为安全邮件Web管理器配置TLSv1.3

目录

简介

本文档介绍思科安全邮件和网络管理器(EWM)的TLS v1.3协议的配置

先决条件

需要具备SEWM设置和配置的一般知识。

使用的组件

- Cisco Secure Email Web Manager (SEWM) AsyncOS 15.5.1及更高版本。
- SSL配置设置。

"本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。”

概述

SEWM集成了TLS v1.3协议，以加密HTTPS相关服务、传统UI、NGUI和Rest API的通信。

TLS v1.3协议具有更安全的通信能力和更快的协商速度，因为业界正在努力使其成为标准。

SEWM使用SSL的SEGWebUI或CLI中的现有SSL配置方法，并突出显示几个值得注意的设置。

- 配置允许的协议时提供预防性建议。
- TLS v1.3密码不能被操纵。
- TLS v1.3只能配置用于GUI HTTPS。
- TLS v1.0和TLS v1.3之间的TLS协议复选框选择选项使用本文中更详细地演示的模式。

配置

SEWM在AsycOS 15.5中集成了用于HTTPS的TLS v1.3协议。

在选择协议设置以防止HTTPS故障时，建议小心谨慎。

TLS v1.3的Web浏览器支持很常见，尽管某些环境需要调整才能访问SEWM。

TLS v1.3协议的Cisco SEWM实施支持3个默认密码，这些密码不能在SEWM中更改或排除。

TLS 1.3密码：

TLS_AES_256_GCM_SHA384

TLS_CHACHA20_POLY1305_SHA256

TLS_AES_128_GCM_SHA256

WebUI中的配置

导航到>系统管理> SSL配置

- 升级到15.5 AsyncOS HTTPS后的默认TLS协议选择仅包括TLS v1.1和TLS v1.2。
- 列出的另外两个服务（安全LDAP服务和更新程序服务）不支持TLS v1.3。

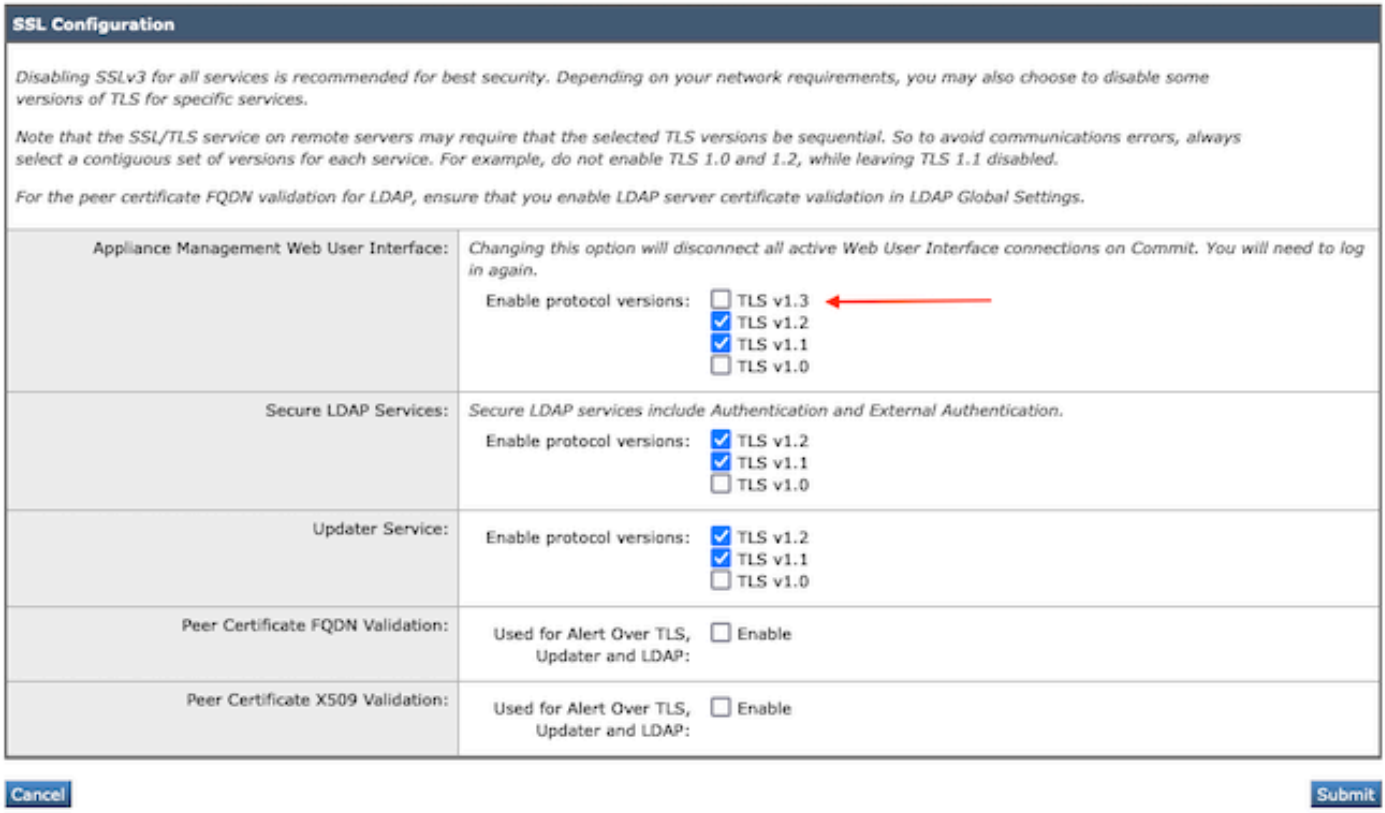
SSL Configuration

SSL Configuration		
Appliance Management Web User Interface:	Enable protocol versions:	TLS v1.2 TLS v1.1
Secure LDAP Services:	Enable protocol versions:	TLS v1.2 TLS v1.1
Updater Service:	Enable protocol versions:	TLS v1.2 TLS v1.1
Peer Certificate FQDN Validation:	Used for Alert Over TLS, Updater and LDAP:	Disabled
Peer Certificate X509 Validation:	Used for Alert Over TLS, Updater and LDAP:	Disabled
		Edit Settings

选择“Edit Settings”（编辑设置）以显示配置选项。

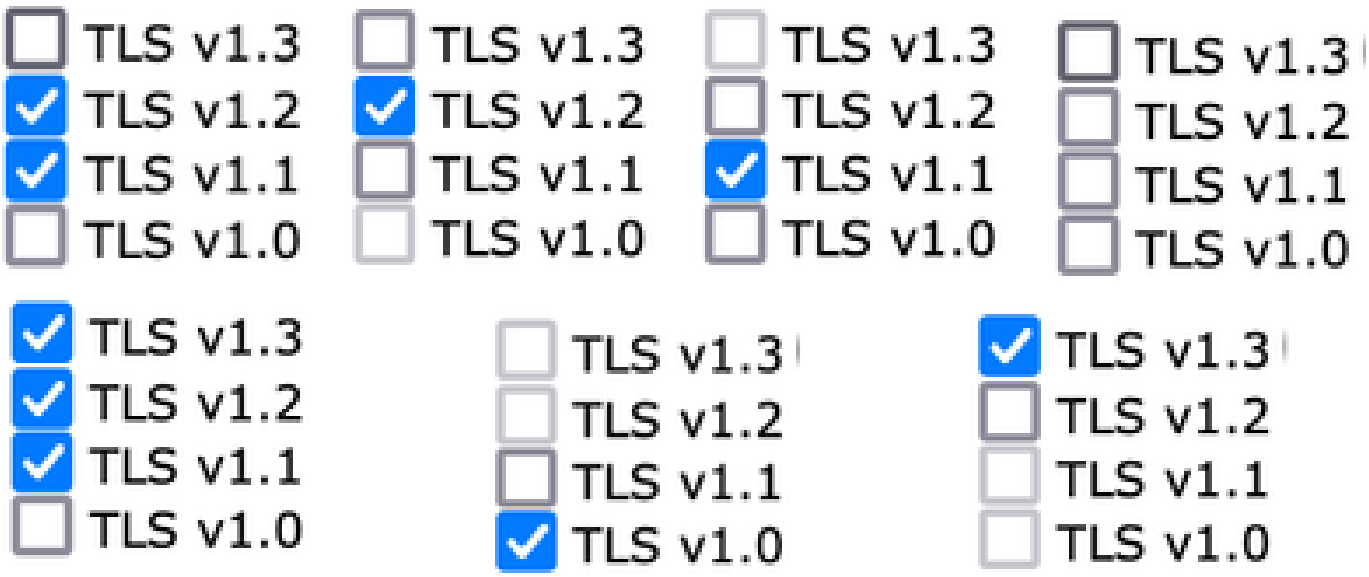
“Web用户界面”的TLS协议选择选项包括TLS v1.0、TLS v1.1、TLS v1.2和TLS v1.3。

- 升级到AsyncOS 15.5后，默认情况下仅选择TLS v1.1和TLS v1.2协议。

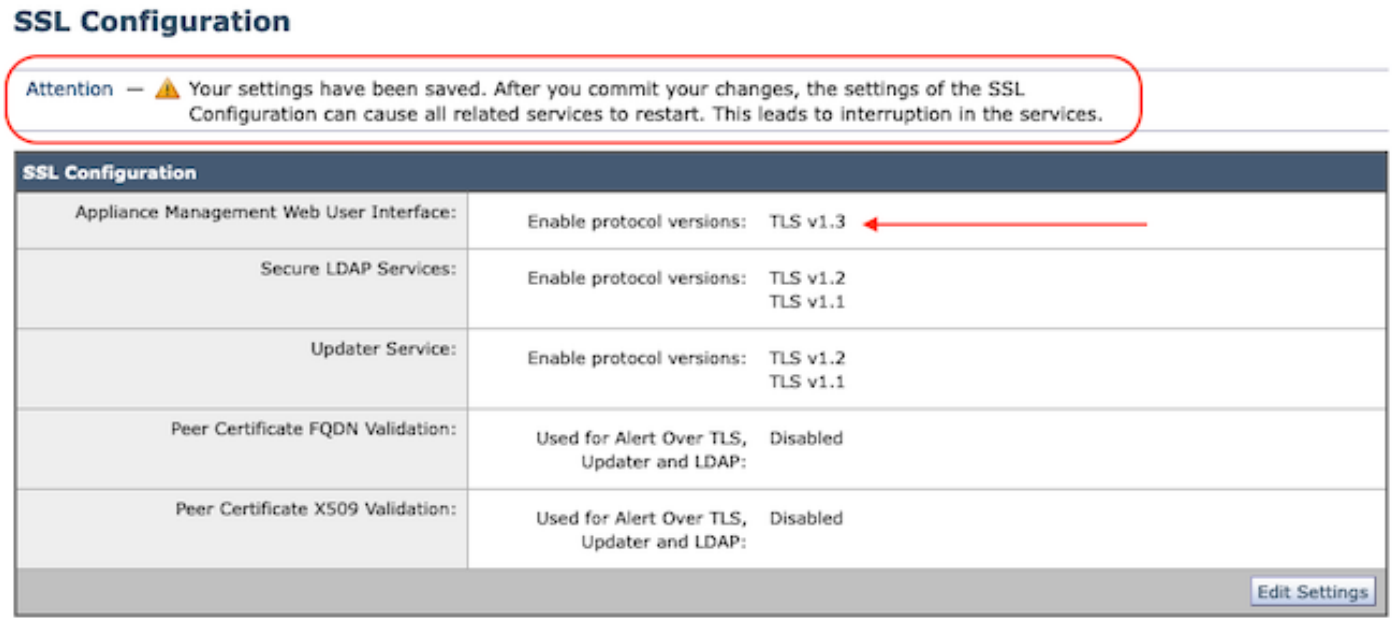


注意：TLS1.0已弃用，因此默认为禁用。如果所有者选择启用TLS v1.0，则它仍然可用。

- 复选框选项亮起，显示可用协议的粗体框和显示不兼容选项的灰色框。
- 图像中的示例选项说明了Web用户界面的复选框选项。



注意：对SSL配置进行修改可能导致相关服务重新启动。这会导致WebUI服务出现短暂中断。



从CLI进行配置

EWM允许在一个服务上使用TLS v1.3：WebUI

sma1.example.com> sslconfig

建议禁用SSLv3以获得最佳安全性。

请注意，远程服务器上的SSL/TLS服务要求所选TLS版本是连续的。为了避免通信错误，请始终选择连续的
每个服务的版本集。例如，请勿启用TLS 1.0和1.2，同时禁用TLS 1.1。

选择要执行的操作：
- 版本-启用或禁用SSL/TLS版本
- PEER_CERT_FQDN -验证通过TLS、更新程序和LDAP发出警报的对等证书FQDN合规性。
- PEER_CERT_X509 -验证对等证书X509是否符合TLS、更新程序和LDAP警报要求。
[]>版本

启用或禁用服务的SSL/TLS版本：

更新程序-更新服务
WebUI -设备管理Web用户界面
LDAPS -安全LDAP服务（包括身份验证和外部身份验证）

请注意，TLSv1.3不可用于更新程序和LDAPS，只有WebUI可以配置为TLSv1.3。

当前按服务启用的SSL/TLS版本：（Y：已启用，N：已禁用）

更新程序WebUI LDAPS
TLSv1.0 N N N
TLSv1.1 Y N Y
TLSv1.2 Y Y

TLSv1.3不适用

选择要为其启用/禁用SSL/TLS版本的服务：

1. 更新程序
2. 网络用户界面
3. LDAPS
4. 所有服务
[]> 2

当前为WebUI启用的协议是TLSv1.2。

要更改特定协议的设置，请选择以下选项：

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

当前已禁用对设备管理Web用户界面的TLSv1.3支持。是否要启用它？[N]> y

当前为WebUI启用的协议是TLSv1.3、TLSv1.2。

选择要执行的操作：
- 版本-启用或禁用SSL/TLS版本
- PEER_CERT_FQDN -验证通过TLS、更新程序和LDAP发出警报的对等证书FQDN合规性。
- PEER_CERT_X509 -验证对等证书X509是否符合TLS、更新程序和LDAP警报要求。
[]>

sma1.example.com> 提交

警告：SSL配置中的更改会导致
这些进程在提交后重新启动- gui，euq_webui。
这会导致SMA操作短暂中断。

请输入一些描述您所做更改的注释：
[]>启用tls v1.3

提交的更改：2024年1月28日星期日23:55:40（东部标准时间）
正在重新启动gui...
gui已重新启动
正在重新启动euq_webui...
euq_webui已重新启动

稍等片刻，确认可以访问WebUI。

> 注意：为服务选择多个版本的TLS需要用户选择服务和协议版本，然后再次重复选择服务和协议直到所有设置都已修改。

验证

本节包括一些基本测试方案以及由于版本不匹配或语法错误导致的错误。

通过打开与EWM WebUI或配置了TLSv1.3的NGUI的Web浏览器会话验证浏览器功能。

我们测试的所有Web浏览器都已配置为接受TLS v1.3。

- 将Firefox上的浏览器设置设置为禁用TLS v1.3支持的示例会在设备的ClassicUI和NGUI上生成错误。

- 将Firefox配置为排除TLS v1.3的传统UI用作测试。
- NGUI将收到相同的错误，唯一的例外是URL中的端口号4431（默认）。

TLS v1.3 Webui故障

- 为确保通信，请验证浏览器设置，以确保包含TLSv1.3。（此示例来自Firefox）

- 使用输入错误的密码值的openssl命令示例将提供以下错误输出：由于密码无效而导致的openssl连接测试失败示例：命令错误："-ciphersuites TLS_AES_256_GCM_SHA386"

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

- 禁用TLS v1.3时对ng-ui执行的示例curl命令生成此错误。

curl： (35) CURL_SSLVERSION_MAX与CURL_SSLVERSION不兼容

相关信息

- 思科内容安全管理设备-版本说明
- 思科内容安全管理设备-最终用户指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。