

# 設定Secure Email Web Manager的TLSv1.3

## 目錄

---

---

## 簡介

本文檔介紹用於思科安全郵件和網路管理器(EWM)的TLS v1.3協定的配置

## 必要條件

需要具備SEWM設定和配置的一般知識。

## 採用元件

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

"本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路處於活動狀態，請確保您瞭解所有命令的潛在影響。"

## 概觀

SEWM整合了TLS v1.3協定，以加密與HTTPS相關的服務；傳統UI、NGUI和Rest API。

TLS v1.3協定具有更高的通訊安全性和更快的協商速度，因為業界正在努力將其作為標準。

SEWM使用SSL的SEGWebUI或CLI中的現有SSL配置方法，並突出顯示一些重要設定。

- 配置允許的協定時提供預防建議。
- 無法操作TLS v1.3密碼。
- TLS v1.3隻能配置為GUI HTTPS。
- TLS v1.0和TLS v1.3之間的TLS協定覈取方塊選擇選項使用本文中詳細介紹的模式。

## 設定

SEWM在AsyncOS 15.5中整合了用於HTTPS的TLS v1.3協定。

在選擇協定設定以防止HTTPS故障時，建議謹慎。

TLS v1.3的Web瀏覽器支援很常見，不過有些環境需要調整才能存取SEWM。

TLS v1.3協定的Cisco SEWM實施支援3個預設密碼，這些密碼不能在SEWM中更改或排除。

TLS 1.3密碼：

TLS\_AES\_256\_GCM\_SHA384

TLS\_CHACHA20\_POLY1305\_SHA256

TLS\_AES\_128\_GCM\_SHA256

## 從WebUI配置

導航至>系統管理> SSL配置

- 升級到15.5 AsyncOS HTTPS後的預設TLS協定選擇僅包括TLS v1.1和TLS v1.2。
- 列出的另外兩項服務 ( 安全LDAP服務和更新程式服務 ) 不支援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](#)

選取「編輯設定」以顯示組態選項。

「Web使用者介面」的TLS協定選擇選項包括TLS v1.0、TLS v1.1、TLS v1.2和TLS v1.3。

- 升級到AsyncOS 15.5後，預設情況下僅選擇TLS v1.1和TLS v1.2協定。

SSL Configuration	
<p>Disabling SSLv3 for all services is recommended for best security. Depending on your network requirements, you may also choose to disable some versions of TLS for specific services.</p> <p>Note that the SSL/TLS service on remote servers may require that the selected TLS versions be sequential. So to avoid communications errors, always select a contiguous set of versions for each service. For example, do not enable TLS 1.0 and 1.2, while leaving TLS 1.1 disabled.</p> <p>For the peer certificate FQDN validation for LDAP, ensure that you enable LDAP server certificate validation in LDAP Global Settings.</p>	
Appliance Management Web User Interface:	<p>Changing this option will disconnect all active Web User Interface connections on Commit. You will need to log in again.</p> <p>Enable protocol versions:</p> <p><input type="checkbox"/> TLS v1.3 ←</p> <p><input checked="" type="checkbox"/> TLS v1.2</p> <p><input checked="" type="checkbox"/> TLS v1.1</p> <p><input type="checkbox"/> TLS v1.0</p>
Secure LDAP Services:	<p>Secure LDAP services include Authentication and External Authentication.</p> <p>Enable protocol versions:</p> <p><input checked="" type="checkbox"/> TLS v1.2</p> <p><input checked="" type="checkbox"/> TLS v1.1</p> <p><input type="checkbox"/> TLS v1.0</p>
Updater Service:	<p>Enable protocol versions:</p> <p><input checked="" type="checkbox"/> TLS v1.2</p> <p><input checked="" type="checkbox"/> TLS v1.1</p> <p><input type="checkbox"/> TLS v1.0</p>
Peer Certificate FQDN Validation:	<p>Used for Alert Over TLS, Updater and LDAP:</p> <p><input type="checkbox"/> Enable</p>
Peer Certificate X509 Validation:	<p>Used for Alert Over TLS, Updater and LDAP:</p> <p><input type="checkbox"/> Enable</p>

Cancel Submit

 注意：TLS1.0已停用，因此預設為停用。如果所有者選擇啟用TLS v1.0，則它仍然可用。

- 核取方塊選項會亮起，顯示可用通訊協定的粗體方塊，不相容選項的灰顯方塊會亮起。
- 影像中的範例選項說明了「Web使用者介面」的核取方塊選項。

<input type="checkbox"/> TLS v1.3	<input type="checkbox"/> TLS v1.3	<input type="checkbox"/> TLS v1.3	<input type="checkbox"/> TLS v1.3
<input checked="" type="checkbox"/> TLS v1.2	<input checked="" type="checkbox"/> TLS v1.2	<input type="checkbox"/> TLS v1.2	<input type="checkbox"/> TLS v1.2
<input checked="" type="checkbox"/> TLS v1.1	<input type="checkbox"/> TLS v1.1	<input checked="" type="checkbox"/> TLS v1.1	<input type="checkbox"/> TLS v1.1
<input type="checkbox"/> TLS v1.0	<input type="checkbox"/> TLS v1.0	<input type="checkbox"/> TLS v1.0	<input type="checkbox"/> TLS v1.0

  

<input checked="" type="checkbox"/> TLS v1.3	<input type="checkbox"/> TLS v1.3	<input checked="" type="checkbox"/> TLS v1.3
<input checked="" type="checkbox"/> TLS v1.2	<input type="checkbox"/> TLS v1.2	<input type="checkbox"/> TLS v1.2
<input checked="" type="checkbox"/> TLS v1.1	<input type="checkbox"/> TLS v1.1	<input type="checkbox"/> TLS v1.1
<input type="checkbox"/> TLS v1.0	<input checked="" type="checkbox"/> TLS v1.0	<input type="checkbox"/> TLS v1.0

 注意：修改SSL組態可能會導致相關服務重新啟動。這會造成WebUI服務暫時中斷。

## SSL Configuration

Attention — ⚠ Your settings have been saved. After you commit your changes, the settings of the SSL Configuration can cause all related services to restart. This leads to interruption in the services.

SSL Configuration	
Appliance Management Web User Interface:	Enable protocol versions: TLS v1.3 ←
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](#)

### 從CLI進行配置

EWM允許在一項服務上使用TLS v1.3 : WebUI

```
sma1.example.com> sslconfig
```

建議停用SSLv3以獲得最佳安全性。

請注意，遠端伺服器上的SSL/TLS服務需要選取的TLS版本是循序的。為了避免通訊錯誤，請始終選擇一個連續的每個服務的版本集。例如，請勿啟用TLS 1.0和1.2，同時停用TLS 1.1。

選擇要執行的作業：

- 版本-啟用或停用SSL/TLS版本
- PEER\_CERT\_FQDN -驗證基於TLS、更新程式和LDAP的警報的對等證書FQDN合規性。
- PEER\_CERT\_X509 -驗證Alert Over TLS、Updater和LDAP的對等證書X509合規性。

[]>版本

啟用或停用服務的SSL/TLS版本：

更新程式-更新服務

WebUI -裝置管理Web使用者介面

LDAPS -安全LDAP服務 (包括身份驗證和外部身份驗證)

請注意，TLSv1.3不適用於Updater和LDAPS，只有WebUI可以配置為TLSv1.3。

目前依服務啟用的SSL/TLS版本：( Y：已啟用，N：已停用 )

更新程式WebUI LDAPS

TLSv1.0 N N N

TLSv1.1 Y N Y

TLSv1.2 Y Y Y

TLSv1.3 N/A N/A

選取要啟用/停用SSL/TLS版本的服務：

1. 更新程式
2. WebUI
3. LDAPS
4. 所有服務

[]> 2

目前為WebUI啟用的通訊協定是TLSv1.2。

要更改特定協定的設定，請選擇以下選項：

1. TLSv1.0
2. TLSv1.1
3. TLSv1.2
4. TLSv1.3

[]> 4

當前已停用對裝置管理Web使用者介面的TLSv1.3支援。是否要啟用它？[N]> y

WebUI當前啟用的協定是TLSv1.3、TLSv1.2。

選擇要執行的作業：

- 版本-啟用或停用SSL/TLS版本
- PEER\_CERT\_FQDN -驗證基於TLS、更新程式和LDAP的警報的對等證書FQDN合規性。
- PEER\_CERT\_X509 -驗證Alert Over TLS、Updater和LDAP的對等證書X509合規性。

[]>

sma1.example.com> commit

警告：SSL配置中的更改會導致  
提交- gui，euq\_webui後要重新啟動這些進程。  
這會導致SMA操作短暫中斷。

請輸入一些描述您變更的註解：

[]>啟用tls v1.3

提交的更改：2024年1月28日星期日23:55:40 EST

正在重新啟動gui...

gui已重新啟動

正在重新啟動euq\_webui...

euq\_webui已重新啟動

請稍等片刻，並確認可以存取WebUI。

 注意：為服務選擇多個TLS版本需要使用者選擇一個服務和協定版本，然後再次重複選擇服務和協定，直到所有設定都已修改為止。

## 驗證

本節包含一些基本測試案例，以及由於版本不符或語法錯誤而出現的錯誤。

打開與TLSv1.3配置的EWM WebUI或NGUI的Web瀏覽器會話，驗證瀏覽器功能。

我們測試的所有網頁瀏覽器都已設定為接受TLS v1.3。

- 在Firefox上將瀏覽器設定設定為停用TLS v1.3支援的示例在裝置的ClassicUI和NGUI上都會產生錯誤。
- 使用Firefox的傳統UI配置為排除TLS v1.3作為測試。
- NGUI會收到相同的錯誤，唯一的例外是URL中的埠號4431（預設）。

## Secure Connection Failed

An error occurred during a connection to dh6219-sma1.iphmx.com. Peer reports incompatible or unsupported protocol version.

Error code: SSL\_ERROR\_PROTOCOL\_VERSION\_ALERT

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

This website might not support the TLS 1.2 protocol, which is the minimum version supported by Firefox.

[Learn more...](#)

It looks like your network security settings might be causing this. Do you want the default settings to be restored?

TLS v1.3 Webui故障

- 為確保通訊，請驗證瀏覽器設定，以確保包含TLSv1.3。（此示例來自Firefox）

security.tls.version.fallback-limit	4	
security.tls.version.max	4	
security.tls.version.min	1	

- 使用輸入錯誤的密碼值對openssl命令進行抽樣時，將產生以下錯誤輸出：sample openssl connection test failure due to invalid cipher : Error with command : "-ciphersuites

TLS\_AES\_256\_GCM\_SHA386"

2226823168 : 錯誤 : 1426E089 : SSL常式 : ciphersuite\_cb : no cipher match : ssl/ssl\_ciph.c : 1299 :

- 停用TLS v1.3時對ng-ui執行的示例curl命令生成此錯誤。

捲曲 : (35) CURL\_SSLVERSION\_MAX與CURL\_SSLVERSION不相容

## 相關資訊

- [思科內容安全管理裝置-發行版本註釋](#)
- [Cisco內容安全管理裝置-最終使用手冊](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。