

Configure TLSv1.3 for Secure Email Gateway

Contents

[Introduction](#)

[Prerequisites](#)

[Components Used](#)

[Overview](#)

[Configure](#)

[Configuration from the WebUI](#)

[CLI configuration:](#)

[Verify](#)

[Related Information](#)

Introduction

This document describes the configuration of TLS v1.3 protocol for Cisco Secure Email Gateway (SEG).

Prerequisites

A general knowledge of the SEG settings and configuration is desired.

Components Used

- The information in this document is based on these software and hardware versions:
 - Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 and newer.
- SEG 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 SEG has integrated TLS v1.3 protocol to encrypt communications for SMTP and HTTPS-Related services; Classic UI, NGUI, and Rest API.

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

The SEG uses the existing SSL Configuration method within the SEG WebUI or CLI of SSL with a few notable settings to highlight.

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

Configure

The SEG integrates the TLS v1.3 protocol for HTTPS and SMTP within AsyncOS 15.5. Caution is recommended when choosing the protocol settings to prevent HTTPS and email delivery/receiving failures.

Previous releases of the Cisco SEG support TLS v1.2 at the high end along with other email providers such as MS O365 supporting TLS v1.2 at the time the article was written.

The Cisco SEG implementation of the TLS v1.3 Protocol supports 3 default ciphers which cannot be changed or excluded within the SEG cipher configuration settings as the other protocols permit.

The existing SEG SSL Configuration settings still permit manipulation of the TLS v1.0, v1.1, v1.2 manipulation to cipher suites.

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 includes TLS v1.1 and TLS v1.2 only.
- The setting for "Other TLS Client Services" utilizes TLS v1.1 and TLS v1.2 with the option to select, only use TLS v1.0.

SSL Configuration		
GUI HTTPS:	Methods:	TLS v1.2 TLS v1.1
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!D ES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA! ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:-aNULL:- EXPORT:-IDEA:!DHE-RSA-AES128-CCM:!DHE-RSA- AES256-CCM:!DHE-RSA-AES256-SHA
	TLS Renegotiation:	Enabled
Inbound SMTP:	Methods:	TLS v1.2 TLS v1.1
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!D ES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA! ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:-aNULL:- EXPORT:-IDEA:!DHE-RSA-AES128-CCM:!DHE-RSA- AES256-CCM:!DHE-RSA-AES256-SHA
	TLS Renegotiation:	Enabled
Outbound SMTP:	Methods:	TLS v1.2 TLS v1.1
	SSL Cipher(s) to use:	ECDH+aRSA:ECDH+ECDSA:DHE+DSS+AES:AES128:A ES256:!3DES:!IDEA:!SRP:IAESGCM+DH+aRSA:IAESG CM+RSA:!aNULL:!eNULL:!kRSA:@STRENGTH:- aNULL:-EXPORT:-IDEA:!DHE-RSA-AES128-CCM:!DHE- RSA-AES256-CCM:!ECDHE-ECDSA-CAMELLIA128- SHA256:!ECDHE-RSA-CAMELLIA128-SHA256:!ECDHE- ECDSA-CAMELLIA256-SHA384:!ECDHE-RSA- CAMELLIA256-SHA384:!ECDHE-ECDSA-AES128- CCM:!ECDHE-ECDSA-AES256-CCM:!DHE-RSA-AES256- SHA
	Other TLS Client Services: ?	<div style="border: 1px solid red; padding: 5px; width: fit-content;"> <p>Other TLS Client Services x</p> <p>TLS method is applicable for the following services:</p> <p>LDAP Updater Client SMTP Call-Ahead Remote Syslog Server</p> </div>
Other TLS Client Services:	Methods:	TLS v1.2, TLS v1.1 are being used as default
Peer Certificate FQDN Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	Disabled
Peer Certificate X509 Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	Disabled

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

- TLS v1.1 and TLS v1.2 are checked with active boxes to select the other protocols.
- The ? next to each TLS v1.3 is a repeat of the static Cipher options.
- The "Other TLS Client Services:" now presents the option to utilize TLS v1.0 only if selected.

SSL Configuration		
GUI HTTPS:	Methods:	<input type="checkbox"/> TLS v1.3 ? <input checked="" type="checkbox"/> TLS v1.2 <input checked="" type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!e
	TLS Renegotiation:	<input checked="" type="checkbox"/> Enable
Inbound SMTP:	Methods:	<input type="checkbox"/> TLS v1.3 ? <input checked="" type="checkbox"/> TLS v1.2 <input checked="" type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!e
	TLS Renegotiation:	<input checked="" type="checkbox"/> Enable
Outbound SMTP:	Methods:	<input type="checkbox"/> TLS v1.3 ? <input checked="" type="checkbox"/> TLS v1.2 <input checked="" type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0
	SSL Cipher(s) to use:	ECDH+aRSA:ECDH+ECDSA:DHE+DSS+
Other TLS Client Services: ?	Methods:	<input type="checkbox"/> TLS v1.0
Peer Certificate FQDN Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	<input type="checkbox"/> Enable
Peer Certificate X509 Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	<input type="checkbox"/> Enable


TLsv1.3 Cipher Info
 TLsv1.3 uses the default ciphers. You do not need to configure any cipher for TLsv1.3.

Informational ? for TLS Default Ciphers

Note:
 TLS protocols can be enabled only in sequence.
 The configured SSL Cipher(s) do not apply to TLS 1.3. The TLS 1.3 protocol uses default ciphers.

The TLS protocol selection options include TLS v1.0, TLS v1.1, TLS v1.2, TLS v1.3.

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

 **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.

<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

Post commit sample view of the selected TLS Protocols.

SSL Configuration		
GUI HTTPS:	Methods:	TLS v1.3 [?] TLS v1.2
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!D ES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA! ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:-aNULL:- EXPORT:!IDEA:!DHE-RSA-AES256-SHA:!DHE-RSA- AES128-CCM:!DHE-RSA-AES256-CCM
	TLS Renegotiation:	Enabled
Inbound SMTP:	Methods:	TLS v1.3 [?] TLS v1.2 TLS v1.1 TLS v1.0
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!D ES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA! ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:-aNULL:- EXPORT:!IDEA:!DHE-RSA-AES256-SHA:!DHE-RSA- AES128-CCM:!DHE-RSA-AES256-CCM
	TLS Renegotiation:	Enabled
Outbound SMTP:	Methods:	TLS v1.3 [?] TLS v1.2 TLS v1.1
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!D ES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA! ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:-aNULL:- EXPORT:!IDEA:!DHE-RSA-AES256-SHA:!DHE-RSA- AES128-CCM:!DHE-RSA-AES256-CCM:!ECDHE-ECDSA- CAMELLIA128-SHA256:!ECDHE-RSA-CAMELLIA128- SHA256:!ECDHE-ECDSA-CAMELLIA256- SHA384:!ECDHE-RSA-CAMELLIA256-SHA384:!ECDHE- ECDSA-AES128-CCM:!ECDHE-ECDSA-AES256-CCM
Other TLS Client Services: [?]	Methods:	TLS v1.2, TLS v1.1 are being used as default
Peer Certificate FQDN Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	Disabled
Peer Certificate X509 Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	Disabled

[Edit Settings...](#)

 **Note:** Modifications to the GUI HTTPS TLS Protocol causes a short disconnect to the WebUI due to the https service reset.

CLI configuration:

The SEG permits TLS v1.3 on 3 services:

- GUI HTTPS
- Inbound SMTP
- Outbound SMTP

Executing the command `> sslconfig`, outputs the currently configured Protocols and ciphers for GUI HTTPS, Inbound SMTP, Outbound SMTP

- GUI HTTPS method: `tlsv1_0tlsv1_1tlsv1_2tlsv1_3`
- Inbound SMTP method: `tlsv1_0tlsv1_1tlsv1_2tlsv1_3`
- Outbound SMTP method: `tlsv1_1tlsv1_2tlsv1_3`

Choose the operation you want to perform:

- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.


- OUTBOUND - Edit Outbound SMTP ssl settings.

[]> **inbound**

Enter the inbound SMTP SSL method you want to use.

1. TLS v1.3
2. TLS v1.2
3. TLS v1.1
4. TLS v1.0

[2-4]> 1-3

 **Note:** The SEG selection process can include a single menu number such as 2, a range of menu numbers such as 1-4, or menu numbers separated by commas 1,2,3.

The CLI `sslconfig` subsequent prompts accept the existing value by pressing 'enter' or modifying the setting as desired.

Complete the change with the command `> commit >>` enter an optional comment if desired `>>` press "Enter" to complete the changes.

Verify

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

Sample log entry of an SEG outgoing SMTP negotiation generating a rejection due to destination unsupported TLS v1.3:

```
Wed Jan 17 20:41:18 2024 Info: DCID 485171 TLS deferring: (336151598, 'error:1409442E:SSL routines:ssl3
```

Sample log entry of a sending SEG receiving a successfully negotiated TLS v1.3:

```
Wed Jan 17 21:09:12 2024 Info: DCID 485206 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384
```


Sample log entry of a receiving SEG without TLS v1.3 enabled.

```
Wed Jan 17 20:11:06 2024 Info: ICID 1020004 TLS failed: (337678594, 'error:14209102:SSL routines:tls_ea
```

Receiving SEG-supported TLS v1.3

```
Wed Jan 17 21:09:12 2024 Info: ICID 1020089 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384
```

To verify your browser functionality, simply open a web browser session to the SEG WebUI or NGUI configured with TLSv1.3.

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

- Test: Configure the browser setting on Firefox disabling 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 dh6062-esa1.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?

- To ensure communication Verify Browser settings to ensure TLSv1.3 is included. (This sample is from Firefox and utilizes numbers 1-4

security.tls.version.fallback-limit	4
security.tls.version.max	4
security.tls.version.min	3

Related Information

- [Cisco Secure Email Gateway - Setup Guide](#)
- [Cisco Secure Email Gateway Launch Page to Support Guides](#)
- [Cisco Secure Email Gateway - Release Notes](#)