

# Configurar TLSv1.3 para Secure Email Gateway

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Componentes Utilizados](#)

[Overview](#)

[Configurar](#)

[Configuração da WebUI](#)

[Configuração de CLI:](#)

[Verificar](#)

[Informações Relacionadas](#)

---

## Introdução

Este documento descreve a configuração do protocolo TLS v1.3 para o Cisco Secure Email Gateway (SEG).

## Pré-requisitos

É desejável ter um conhecimento geral das definições e da configuração do SEG.

## Componentes Utilizados

- As informações neste documento são baseadas nestas versões de software e hardware:
  - Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 e mais recente.
- Definições de Configuração SSL do SEG.

"As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que você compreende o impacto potencial de qualquer comando."

## Overview

O SEG integrou o protocolo TLS v1.3 para criptografar comunicações para SMTP e serviços relacionados a HTTPS; interface de usuário clássica, NGUI e API Rest.

O protocolo TLS v1.3 apresenta comunicação mais segura e negociação mais rápida à medida que a indústria trabalha para torná-lo o padrão.

O SEG usa o método de configuração SSL existente no SEG WebUI ou CLI do SSL com algumas configurações notáveis para destacar.

- Recomendações de precaução ao configurar os protocolos permitidos.
- As Cifras não podem ser manipuladas.
- O TLS v1.3 pode ser configurado para a GUI HTTPS, e-mail de entrada e e-mail de saída.
- As opções de seleção da caixa de verificação do protocolo TLS entre TLS v1.0 a TLS v1.3 usam um padrão ilustrado em mais detalhes no artigo.

## Configurar

O SEG integra o protocolo TLS v1.3 para HTTPS e SMTP no AsyncOS 15.5. É recomendável ter cuidado ao escolher as configurações do protocolo para evitar falhas de HTTPS e de entrega/recebimento de e-mail.

Versões anteriores do Cisco SEG suportam TLS v1.2 no high-end junto com outros provedores de e-mail como MS O365 suportando TLS v1.2 no momento em que o artigo foi escrito.

A implementação SEG da Cisco do protocolo TLS v1.3 suporta 3 cifras padrão que não podem ser alteradas ou excluídas dentro das definições de configuração de cifra SEG como os outros protocolos permitem.

As definições de Configuração SSL do SEG existentes ainda permitem a manipulação da manipulação de TLS v1.0, v1.1 e v1.2 para pacotes de codificação.

Cifras TLS 1.3:

TLS\_AES\_256\_GCM\_SHA384

TLS\_CHACHA20\_POLY1305\_SHA256

TLS\_AES\_128\_GCM\_SHA256

## Configuração a partir da WebUI

Navegue até > Administração do sistema > Configuração de SSL

- A seleção padrão do protocolo TLS após a atualização para o AsyncOS 15.5 inclui apenas TLS v1.1 e TLS v1.2.
- A configuração para "Outros serviços de cliente TLS" utiliza TLS v1.1 e TLS v1.2 com a opção de selecionar, usar apenas 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: ?	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

**Other TLS Client Services**

TLS method is applicable for the following services:

- LDAP
- Updater Client
- SMTP Call-Ahead
- Remote Syslog Server

Default TLS Selections

Selecione "Edit Settings" (Editar configurações) para apresentar as opções de configuração.


- TLS v1.1 e TLS v1.2 são marcados com caixas ativas para selecionar os outros protocolos.
- O ? ao lado de cada TLS v1.3 é uma repetição das opções de Cifra estática.
- A opção "Outros serviços de cliente TLS:" agora apresenta a opção de utilizar o TLS v1.0 somente se selecionado.

SSL Configuration	
GUI HTTPS:	Methods: <input type="checkbox"/> TLS v1.3 <sup>?</sup> <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:	<div style="border: 1px solid gray; padding: 2px; width: fit-content;"> <b>TLSv1.3 Cipher Info</b>  <small>TLSv1.3 uses the default ciphers. You do not need to configure any cipher for TLSv1.3.</small> </div> <p style="color: red; margin-left: 20px;">Informational ? for TLS Default Ciphers</p> Methods: <input type="checkbox"/> TLS v1.3 <sup>?</sup> <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 <sup>?</sup> <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: <sup>?</sup>	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

*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.

As opções de seleção de protocolo TLS incluem TLS v1.0, TLS v1.1, TLS v1.2, TLS v1.3.

- Após a atualização para o AsyncOS 15.5, somente os protocolos TLS v1.1 e TLS v1.2 são selecionados por padrão.

 **Observação:** o TLS1.0 é preterido e, portanto, desabilitado por padrão. O TLS v1.0 ainda estará disponível se o proprietário optar por ativá-lo.

- As opções da caixa de seleção acendem com caixas em negrito, apresentando as caixas Protocolos disponíveis e Esmacido, para opções incompatíveis.
- As opções de exemplo na imagem ilustram as opções da caixa de seleção.

<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

Visualização de exemplo pós-confirmação dos protocolos TLS selecionados.

SSL Configuration		
GUI HTTPS:	Methods:	TLS v1.3 <sup>?</sup> 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 <sup>?</sup> 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 <sup>?</sup> 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: <sup>?</sup>	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...](#)

 Observação: as modificações no protocolo TLS HTTPS da GUI causam uma breve desconexão com a WebUI devido à redefinição do serviço https.

## Configuração de CLI:

O SEG permite TLS v1.3 em 3 serviços:

- HTTPS DA GUI
- SMTP de entrada
- SMTP de saída

A execução do comando `> sslconfig`, gera os protocolos e as cifras configurados no momento para a GUI HTTPS, SMTP de entrada, SMTP de saída

- Método HTTPS da GUI: `tlsv1_0tlsv1_1tlsv1_2tlsv1_3`
- Método SMTP de entrada: `tlsv1_0tlsv1_1tlsv1_2tlsv1_3`
- Método SMTP de saída: `tlsv1_1tlsv1_2tlsv1_3`

Escolha a operação que deseja executar:

- GUI - Editar GUI HTTPS ssl configurações.
- INBOUND - Edite as configurações de ssl SMTP de Entrada.
- OUTBOUND - Edite as configurações de ssl SMTP de Saída.


[ ]> entrada

Insira o método SSL SMTP de entrada que deseja usar.

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

[2-4]> 1-3

---

 Observação: o processo de seleção de SEG pode incluir um único número de menu, como 2, uma faixa de números de menu, como 1-4, ou números de menu separados por vírgulas 1,2,3.

---

Os prompts subsequentes do `sslconfig` da CLI aceitam o valor existente pressionando 'enter' ou modificando a configuração conforme desejado.

Conclua a alteração com o comando `> commit >>` insira um comentário opcional se desejar `>>` pressione "Enter" para concluir as alterações.

## Verificar

Esta seção inclui alguns cenários básicos de teste e erros que podem ser apresentados devido a versões incompatíveis do protocolo TLS ou erros de sintaxe.

Exemplo de entrada de log de uma negociação SMTP de saída SEG que gera uma rejeição

devido a um TLS v1.3 de destino sem suporte:

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

Exemplo de entrada de log de um SEG emissor que recebe um TLS v1.3 negociado com êxito:

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

Exemplo de entrada de log de um SEG receptor sem TLS v1.3 habilitado.


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

Recebimento de TLS v1.3 suportado por SEG

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

Para verificar a funcionalidade do seu navegador, basta abrir uma sessão do navegador da Web no SEG WebUI ou NGUI configurado com TLSv1.3.

---

 Observação: todos os navegadores da Web testados já estão configurados para aceitar TLS v1.3.

---

- Teste: defina a configuração do navegador no Firefox desabilitando o suporte TLS v1.3 produz erros na ClassicUI e na NGUI do dispositivo.
- Interface de usuário clássica usando o Firefox configurada para excluir TLS v1.3, como um teste.
- A NGUI receberia o mesmo erro, com a única exceção sendo o número de porta 4431 (padrão) no 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?

- Para garantir a comunicação, verifique as configurações do navegador para garantir que TLSv1.3 esteja incluído. (Este exemplo é do Firefox e utiliza números de 1 a 4

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

## Informações Relacionadas

- [Cisco Secure Email Gateway - Guia de configuração](#)
- [Página inicial do Cisco Secure Email Gateway para guias de suporte](#)
- [Cisco Secure Email Gateway - Notas de versão](#)



## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.