.

Elija la operación que desea realizar:
- VERSIONES - Activar o desactivar las versiones SSL/TLS
- PEER_CERT_FQDN - Validar el cumplimiento de FQDN del certificado de peer para Alert Over TLS, Updater y LDAP.
- PEER_CERT_X509 - Validar el cumplimiento del certificado de peer X509 para Alert Over TLS, Updater y LDAP.
[]> versiones

Habilitar o deshabilitar la versión SSL/TLS para los servicios:

Actualizador - Servicio de actualización
WebUI - Interfaz de usuario web de administración de dispositivos
LDAPS - Servicios LDAP seguros (incluidos autenticación y autenticación externa)

Tenga en cuenta que TLSv1.3 no está disponible para Updater y LDAPS, solo WebUI se puede configurar con TLSv1.3.

Versiones SSL/TLS habilitadas actualmente por servicio: (S: habilitado, N: deshabilitado)

LDAPS de WebUI del actualizador
TLSv1.0 N N N
TLSv1.1 Y N Y
TLSv1.2 Y Y
TLSv1.3 N/A N/A

Seleccione el servicio para el que desea activar/desactivar las versiones SSL/TLS:

1. Actualizador
2. InterfazWeb
3. PADP
4. Todos los servicios
[]> 2

Los protocolos habilitados actualmente para WebUI son TLSv1.2.

Para cambiar la configuración de un protocolo específico, seleccione una de las siguientes opciones:

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

La compatibilidad con TLSv1.3 para la interfaz de usuario web de administración de dispositivos está deshabilitada actualmente. ¿Desea activarla? [N]> y

Los protocolos habilitados actualmente para WebUI son TLSv1.3 y TLSv1.2.

Elija la operación que desea realizar:
- VERSIONES - Activar o desactivar las versiones SSL/TLS
- PEER_CERT_FQDN - Validar el cumplimiento de FQDN del certificado de peer para Alert Over TLS, Updater y LDAP.
- PEER_CERT_X509 - Validar el cumplimiento del certificado de peer X509 para Alert Over TLS, Updater y LDAP.
[]>

sma1.ejemplo.com> commit

Advertencia: los cambios en la configuración de SSL provocan el
estos procesos se reiniciarán después de Commit - gui,euq_webui.
Esto provoca una breve interrupción en las operaciones de SMA.

Introduzca algunos comentarios que describan los cambios:
[]> enable tls v1.3

Cambios realizados: Dom Ene 28 23:55:40 2024 EST
Reiniciando GUI...
GUI reiniciado
Reiniciando euq_webui...
euq_webui reiniciado

Espere un momento y confirme que WebUI está accesible.

Nota: Para seleccionar varias versiones de TLS para un servicio, el usuario debe seleccionar un servicio y una versión de protocolo y, a continuación, repetir la selección de un servicio y un protocolo una vez más hasta que se hayan modificado todos los parámetros.

Verificación

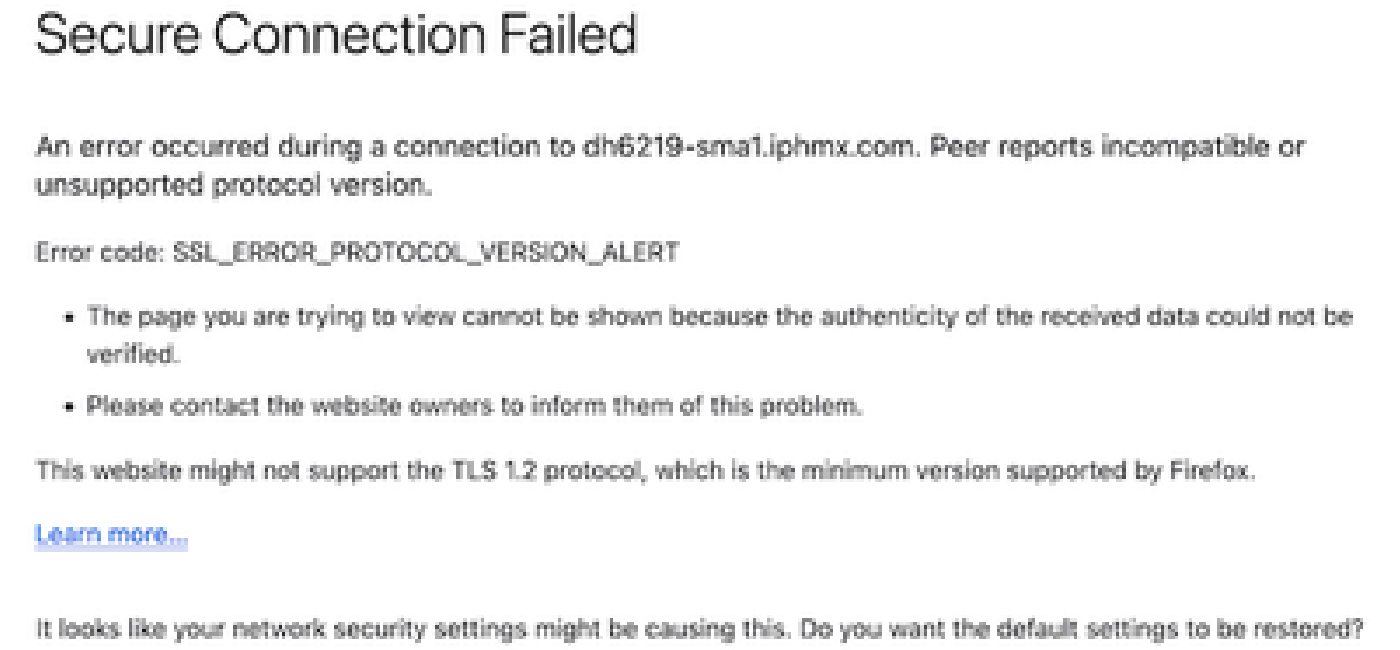
Esta sección incluye algunos escenarios de prueba básicos y los errores que se producen debido a versiones no coincidentes o a errores de sintaxis.

Verifique la funcionalidad del explorador abriendo una sesión del explorador Web en la interfaz de usuario Web o NGUI de EWM configurada con TLSv1.3.

Todos los exploradores web que probamos ya están configurados para aceptar TLS v1.3.

- Ejemplo de configuración del navegador en Firefox para deshabilitar la compatibilidad con TLS v1.3 produce errores tanto en la interfaz de usuario clásica como en la interfaz de usuario de última generación del dispositivo.

- Interfaz de usuario clásica con Firefox configurado para excluir TLS v1.3, como prueba.
- NGUI recibiría el mismo error con la única excepción del número de puerto 4431 (predeterminado) dentro de la URL.



Falla de TLS v1.3 en WebBui

- Para garantizar la comunicación, compruebe la configuración del explorador para asegurarse de que se incluye TLSv1.3. (Este ejemplo es de Firefox)

- El comando openssl de ejemplo que usa un valor de cifrado mal escrito daría este resultado de error: ejemplo de falla de prueba de conexión openssl debido a cifrado no válido: Error con el comando: "-ciphersuites TLS_AES_256_GCM_SHA386"

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

- El comando curl de ejemplo ejecutado en ng-ui cuando TLS v1.3 está inhabilitado genera este error.

curl: (35) CURL_SSLVERSION_MAX incompatible con CURL_SSLVERSION

Información Relacionada

- Cisco Content Security Management Appliance: notas de la versión
- Cisco Content Security Management Appliance: Guías para el usuario final

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).