Configure TLSv1.3 for Secure Email Web Manager

Contents

Introduction

This document describes the configuration of the TLS v1.3 protocol for Cisco Secure Email and Web Manager (EWM)

Prerequisites

General knowledge of the SEWM settings and configuration is desired.

Components Used

- Cisco Secure Email Web Manager (SEWM) AsyncOS 15.5.1 and newer.
- SSL Configuration Settings.

"The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command."

Overview

The SEWM has integrated TLS v1.3 protocol to encrypt communications for HTTPS-Related services; Classic UI, NGUI, and Rest API.

TLS v1.3 Protocol boasts more secure communication and faster negotiation as the industry strives to make it the standard.

The SEWM uses the existing SSL Configuration method within the SEGWebUIor CLI of SSL with a few notable settings to highlight.

- Precautionary advice when configuring the permitted protocols.
- The TLS v1.3 Ciphers cannot be manipulated.
- TLS v1.3 can be configured for GUI HTTPS only.
- The TLS protocol checkbox selection options between TLS v1.0 and TLS v1.3 use a pattern illustrated in more detail within the article.

Configure

The SEWM has integrated the TLS v1.3 protocol for HTTPS within AsycOS 15.5.

Caution is recommended when choosing the protocol settings to prevent HTTPS failure.

Web Browser support for TLS v1.3 is common although some environments require adjustments to access the SEWM.

The Cisco SEWM implementation of the TLS v1.3 Protocol supports 3 default ciphers which cannot be changed or excluded within the SEWM.

TLS 1.3 ciphers:

TLS_AES_256_GCM_SHA384

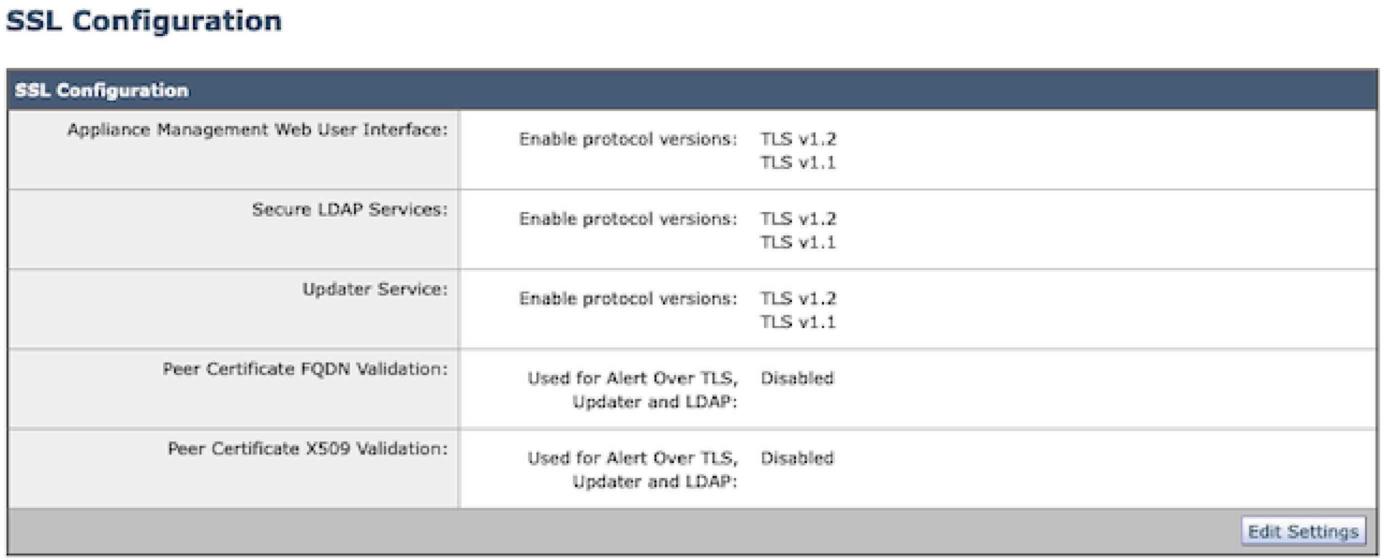
TLS_CHACHA20_POLY1305_SHA256

TLS_AES_128_GCM_SHA256

Configuration from the WebUI

Navigate to > System Administration > SSL Configuration

- The default TLS Protocol selection post upgrade to 15.5 AsyncOS HTTPS includes TLS v1.1 and TLS v1.2 only.
- The two additional services listed, Secure LDAP Services and Updater Services, do not support TLS v1.3.



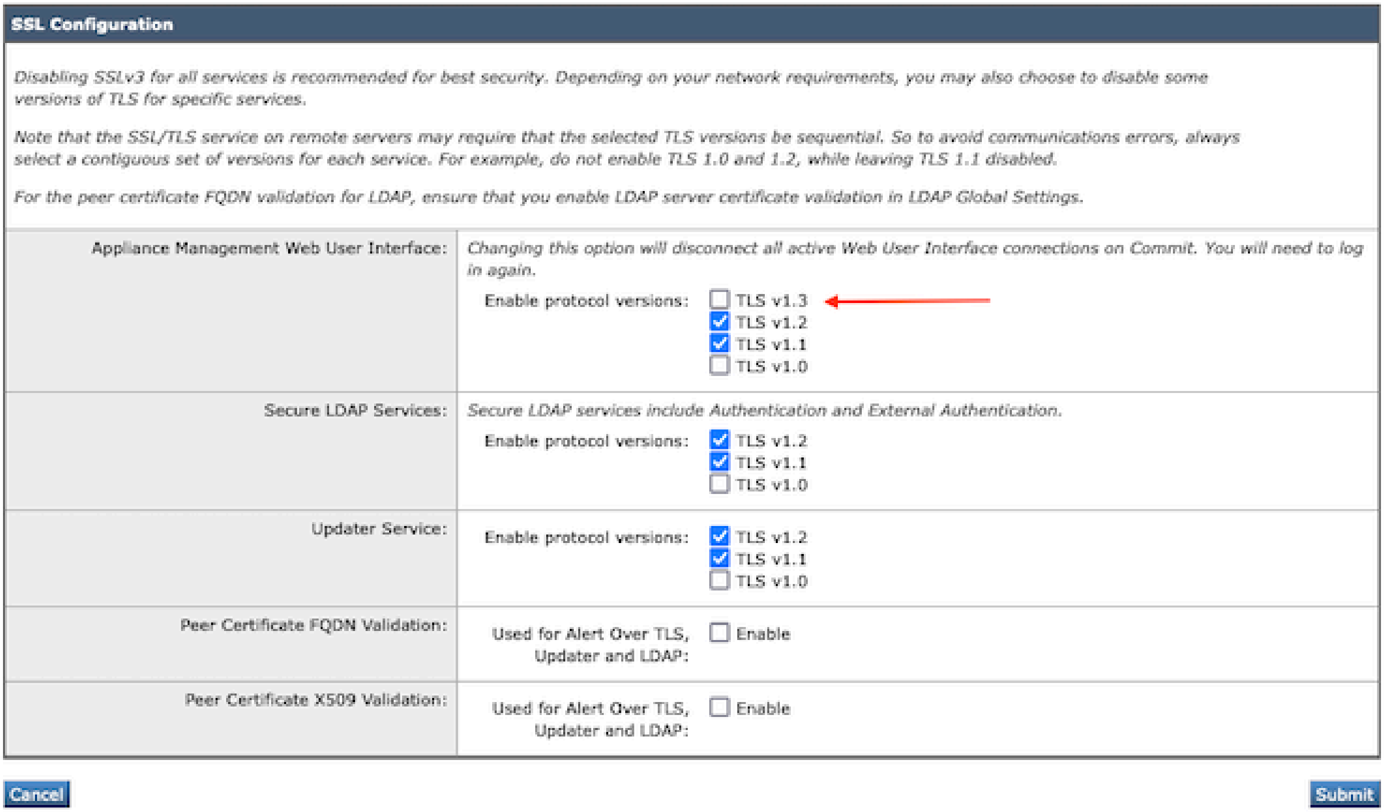
SSL Configuration

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

Select "Edit Settings," to present the configuration options.

The TLS protocol selection options for "Web User Interface," include TLS v1.0, TLS v1.1, TLS v1.2, and TLS v1.3.

- Post upgrade to AsyncOS 15.5, only TLS v1.1 and TLS v1.2 protocols are selected by default.



SSL Configuration

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.

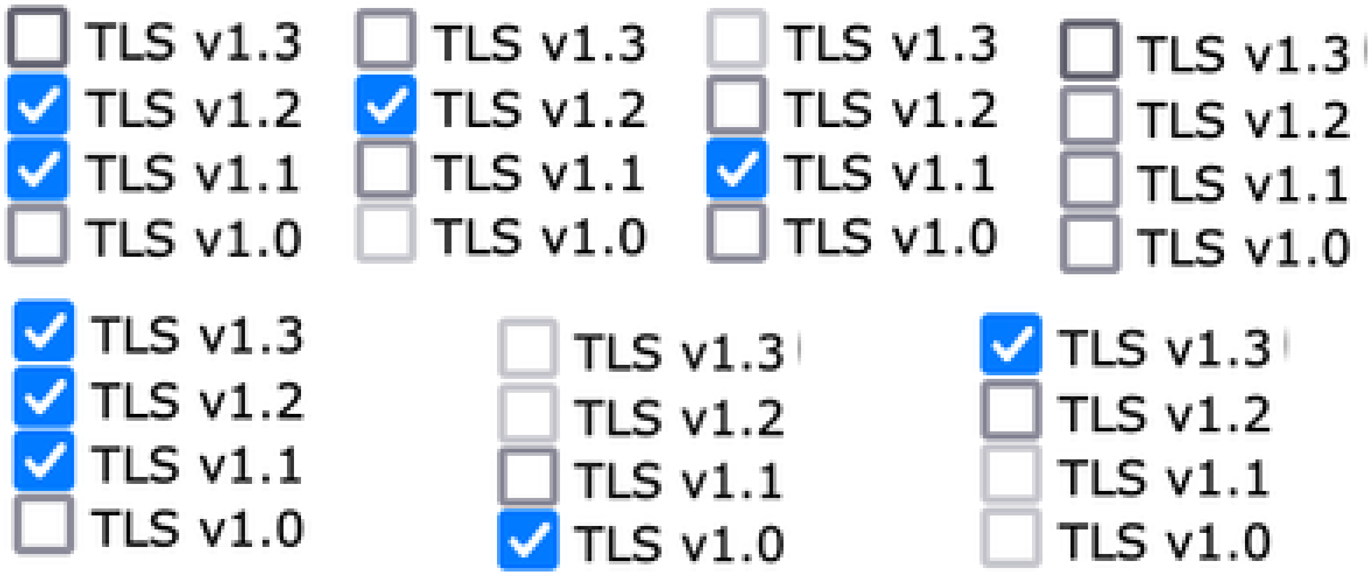
Note that the SSL/TLS service on remote servers may require that the selected TLS versions be sequential. So to avoid communications errors, always select a contiguous set of versions for each service. For example, do not enable TLS 1.0 and 1.2, while leaving TLS 1.1 disabled.

For the peer certificate FQDN validation for LDAP, ensure that you enable LDAP server certificate validation in LDAP Global Settings.

Appliance Management Web User Interface:	*Changing this option will disconnect all active Web User Interface connections on Commit. You will need to log in again.* Enable protocol versions: ☐ TLS v1.3 ☑ TLS v1.2 ☑ TLS v1.1 ☐ TLS v1.0
Secure LDAP Services:	*Secure LDAP services include Authentication and External Authentication.* Enable protocol versions: ☑ TLS v1.2 ☑ TLS v1.1 ☐ TLS v1.0
Updater Service:	Enable protocol versions: ☑ TLS v1.2 ☑ TLS v1.1 ☐ TLS v1.0
Peer Certificate FQDN Validation:	Used for Alert Over TLS, Updater and LDAP: ☐ Enable
Peer Certificate X509 Validation:	Used for Alert Over TLS, Updater and LDAP: ☐ Enable

Note: TLS1.0 is deprecated and thus disabled by default. TLS v1.0 is still available if the owner chooses to enable it.

- The checkbox options light up with bolded boxes presenting the available Protocols and Grayed Out boxes for non-compatible options.
- The sample options in the image illustrate the checkbox options for the Web User Interface.



☐ TLS v1.3
☑ TLS v1.2
☑ TLS v1.1
☐ TLS v1.0

☐ TLS v1.3
☑ TLS v1.2
☐ TLS v1.1
☐ TLS v1.0

☐ TLS v1.3
☐ TLS v1.2
☑ TLS v1.1
☐ TLS v1.0

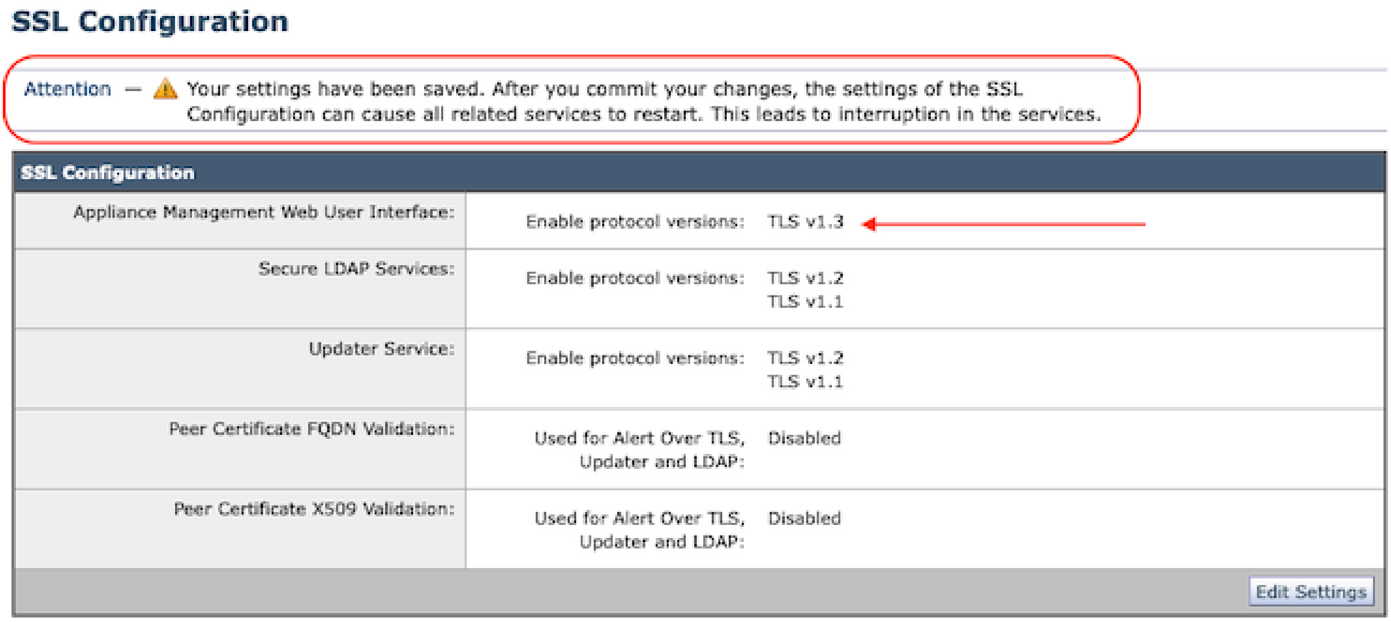
☐ TLS v1.3
☐ TLS v1.2
☐ TLS v1.1
☐ TLS v1.0

☑ TLS v1.3
☑ TLS v1.2
☑ TLS v1.1
☐ TLS v1.0

☐ TLS v1.3
☐ TLS v1.2
☐ TLS v1.1
☑ TLS v1.0

☑ TLS v1.3
☐ TLS v1.2
☐ TLS v1.1
☐ TLS v1.0

Note: Modifications to the SSL Configuration can cause related services to restart. it causes a short interruption to the WebUI Service.



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

Configuration from CLI

The EWM permits TLS v1.3 on one service: WebUI

sma1.example.com> **sslconfig**

Disabling SSLv3 is recommended for the best security.

Note that the SSL/TLS service on remote servers require that the selected TLS versions be sequential. So to avoid communication 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.

Choose the operation you want to perform:
- VERSIONS - Enable or disable SSL/TLS versions
- PEER_CERT_FQDN - Validate peer certificate FQDN compliance for Alert Over TLS, updater and LDAP.
- PEER_CERT_X509 - Validate peer certificate X509 compliance for Alert Over TLS, updater and LDAP.
[]> **versions**

Enable or disable SSL/TLS version for the services:

Updater - Update Service
WebUI - Appliance Management Web User Interface
LDAPS - Secure LDAP Services (including Authentication and External Authentication)

Note that TLSv1.3 is not available for Updater and LDAPS, only WebUI can be configured with TLSv1.3.

Currently enabled SSL/TLS versions by service: (Y : Enabled, N : Disabled)

```
        Updater   WebUI   LDAPS
TLSv1.0   N         N       N
TLSv1.1   Y         N       Y
TLSv1.2   Y         Y       Y
TLSv1.3  N/A        N      N/A
```

```
Select the service for which to enable/disable SSL/TLS versions:

1. Updater
2. WebUI
3. LDAPS
4. All Services
[]> 2

Currently enabled protocol(s) for WebUI are TLSv1.2.


To change the setting for a specific protocol, select an option below:

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

TLSv1.3 support for Appliance Management Web User Interface is currently disabled. Do you want to
enable it? [N]> y


Currently enabled protocol(s) for WebUI are TLSv1.3, TLSv1.2.


Choose the operation you want to perform:
- VERSIONS - Enable or disable SSL/TLS versions
- PEER_CERT_FQDN - Validate peer certificate FQDN compliance for Alert Over TLS, updater, and
LDAP.
- PEER_CERT_X509 - Validate peer certificate X509 compliance for Alert Over TLS, updater, and LDAP.
[]>

sma1.example.com> commit

Warning: Changes in SSL configuration cause the
these processes to restart after Commit - gui,euq_webui.
This causes a brief interruption in SMA operations.

Please enter some comments describing your changes:
[]> enable tls v1.3

Changes committed: Sun Jan 28 23:55:40 2024 EST
Restarting gui...
gui restarted
Restarting euq_webui...
euq_webui restarted
```

Wait a short time and confirm the WebUI is accessible.

Note: Selecting multiple versions of TLS for a service requires the user to select a service and a protocol version, then repeat the selection of a service and a protocol once more until all settings have been modified.

Verify

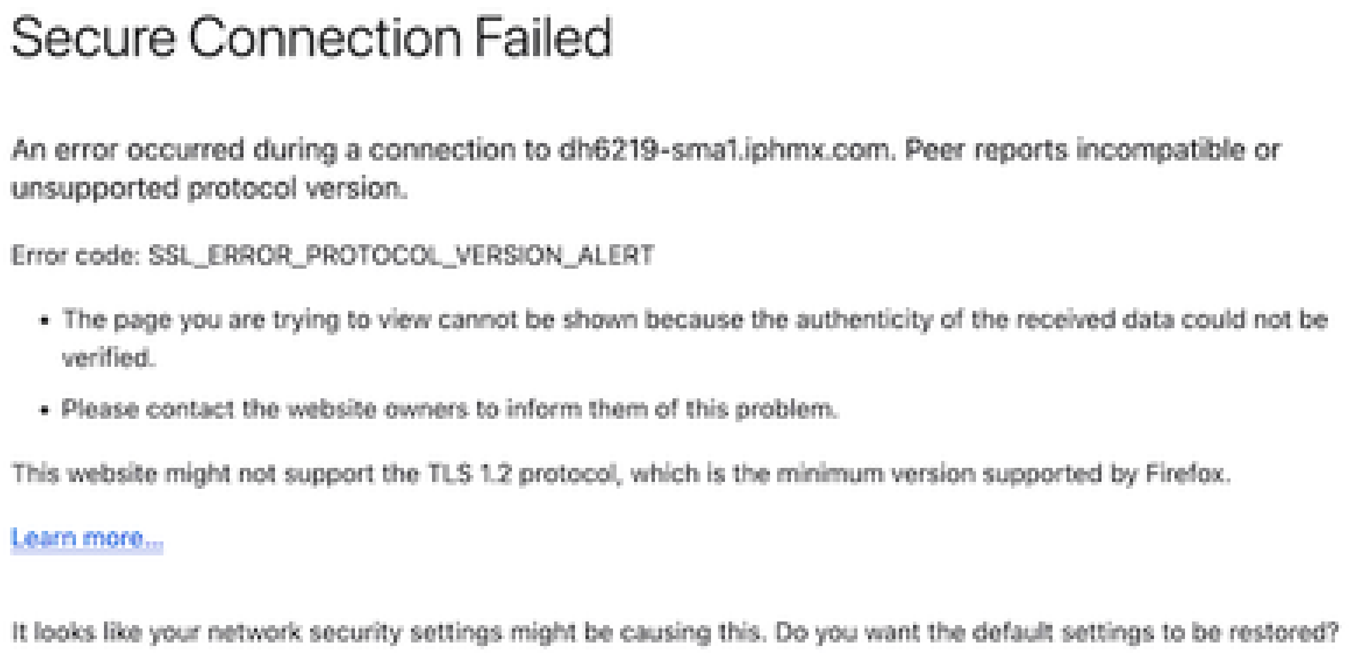
This section includes some basic test scenarios and the errors that present due to mismatched versions or syntax errors.

Verify browser functionality by opening a web browser session to the EWM WebUI or NGUI configured with TLSv1.3.

All the Web Browsers we tested are already configured to accept TLS v1.3.

- Sample set the browser setting on Firefox to disable TLS v1.3 support produces errors on both the ClassicUI and the NGUI of the appliance.

- Classic UI using Firefox configured to exclude TLS v1.3, as a test.
- NGUI would receive the same error with the only exception being the port number 4431(default) within the URL.



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.

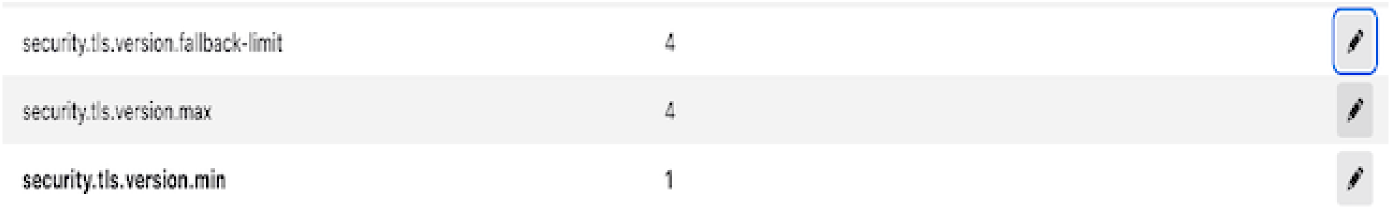
This website might not support the TLS 1.2 protocol, which is the minimum version supported by Firefox.

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 Failure

- To ensure communication Verify Browser settings to ensure TLSv1.3 is included. (This sample is from Firefox)



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

- Sample openssl command using a mistyped cipher value would give this error output: sample openssl connection test failure due to invalid cipher: Error with command: "-ciphersuites TLS_AES_256_GCM_SHA38**6**"

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

- Sample curl command executed to the ng-ui when TLS v1.3 is disabled generates this error.

```
curl: (35) CURL_SSLVERSION_MAX incompatible with CURL_SSLVERSION
```

Related Information

- Cisco Content Security Management Appliance - Release Notes
- Cisco Content Security Management Appliance - End-User Guides