Configurar TLSv1.3 para Secure Email Web Manager

Contents

Introdução

Este documento descreve a configuração do protocolo TLS v1.3 para o Cisco Secure Email and Web Manager (EWM)

Pré-requisitos

É desejável ter conhecimento geral das definições e da configuração do SEWM.

Componentes Utilizados

- Cisco Secure Email Web Manager (SEWM) AsyncOS 15.5.1 e mais recente.
- Definições de configuração de SSL.

"As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que você compreende o impacto potencial de qualquer comando."

Overview

O SEWM integrou o protocolo TLS v1.3 para criptografar comunicações para serviços relacionados a HTTPS; Classic UI, NGUI e Rest API.

O protocolo TLS v1.3 apresenta comunicação mais segura e negociação mais rápida à medida que o setor se esforça para torná-lo o padrão.

O SEWM usa o método de configuração SSL existente no SEGWebUI ou CLI do SSL com algumas configurações notáveis para destacar.

- Recomendações de precaução ao configurar os protocolos permitidos.
- As Cifras TLS v1.3 não podem ser manipuladas.
- O TLS v1.3 pode ser configurado somente para HTTPS com GUI.
- As opções de seleção da caixa de verificação do protocolo TLS entre TLS v1.0 e TLS v1.3 usam um padrão ilustrado em mais detalhes no artigo.

Configurar

O SEWM integrou o protocolo TLS v1.3 para HTTPS no AsycOS 15.5.

Recomenda-se cuidado ao escolher as configurações do protocolo para evitar falha de HTTPS.

O suporte do navegador da Web para TLS v1.3 é comum, embora alguns ambientes exijam ajustes para acessar o SEWM.

A implementação Cisco SEWM do protocolo TLS v1.3 suporta 3 cifras padrão que não podem ser alteradas ou excluídas dentro do SEWM.

Cifras TLS 1.3:

TLS_AES_256_GCM_SHA384

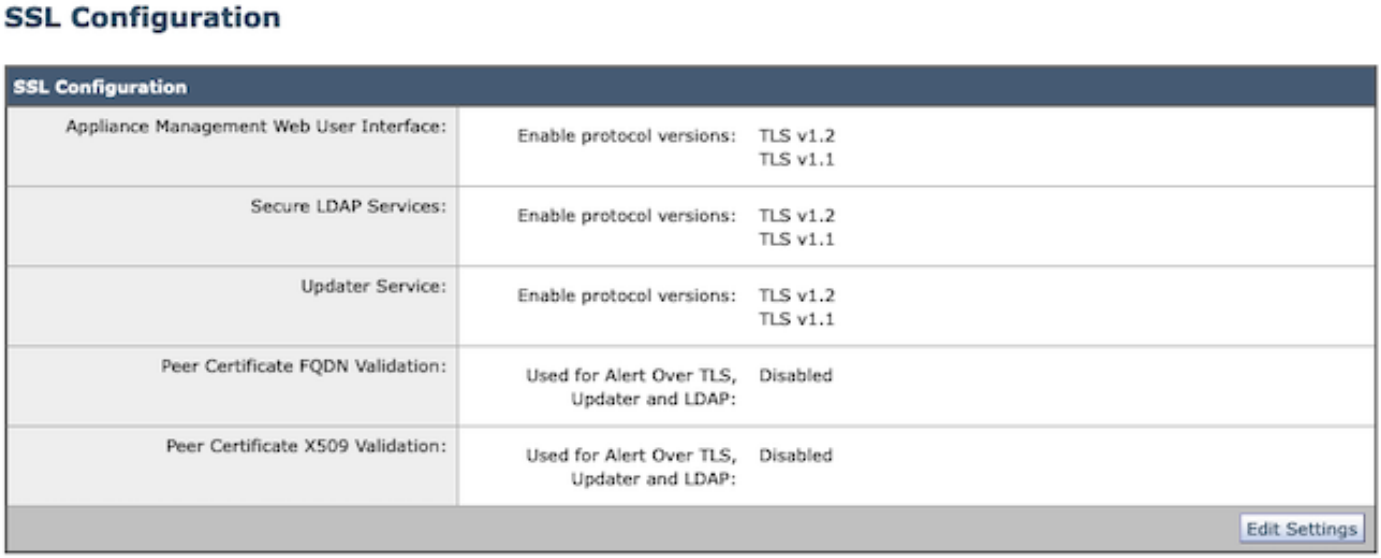
TLS_CHACHA20_POLY1305_SHA256

TLS_AES_128_GCM_SHA256

Configuração a partir da WebUI

Navegue até > Administração do sistema > Configuração de SSL

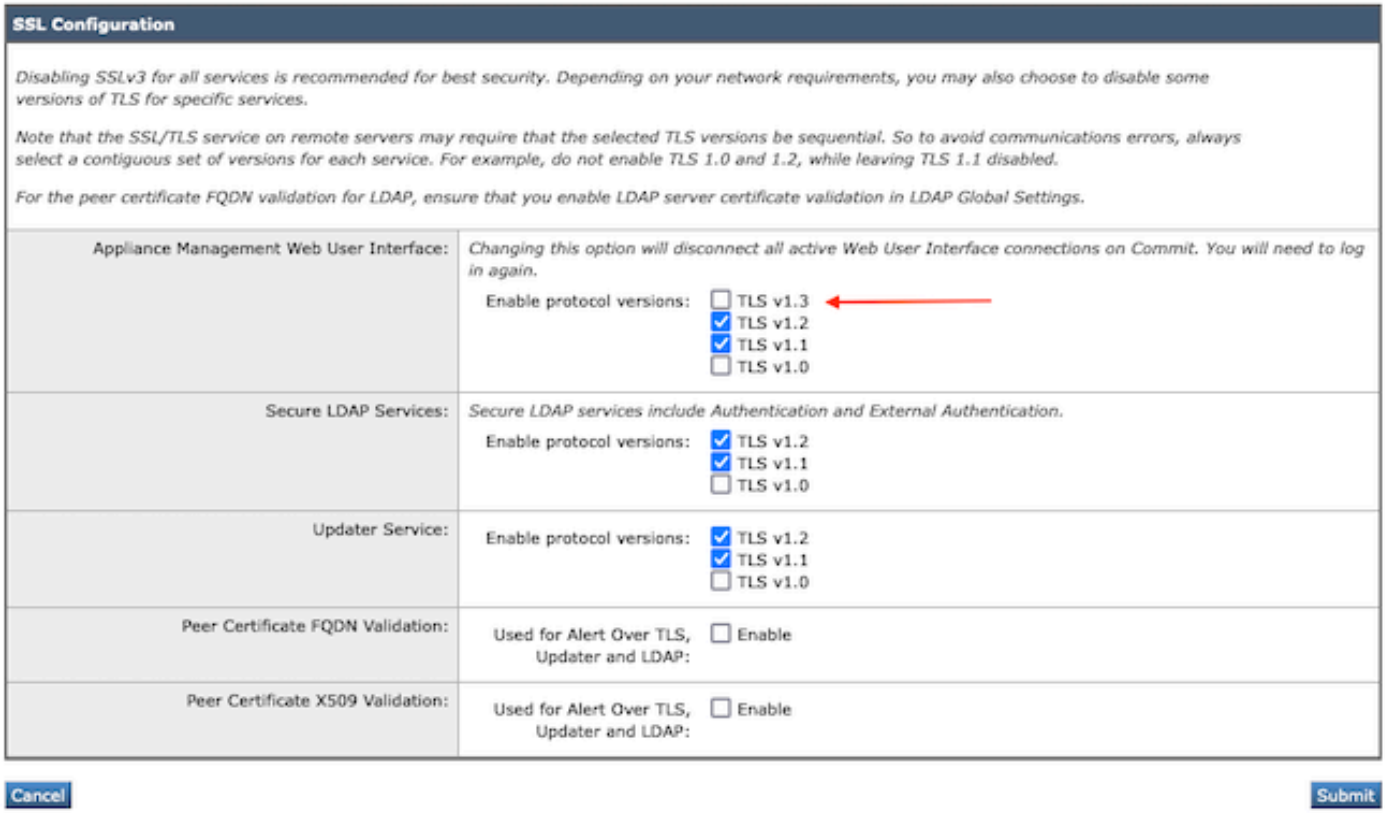
- A seleção padrão do protocolo TLS após a atualização para o AsyncOS HTTPS 15.5 inclui apenas TLS v1.1 e TLS v1.2.
- Os dois serviços adicionais listados, Secure LDAP Services e Updater Services, não suportam TLS v1.3.



Selecione "Edit Settings" (Editar configurações) para apresentar as opções de configuração.

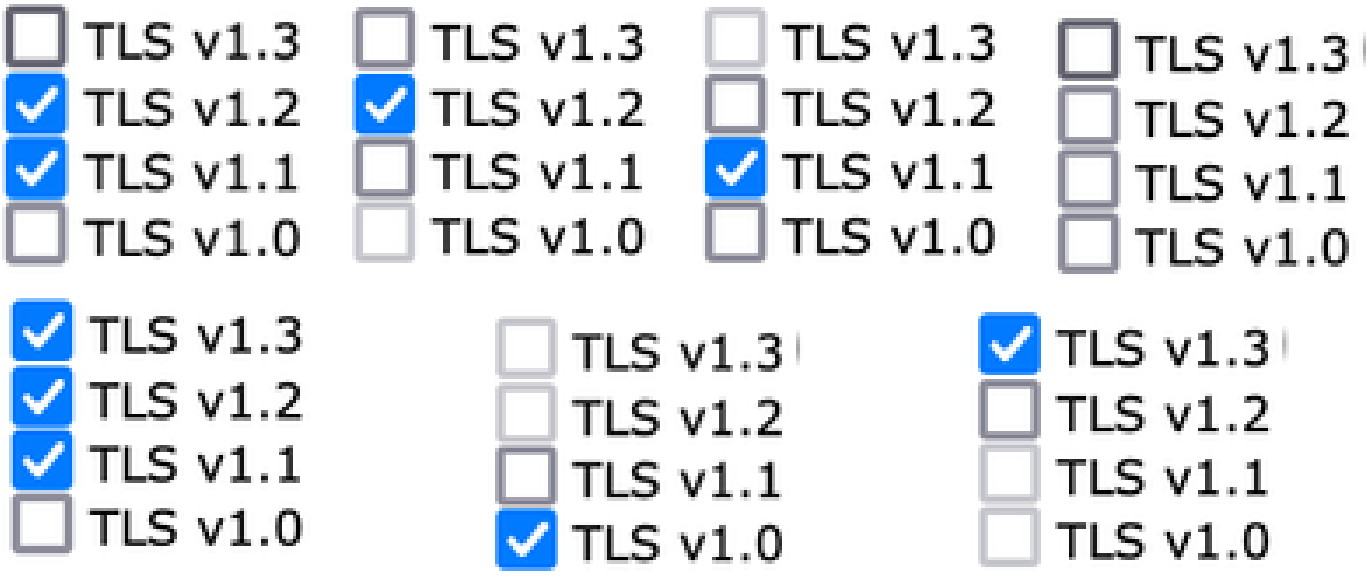
As opções de seleção do protocolo TLS para a "Interface de usuário da Web" incluem TLS v1.0, TLS v1.1, TLS v1.2 e TLS v1.3.

- Após a atualização para o AsyncOS 15.5, somente os protocolos TLS v1.1 e TLS v1.2 são selecionados por padrão.

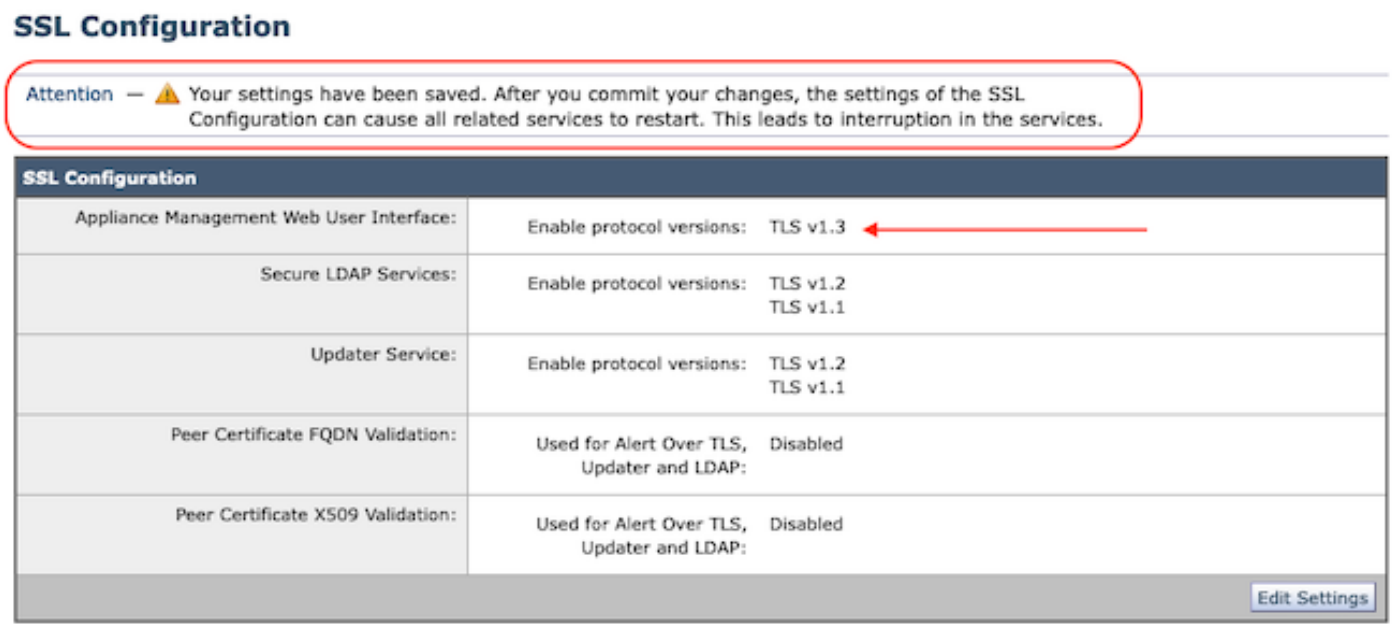


Observação: o TLS1.0 é preterido e, portanto, desabilitado por padrão. O TLS v1.0 ainda estará disponível se o proprietário optar por ativá-lo.

- As opções da caixa de seleção acendem com caixas em negrito, apresentando as caixas Protocolos disponíveis e Esmaecido, para opções incompatíveis.
- As opções de exemplo na imagem ilustram as opções da caixa de seleção para a Interface de usuário da Web.



Observação: Modificações na Configuração SSL podem fazer com que os serviços relacionados sejam reiniciados. Isso causa uma breve interrupção no Serviço WebUI.



Configuração a partir da CLI

O EWM permite TLS v1.3 em um serviço: WebUI

sma1.example.com> sslconfig

É recomendável desabilitar o SSLv3 para obter a melhor segurança.

Observe que o serviço SSL/TLS em servidores remotos exige que as versões TLS selecionadas sejam sequenciais. Para evitar erros de comunicação, sempre selecione um contíguo conjunto de versões para cada serviço. Por exemplo, não ative o TLS 1.0 e 1.2, deixando o TLS 1.1 desativado.

Escolha a operação que deseja executar:
- VERSIONS - Habilitar ou desabilitar versões de SSL/TLS
- PEER_CERT_FQDN - Valide a conformidade FQDN de certificado de mesmo nível para Alerta sobre TLS, atualizador e LDAP.
- PEER_CERT_X509 - Validar conformidade X509 de certificado de mesmo nível para Alerta sobre TLS, atualizador e LDAP.
[]> versões

Habilitar ou desabilitar a versão de SSL/TLS para os serviços:

Atualizador - Serviço de Atualização
WebUI - Interface de usuário da Web de gerenciamento de dispositivos
LDAPS - Serviços LDAP seguros (incluindo autenticação e autenticação externa)

Observe que o TLSv1.3 não está disponível para o Atualizador e LDAPS, somente a WebUI pode

ser configurada com o TLSv1.3.

Versões SSL/TLS atualmente habilitadas por serviço: (Y : habilitado, N : desabilitado)

Atualizador WebUI LDAPS
TLSv1.0 N N N
TLSv1.1 Y N Y
TLSv1.2 Y Y Y
TLSv1.3 N/D N/D

Selecione o serviço para o qual ativar/desativar versões de SSL/TLS:

1. Atualizador
2. Interface Web
3. LDAPS
4. Todos os serviços
[]> 2

Os protocolos atualmente habilitados para WebUI são TLSv1.2.

Para alterar a configuração de um protocolo específico, selecione uma opção abaixo:

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

O suporte TLSv1.3 para a interface de usuário da Web de gerenciamento do dispositivo está desabilitado no momento. Deseja ativá-lo? [N]> s

Os protocolos atualmente habilitados para WebUI são TLSv1.3, TLSv1.2.

Escolha a operação que deseja executar:
- VERSIONS - Habilitar ou desabilitar versões de SSL/TLS
- PEER_CERT_FQDN - Valide a conformidade FQDN do certificado de mesmo nível para Alerta sobre TLS, atualizador e LDAP.
- PEER_CERT_X509 - Valide a conformidade X509 do certificado de mesmo nível para Alerta sobre TLS, atualizador e LDAP.
[]>

sma1.example.com> confirmar

Aviso: as alterações na configuração SSL fazem com que o
estes processos serão reiniciados após Commit - gui,euq_webui.

Isso causa uma breve interrupção nas operações do SMA.

Insira alguns comentários descrevendo suas alterações:
[]> ativar o tls v1.3

Alterações confirmadas: Sun Jan 28 23:55:40 2024 EST
Reiniciando a GUI...
gui reiniciada
Reiniciando euq_webui...
euq_webui reiniciado

Aguarde um pouco e confirme se a WebUI está acessível.

Observação: selecionar várias versões de TLS para um serviço exige que o usuário selecione um serviço e uma versão de protocolo e repita a seleção de um serviço e um protocolo mais uma vez até que todas as configurações tenham sido modificadas.

Verificar

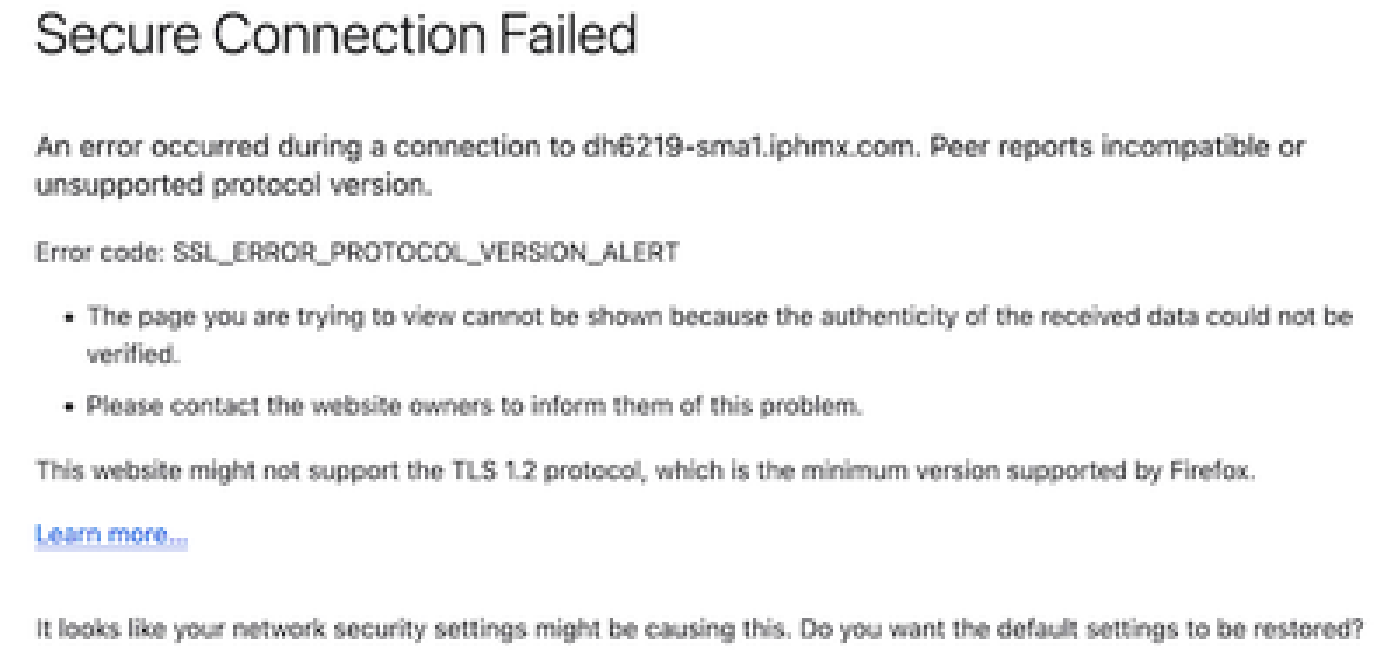
Esta seção inclui alguns cenários básicos de teste e os erros que ocorrem devido a versões incompatíveis ou erros de sintaxe.

Verifique a funcionalidade do navegador abrindo uma sessão do navegador da Web para a WebUI ou NGUI do EWM configurada com TLSv1.3.

Todos os navegadores da Web testados já estão configurados para aceitar TLS v1.3.

- Exemplo: defina a configuração do navegador no Firefox para desabilitar o suporte TLS v1.3 para produzir erros na ClassicUI e na NGUI do dispositivo.

- Interface de usuário clássica usando o Firefox configurada para excluir TLS v1.3, como um teste.
- A NGUI receberia o mesmo erro, com a única exceção sendo o número de porta 4431 (padrão) no URL.



Falha de TLS v1.3 Webui

- Para garantir a comunicação, verifique as configurações do navegador para garantir que TLSv1.3 esteja incluído. (Este exemplo é do Firefox)

- Um exemplo de comando openssl usando um valor de cifra digitado incorretamente forneceria esta saída de erro: exemplo de falha de teste de conexão openssl devido à cifra inválida: Erro com o comando: "-ciphersuites TLS_AES_256_GCM_SHA386"

2226823168:ERROR:1426E089:rotinas SSL:ciphersuite_cb:nenhuma correspondência de cifra:ssl/ssl_ciph.c:1299:

- O comando curl de exemplo executado para a ng-ui quando o TLS v1.3 está desabilitado gera esse erro.

curl: (35) CURL_SSLVERSION_MAX incompatível com CURL_SSLVERSION

Informações Relacionadas

- Cisco Content Security Management Appliance - Notas de versão
- Dispositivo de gerenciamento de segurança de conteúdo da Cisco - Guias do usuário final

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.