セキュリティで保護された電子メールWebマネージャのTLSv1.3の設定

内容

はじめに

このドキュメントでは、Cisco Secure Email and Web Manager(EWM)のTLS v1.3プロトコルの設定について説明します

前提条件

SEWM(SV+)の設定と設定に関する一般的な知識が必要です。

使用するコンポーネント

- Cisco Secure Email Web Manager(SEWM)AsyncOS 15.5.1以降。
- SSLの設定。

"このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください」

概要

SEWMはTLS v1.3プロトコルを統合して、HTTPS関連サービス（Classic UI、NGUI、およびRest API）の通信を暗号化します。

TLS v1.3プロトコルは、業界が標準にするために努めているので、より安全な通信とより迅速なネゴシエーションを誇っています。

SEWMでは、SSLのSEGWebUIまたはCLI内の既存のSSL設定方法を使用します。いくつかの重要な設定が強調表示されています。

- 許可されたプロトコルを設定する際の注意事項。
- TLS v1.3暗号は操作できません。
- TLS v1.3は、GUI HTTPSに対してのみ設定できます。
- TLS v1.0とTLS v1.3の間のTLSプロトコルのチェックボックス選択オプションでは、この記事で詳しく説明されているパターンを使用します。

設定

SEWMはAsycOS 15.5内にHTTPSのTLS v1.3プロトコルを統合しています。

プロトコル設定を選択する際は、HTTPS障害を防ぐために注意が必要です。

TLS v1.3のWebブラウザのサポートは一般的ですが、一部の環境ではSEWMにアクセスするために調整が必要です。

TLS v1.3プロトコルのCisco SEWM実装では、SEWM内で変更または除外できない3つのデフォルト暗号がサポートされています。

TLS 1.3暗号：

TLS_AES_256_GCM_SHA384

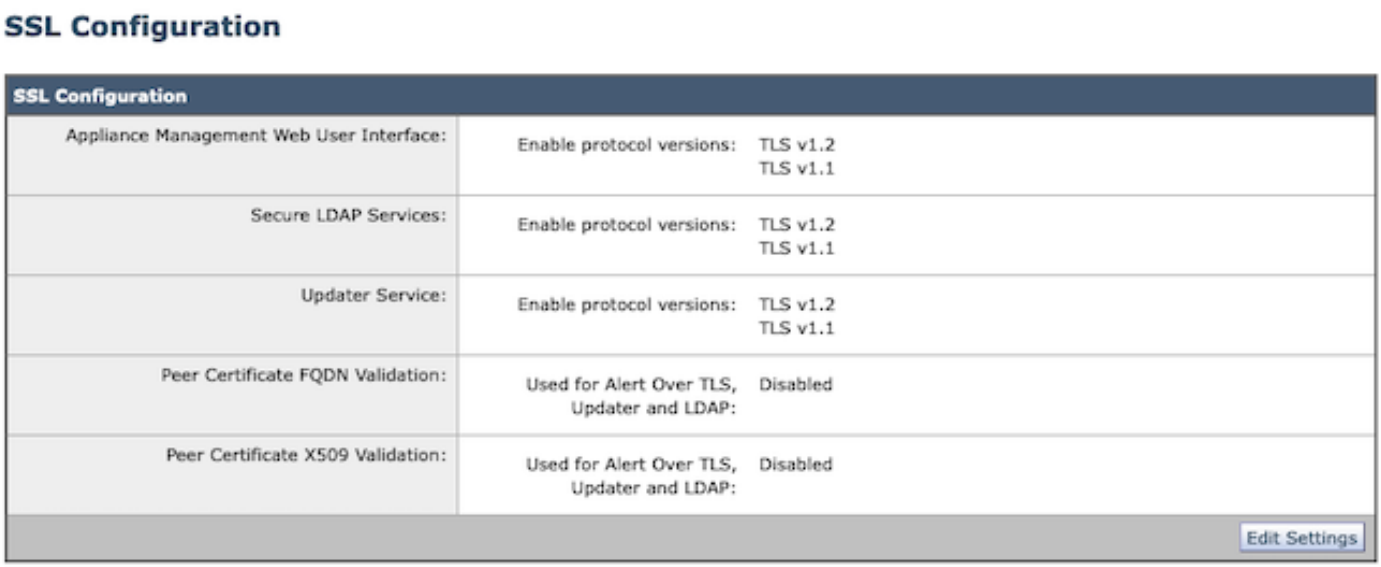
TLS_CHACHA20_POLY1305_SHA256

TLS_AES_128_GCM_SHA256

WebUIからの設定

>システム管理> SSL設定に移動します

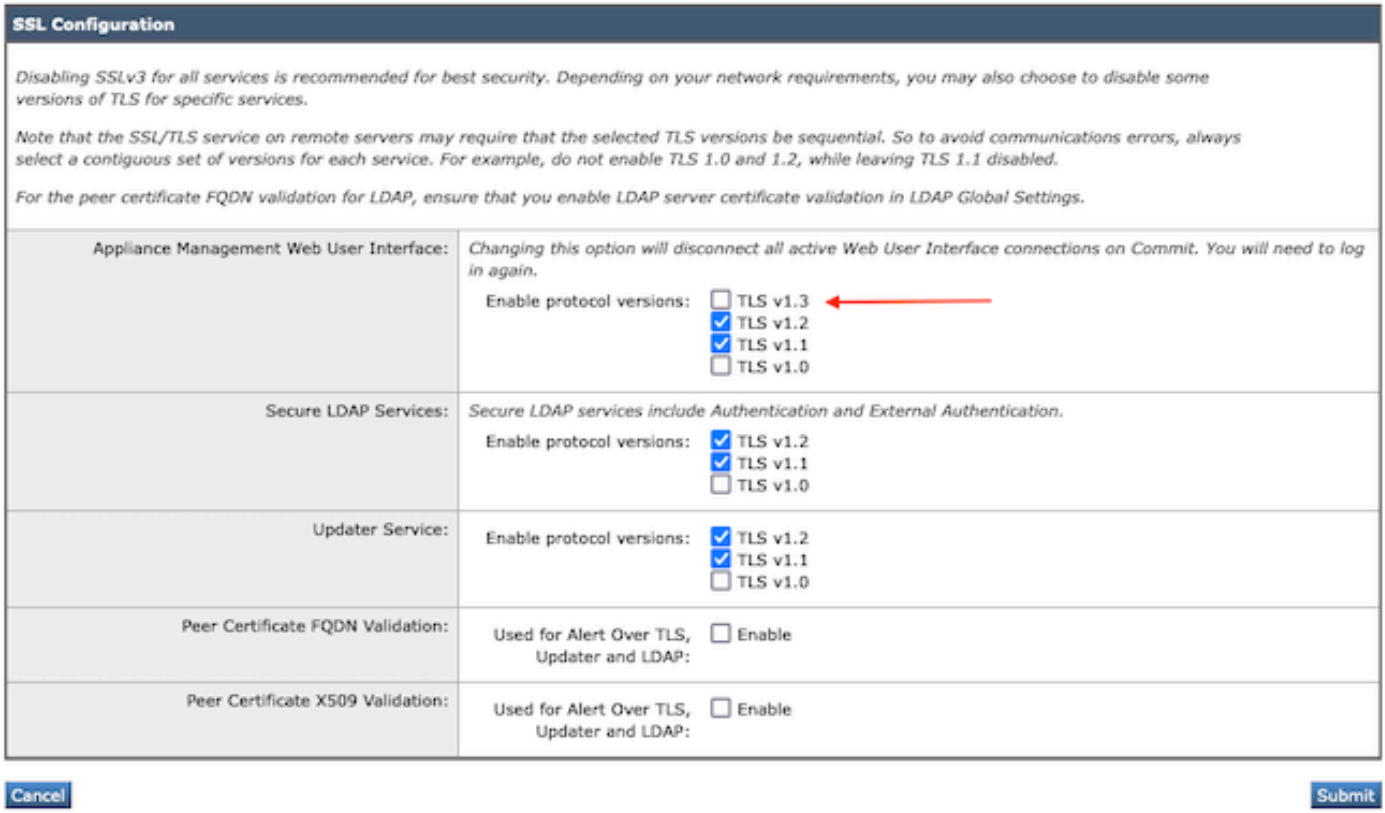
- 15.5 AsyncOS HTTPSへのアップグレード後に選択されるデフォルトのTLSプロトコルには、TLS v1.1とTLS v1.2のみが含まれます。
- リストされている2つの追加サービスであるSecure LDAP ServicesとUpdater Servicesは、TLS v1.3をサポートしていません。



「設定の編集」を選択して、構成オプションを表示します。

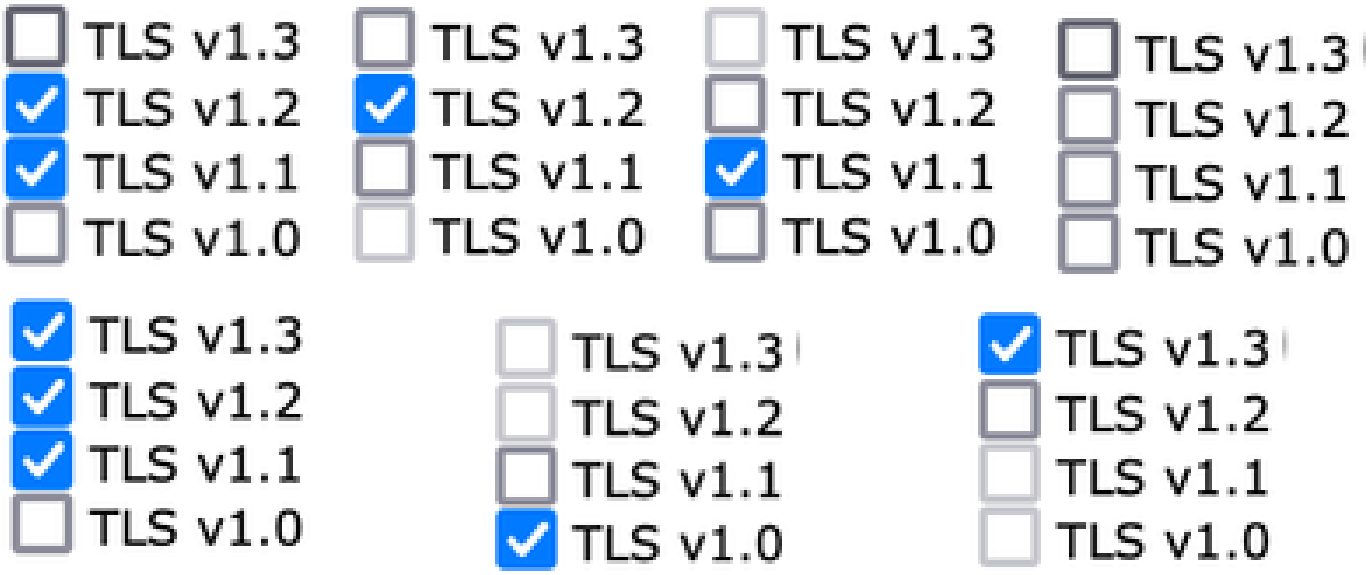
「Webユーザインターフェイス」のTLSプロトコル選択オプションには、TLS v1.0、TLS v1.1、TLS v1.2、およびTLS v1.3が含まれます。

- AsyncOS 15.5へのアップグレード後は、TLS v1.1およびTLS v1.2プロトコルのみがデフォルトで選択されます。

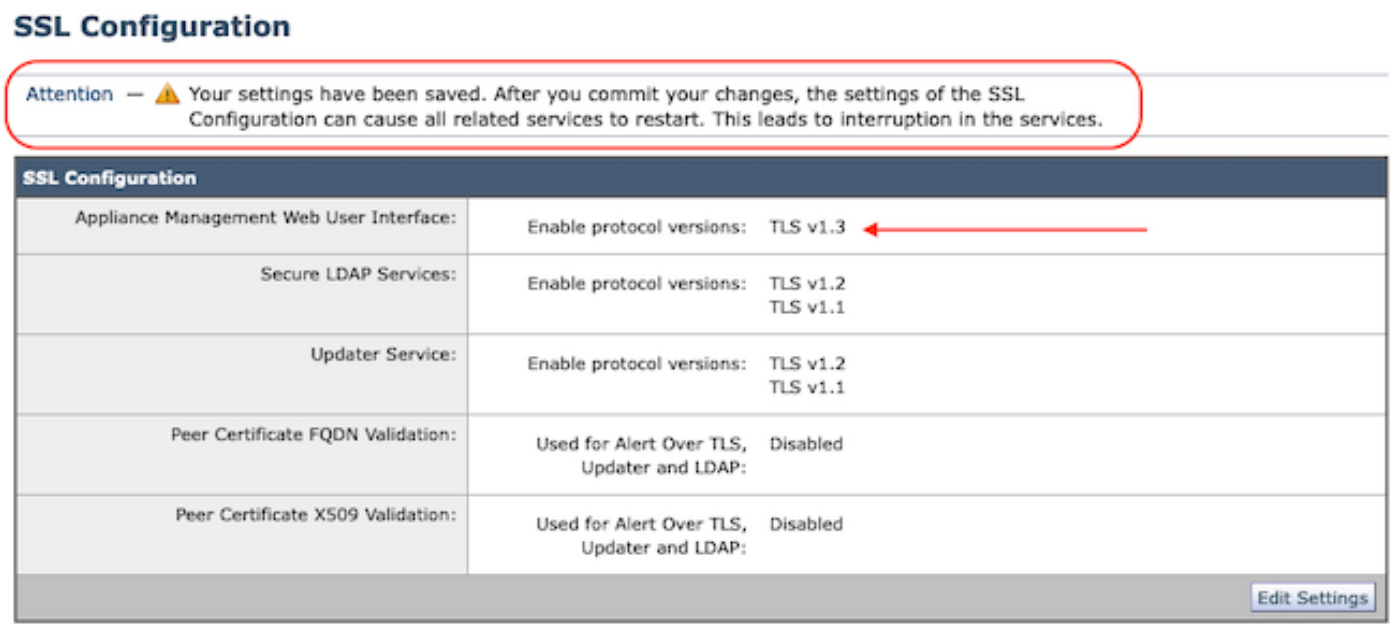


注:TLS1.0は非推奨であるため、デフォルトでは無効になっています。所有者が有効にすることを選択した場合、TLS v1.0は引き続き使用できます。

- チェックボックスのオプションは、互換性のないオプションで使用可能なプロトコルを示す太字のボックスとグレー表示のボックスで点灯します。
- 図のオプション例は、Webユーザー・インタフェースのチェックボックス・オプションを示しています。



注意: SSL構成を変更すると、関連サービスが再起動する場合があります。これにより、WebUIサービスが一時的に中断されます。



CLI からの設定

EWMは、WebUIという1つのサービスでTLS v1.3を許可します。

sma1.example.com> sslconfig

最適なセキュリティを確保するために、SSLv3を無効にすることを推奨します。

リモートサーバー上のSSL/TLSサービスでは、選択したTLSバージョンがシーケンシャルである必要があります。したがって、通信エラーを回避するには、常に連続する
各サービスのバージョンセット。たとえば、TLS 1.1を無効にしたまま、TLS 1.0と1.2を有効にしないでください。

実行する操作を選択します。
- VERSIONS:SSL/TLSバージョンを有効または無効にします。
- PEER_CERT_FQDN:Alert Over TLS、アップデータ、およびLDAPのピア証明書FQDNコンプライアンスを検証します。
- PEER_CERT_X509:Alert Over TLS、アップデータ、およびLDAPのピア証明書X509への準拠を検証します。
[]>バージョン

サービスのSSL/TLSバージョンを有効または無効にします。

Updater – サービスの更新
WebUI:Appliance Management Web User Interface (アプライアンス管理Webユーザー・インターフェイス)
LDAPS：セキュアLDAPサービス (認証および外部認証を含む)

TLSv1.3はUpdaterおよびLDAPSでは使用できません。TLSv1.3ではWebUIのみを設定できます。

サービスによって現在有効になっているSSL/TLSバージョン：（Y：有効、N：無効）

WebUI LDAPSの更新
TLSv1.0 N N N
TLSv1.1 Y N Y
TLSv1.2前年比
TLSv1.3該当なし該当なし

SSL/TLSバージョンを有効または無効にするサービスを選択してください：

1. アップデータ
2. WebUI
（三）LDAPS
4. すべてのサービス
[]> 2

WebUIで現在有効なプロトコルはTLSv1.2です。

特定のプロトコルの設定を変更するには、次のいずれかのオプションを選択します。

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

アプライアンス管理Webユーザーインターフェイスの TLSv1.3サポートは現在無効です。有効にしますか？[N]> y

WebUIで現在有効なプロトコルはTLSv1.3、TLSv1.2です。

実行する操作を選択します。
- VERSIONS:SSL/TLSバージョンを有効または無効にします。
- PEER_CERT_FQDN:Alert Over TLS、アップデータ、およびLDAPのピア証明書FQDNコンプライアンスを検証します。
- PEER_CERT_X509:Alert Over TLS、Updater、およびLDAPのピア証明書X509への準拠を検証します。
[]>

sma1.example.com>コミット

警告： SSL構成の変更により、
コミット後に再起動するプロセス – gui、euq_webui。

これにより、SMAの動作が短時間中断します。

変更を説明するコメントを入力してください：
[]> tls v1.3を有効にする

変更のコミット：2024年1月28日（日） 23:55:40 EST
guiを再起動しています…
guiの再起動
euq_webuiを再起動しています…
euq_webuiが再起動しました

少し待ち、WebUIにアクセスできることを確認します。

注：サービスに対してTLSの複数のバージョンを選択するには、ユーザがサービスとプロトコルバージョンを選択し、すべての設定が変更されるまでサービスとプロトコルの選択をもう一度繰り返す必要があります。

確認

このセクションでは、基本的なテストシナリオと、バージョンの不一致や構文エラーが原因で発生するエラーについて説明します。

TLSv1.3で設定されたEWM WebUIまたはNGUIへのWebブラウザセッションを開いて、ブラウザの機能を確認します。

テストしたすべてのWebブラウザは、TLS v1.3を受け入れるように設定済みです。

- Firefoxのブラウザ設定でTLS v1.3サポートを無効にした例では、アプライアンスのClassicUIとNGUIの両方でエラーが発生します。
- Firefoxを使用したクラシックUIで、テストとしてTLS v1.3を除外するように設定されている。
- NGUIは、URL内のポート番号4431（デフォルト）を例外として、同じエラーを受信します。

TLS v1.3 Webuiの障害

- 通信を確保するには、TLSv1.3が含まれるようにブラウザの設定を確認します。（このサンプルはFirefoxのものです）

- 誤って入力された暗号値を使用したopensslコマンドの例では、次のエラー出力が表示されます。「sample openssl connection test failure due to invalid cipher: Error with command: "-ciphersuites TLS_AES_256_GCM_SHA386」

2226823168:ERROR:1426E089:SSLルーチン：ciphersuite_cb：一致しない暗号
：ssl/ssl_ciph.c:1299:

- TLS v1.3が無効なときにng-uiに対してcurlコマンドを実行すると、このエラーが生成されます。

curl: (35) CURL_SSLVERSION_MAXはCURL_SSLVERSIONと互換性がありません

関連情報

- Ciscoコンテンツセキュリティ管理アプライアンス – リリースノート
- Ciscoコンテンツセキュリティ管理アプライアンス – エンドユーザガイド

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。