Konfigurieren von TLSv1.3 für Secure Email Gateway

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration des TLS v1.3-Protokolls für Cisco Secure Email Gateway (SEG) beschrieben.

Voraussetzungen

Eine allgemeine Kenntnis der SEG Einstellungen und Konfiguration ist erwünscht.

Verwendete Komponenten

- Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:
  - Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 und höher
- SEG SSL-Konfigurationseinstellungen.

"Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen aller Befehle verstehen."

Überblick

Die SEG verfügt über ein integriertes TLS v1.3-Protokoll zur Verschlüsselung der Kommunikation für SMTP- und HTTPS-bezogene Dienste, die klassische Benutzeroberfläche, die Benutzeroberfläche und die Rest-API.

Das TLS v1.3 Protocol bietet eine sicherere Kommunikation und schnellere Verhandlungen, da die Branche daran arbeitet, es zum Standard zu machen.

Die SEG verwendet die vorhandene SSL-Konfigurationsmethode innerhalb der SEG WebUI oder CLI von SSL mit einigen bemerkenswerten Einstellungen, um diese hervorzuheben.

- Sicherheitshinweise bei der Konfiguration der zulässigen Protokolle
- Die Chiffren können nicht manipuliert werden.
- TLS v1.3 kann für GUI HTTPS, eingehende und ausgehende E-Mails konfiguriert werden.
- Die Auswahloptionen für das TLS-Protokoll-Kontrollkästchen zwischen TLS v1.0 und TLS v1.3 verwenden ein Muster, das im Artikel detaillierter dargestellt wird.

Konfigurieren

Die SEG integriert das TLS v1.3-Protokoll für HTTPS und SMTP in AsycOS 15.5. Bei der Auswahl der Protokolleinstellungen ist Vorsicht geboten, um HTTPS- und E-Mail-Zustellungs-/Empfangsfehler zu vermeiden.

Frühere Versionen von Cisco SEG unterstützen zum Zeitpunkt der Erstellung des Artikels TLS v1.2 im High-End-Bereich sowie andere E-Mail-Anbieter wie MS O365, die TLS v1.2 unterstützen.

Die Cisco SEG-Implementierung des TLS v1.3-Protokolls unterstützt drei Standardchiffren, die nicht innerhalb der SEG-Chiffrierkonfigurationseinstellungen geändert oder ausgeschlossen werden können, wie dies die anderen Protokolle zulassen.

Die vorhandenen SEG SSL-Konfigurationseinstellungen erlauben weiterhin die Manipulation von TLS v1.0, v1.1, v1.2 an Verschlüsselungssuiten.

TLS 1.3-Verschlüsselungen:

TLS_AES_256_GCM_SHA384

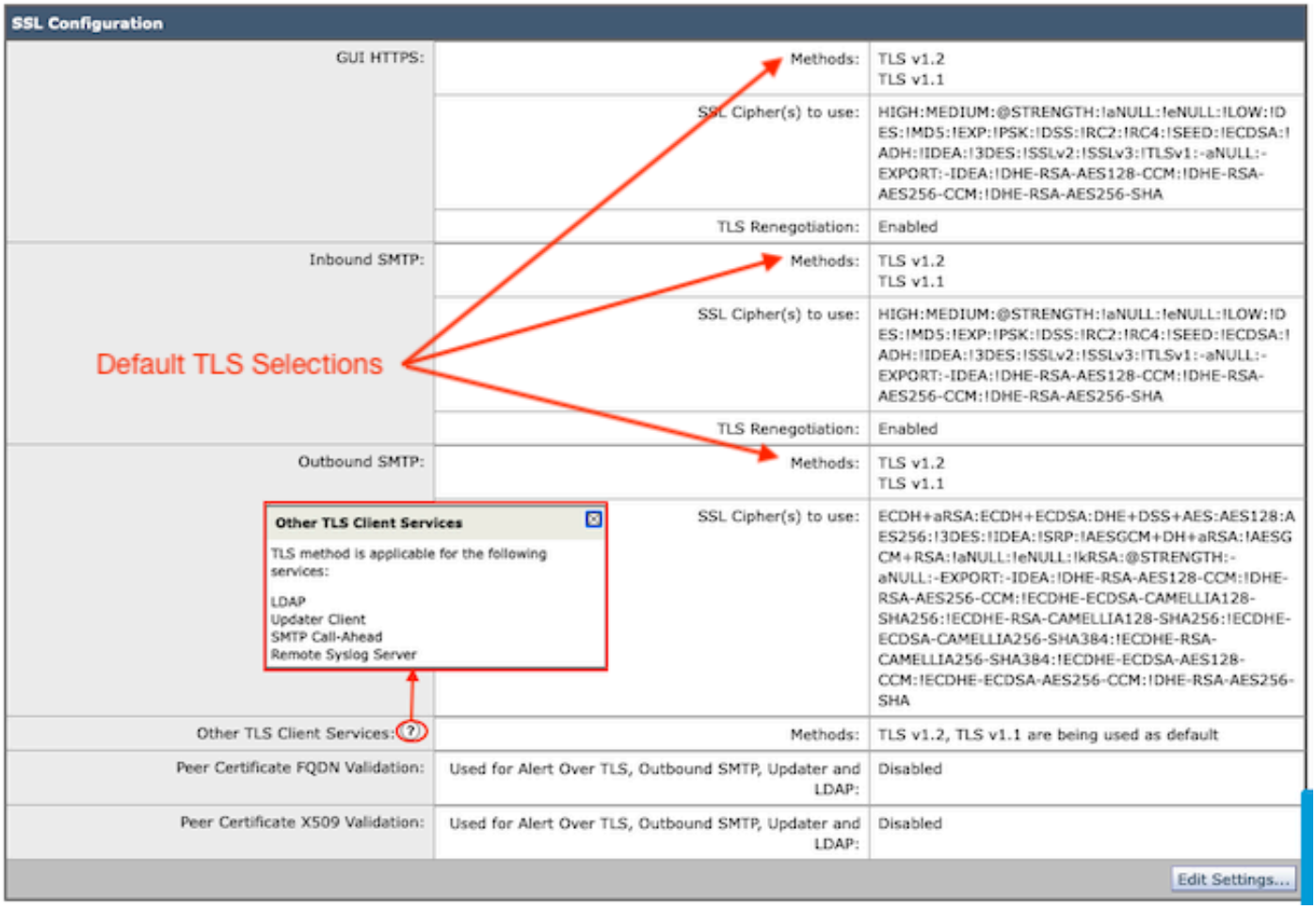
TLS_CHACHA20_POLY1305_SHA256

TLS_AES_128_GCM_SHA256

Konfiguration über die WebUI

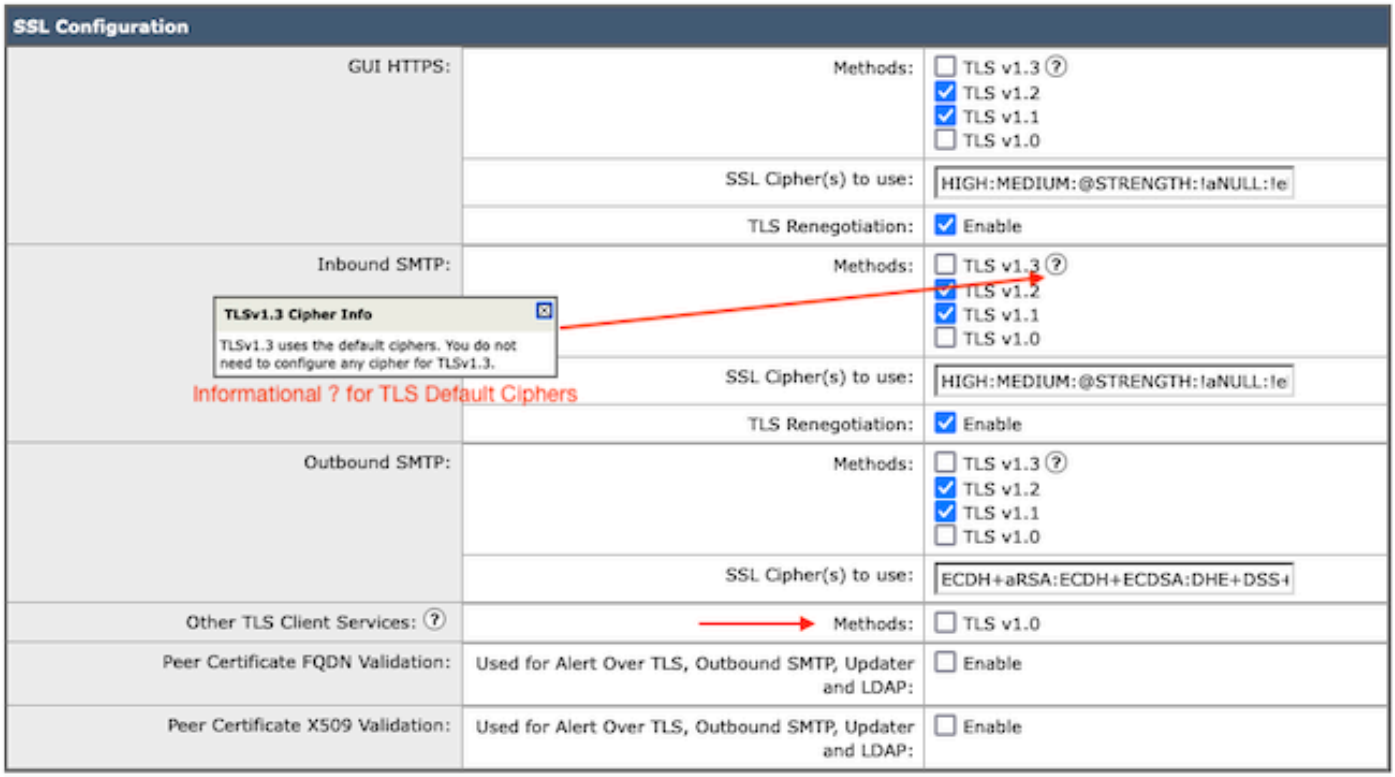
Navigieren Sie zu > Systemverwaltung > SSL-Konfiguration

- Die standardmäßige TLS-Protokollauswahl nach dem Upgrade auf 15.5 AsyncOS enthält nur TLS v1.1 und TLS v1.2.
- Die Einstellung für "Other TLS Client Services" (Andere TLS-Client-Services) verwendet TLS v1.1 und TLS v1.2, wobei die Option ausgewählt ist und nur TLS v1.0 verwendet wird.



Wählen Sie "Einstellungen bearbeiten", um die Konfigurationsoptionen anzuzeigen.

- TLS v1.1 und TLS v1.2 sind mit aktiven Kontrollkästchen aktiviert, um die anderen Protokolle auszuwählen.
- Das ? neben jedem TLS v1.3 ist eine Wiederholung der statischen Cipher-Optionen.
- Im Fenster "Other TLS Client Services:" (Andere TLS-Clientdienste) wird nun die Option zur ausschließlichen Verwendung von TLS v1.0 angezeigt, wenn diese Option ausgewählt ist.



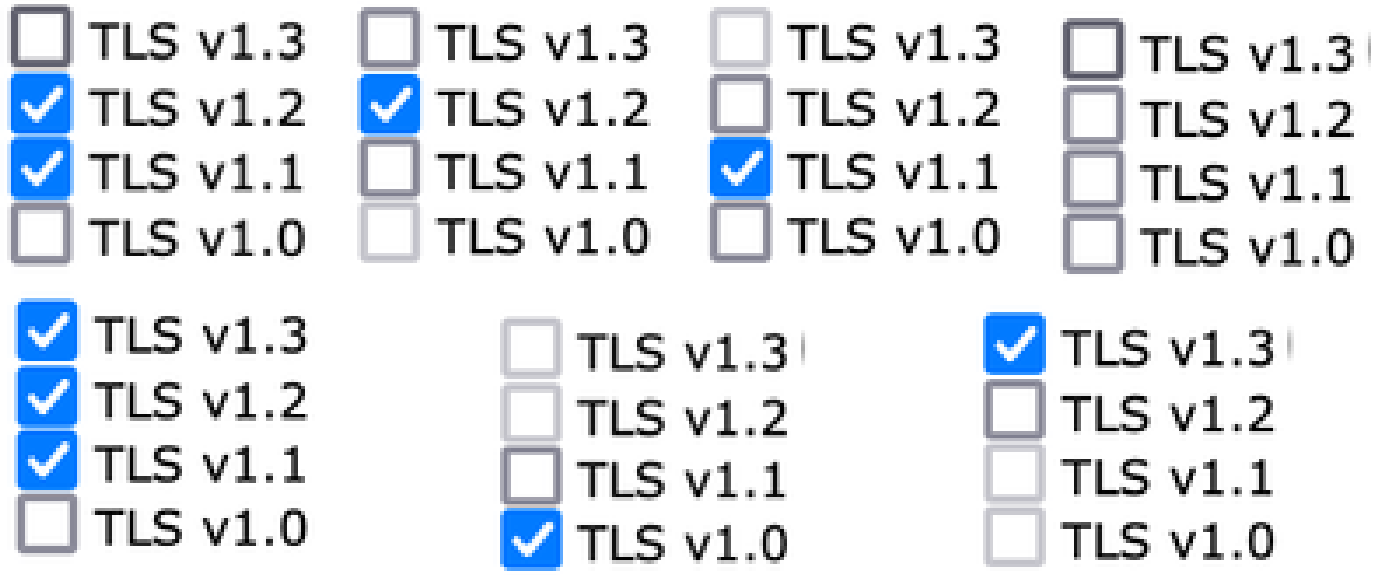
Note:
TLS protocols can be enabled only in sequence.
The configured SSL Cipher(s) do not apply to TLS 1.3. The TLS 1.3 protocol uses default ciphers.

Die Optionen zur Auswahl des TLS-Protokolls umfassen TLS v1.0, TLS v1.1, TLS v1.2 und TLS v1.3.

- Nach dem Upgrade auf AsyncOS 15.5 sind standardmäßig nur die Protokolle TLS v1.1 und TLS v1.2 ausgewählt.

Hinweis: TLS1.0 ist veraltet und daher standardmäßig deaktiviert. TLS v1.0 ist weiterhin verfügbar, wenn der Besitzer die Option aktiviert.

- Die Kontrollkästchen werden durch Fettformatierungen mit den verfügbaren Protokollen und Graustufen für nicht kompatible Optionen angezeigt.
- Die Beispieloptionen im Bild veranschaulichen die Optionen des Kontrollkästchens.



Nach dem Übertragen der Stichprobenansicht der ausgewählten TLS-Protokolle.

SSL Configuration

GUI HTTPS:	Methods:	TLS v1.3 TLS v1.2
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!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:!DES:!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:!DES:!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...

Hinweis: Änderungen am HTTPS TLS-Protokoll der Benutzeroberfläche führen zu einer kurzen Unterbrechung der Verbindung zur WebUI, da der HTTPS-Dienst zurückgesetzt wird.

CLI-Konfiguration:

Die SEG lässt TLS v1.3 für drei Dienste zu:

- GUI HTTPS
- Eingehendes SMTP
- SMTP ausgehend

Mit dem Befehl **>** sslconfig werden die aktuell konfigurierten Protokolle und Chiffren für GUI HTTPS, Inbound SMTP, Outbound SMTP ausgegeben

- GUI - HTTPS-Methode: tlsv1_0tlsv1_1tlsv1_2tlsv1_3
- Eingehende SMTP-Methode: tlsv1_0tlsv1_1tlsv1_2tlsv1_3
- Ausgehende SMTP-Methode: tlsv1_1tlsv1_2tlsv1_3

Wählen Sie den Vorgang aus, den Sie ausführen möchten:

- GUI - GUI-HTTPS-SSL-Einstellungen bearbeiten.
- INBOUND - Dient zum Bearbeiten eingehender SMTP SSL-Einstellungen.
- OUTBOUND - Dient zum Bearbeiten der ausgehenden SMTP-SSL-Einstellungen.

[]**>** Eingehend

Geben Sie die eingehende SMTP-SSL-Methode ein, die Sie verwenden möchten.

1. TLS v1.3
2. TLS v1.2
3. TLS Version 1.1
4. TLS Version 1.0

[2-4]**>** 1-3

Hinweis: Der SEG-Auswahlprozess kann eine einzelne Menünummer (z. B. 2), einen Bereich von Menünummern (z. B. 1-4) oder durch Kommas getrennte Menünummern (z. B. 1, 2, 3) enthalten.

Die nachfolgenden CLI sslconfig-Eingabeaufforderungen akzeptieren den vorhandenen Wert, indem sie die Eingabetaste drücken oder die Einstellung wie gewünscht ändern.

Vervollständigen Sie die Änderung mit dem Befehl **>** commit **>>** geben Sie bei Bedarf einen optionalen Kommentar ein **>>** drücken Sie die Eingabetaste, um die Änderungen abzuschließen.

Überprüfung

Dieser Abschnitt enthält einige grundlegende Testszenarien und Fehler, die aufgrund von nicht übereinstimmenden TLS-Protokollversionen oder Syntaxfehlern auftreten können.

Beispiel für einen Protokolleintrag einer ausgehenden SEG-SMTP-Verhandlung, der eine

Ablehnung aufgrund des nicht unterstützten TLS v1.3-Ziels generiert:

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

Beispiel für einen Protokolleintrag einer sendenden SEG, die ein erfolgreich ausgehandeltes TLS v1.3 empfängt:

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

Beispiel-Protokolleintrag eines empfangenden SEGs ohne aktivierte TLS v1.3.

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

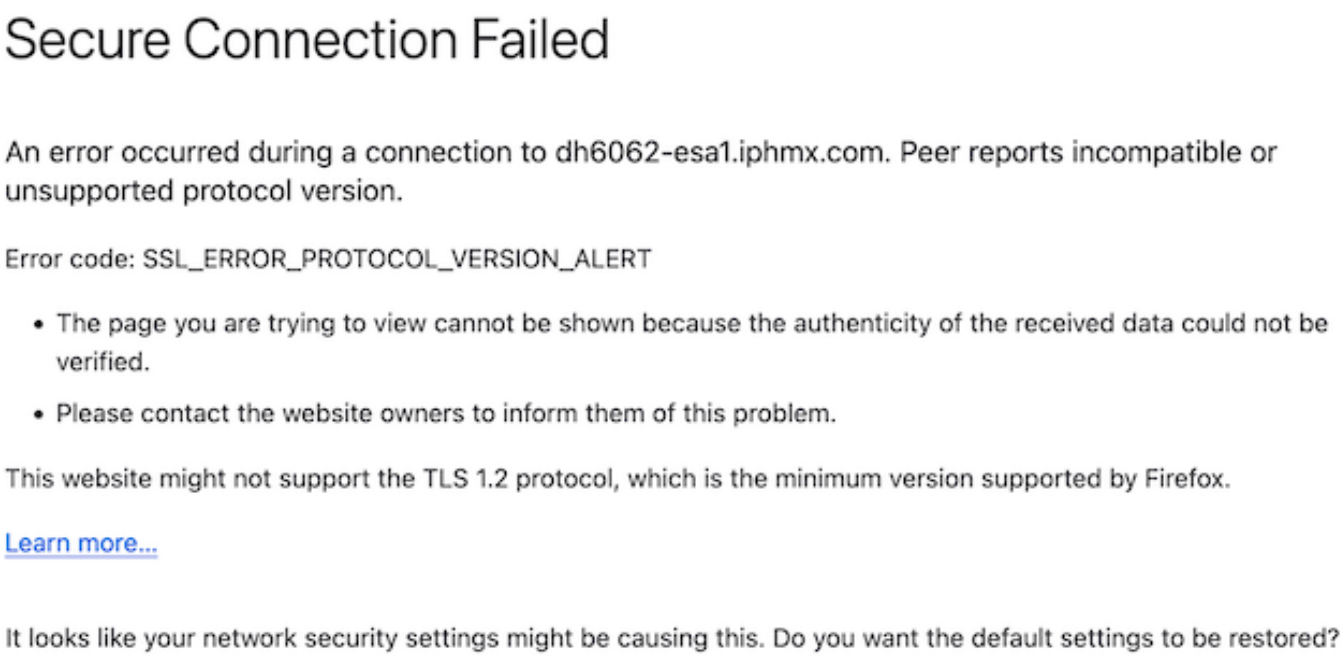
Empfangen von SEG-unterstütztem TLS v1.3

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

Öffnen Sie zur Überprüfung Ihrer Browser-Funktionalität einfach eine Webbrowser-Sitzung mit der SEG WebUI oder NGUI, die mit TLSv1.3 konfiguriert wurde.

Hinweis: Alle von uns getesteten Webbrowser sind bereits für die Annahme von TLS v1.3 konfiguriert.

- Test: Konfigurieren Sie die Browsereinstellung bei Firefox, indem Sie die TLS v1.3-Unterstützung deaktivieren, und es werden Fehler sowohl in der ClassicUI als auch in der NGUI der Appliance erzeugt.
- Klassische Benutzeroberfläche, die Firefox verwendet und so konfiguriert ist, dass TLS v1.3 als Test ausgeschlossen wird.
- NGUI würde den gleichen Fehler erhalten, mit der einzigen Ausnahme, dass die Port-Nummer 4431 (Standard) innerhalb der URL lautet.



- Überprüft die Browser-Einstellungen, um sicherzustellen, dass TLSv1.3 enthalten ist. (Dieses Beispiel stammt von Firefox und verwendet die Zahlen 1-4

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

Zugehörige Informationen

- Cisco Secure Email Gateway - Einrichtungsleitfaden
- Cisco Secure Email Gateway Launch-Website für Support-Leitfäden
- Cisco Secure Email Gateway - Versionshinweise

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.