Konfigurieren von TLSv1.3 für Secure Email Web Manager

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration des TLS v1.3-Protokolls für Cisco Secure Email und Web Manager (EWM) beschrieben

Voraussetzungen

Allgemeine Kenntnisse der SEWM Einstellungen und Konfiguration sind erwünscht.

Verwendete Komponenten

- Cisco Secure Email Web Manager (SEWM) AsyncOS 15.5.1 und höher
- 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

Das SEWM verfügt über ein integriertes TLS v1.3-Protokoll zur Verschlüsselung der Kommunikation für 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 danach strebt, das Protokoll zum Standard zu machen.

Der SEWM verwendet die vorhandene SSL-Konfigurationsmethode innerhalb der SEGWebUI oder CLI von SSL mit einigen wichtigen Einstellungen, um diese hervorzuheben.

- Sicherheitshinweise bei der Konfiguration der zulässigen Protokolle
- Die TLS v1.3-Chiffren können nicht verändert werden.
- TLS v1.3 kann nur für GUI-HTTPS 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

SEWM hat das TLS v1.3-Protokoll für HTTPS in AsycOS 15.5 integriert.

Bei der Auswahl der Protokolleinstellungen ist Vorsicht geboten, um HTTPS-Fehler zu vermeiden.

Webbrowser-Unterstützung für TLS v1.3 ist weit verbreitet, obwohl in einigen Umgebungen Anpassungen erforderlich sind, um auf das SEWM zuzugreifen.

Die Cisco SEWM-Implementierung des TLS v1.3-Protokolls unterstützt drei Standardchiffren, die innerhalb des SEWM nicht geändert oder ausgeschlossen werden können.

TLS 1.3-Verschlüsselungen:

TLS_AES_256_GCM_SHA384

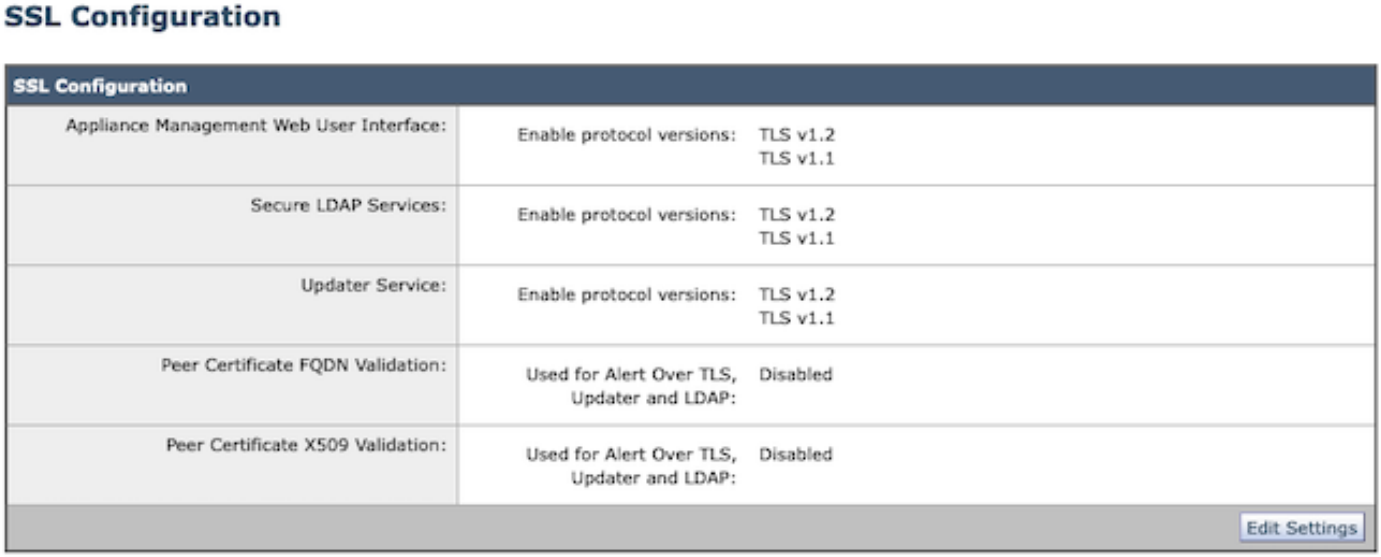
TLS_CHACHA20_POLY1305_SHA256

TLS_AES_128_GCM_SHA256

Konfiguration über die WebUI

Navigieren Sie zu > Systemverwaltung > SSL-Konfiguration

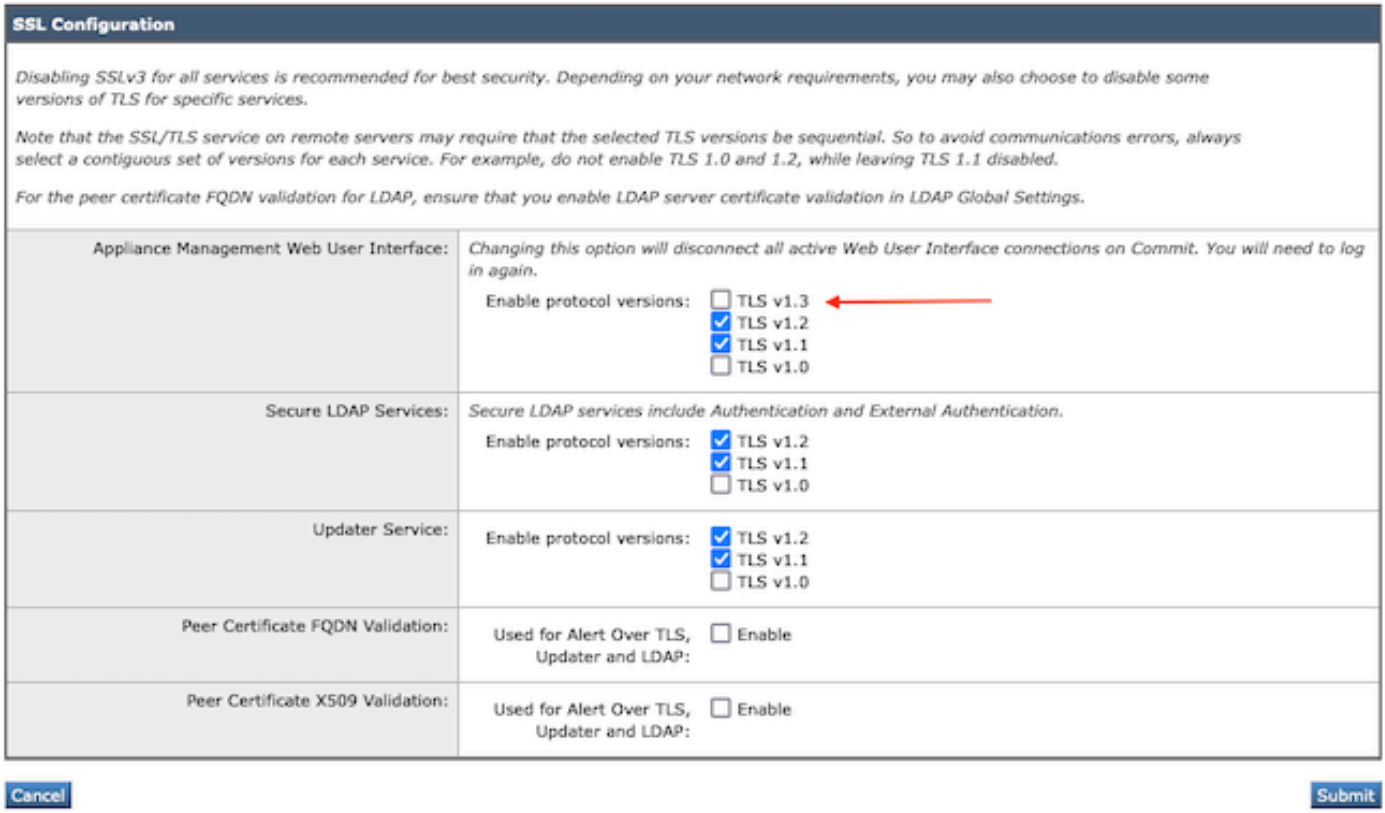
- Die standardmäßige TLS-Protokollauswahl nach dem Upgrade auf 15.5 AsyncOS HTTPS umfasst nur TLS v1.1 und TLS v1.2.
- Die beiden zusätzlichen Dienste Secure LDAP Services und Updater Services unterstützen TLS v1.3 nicht.



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

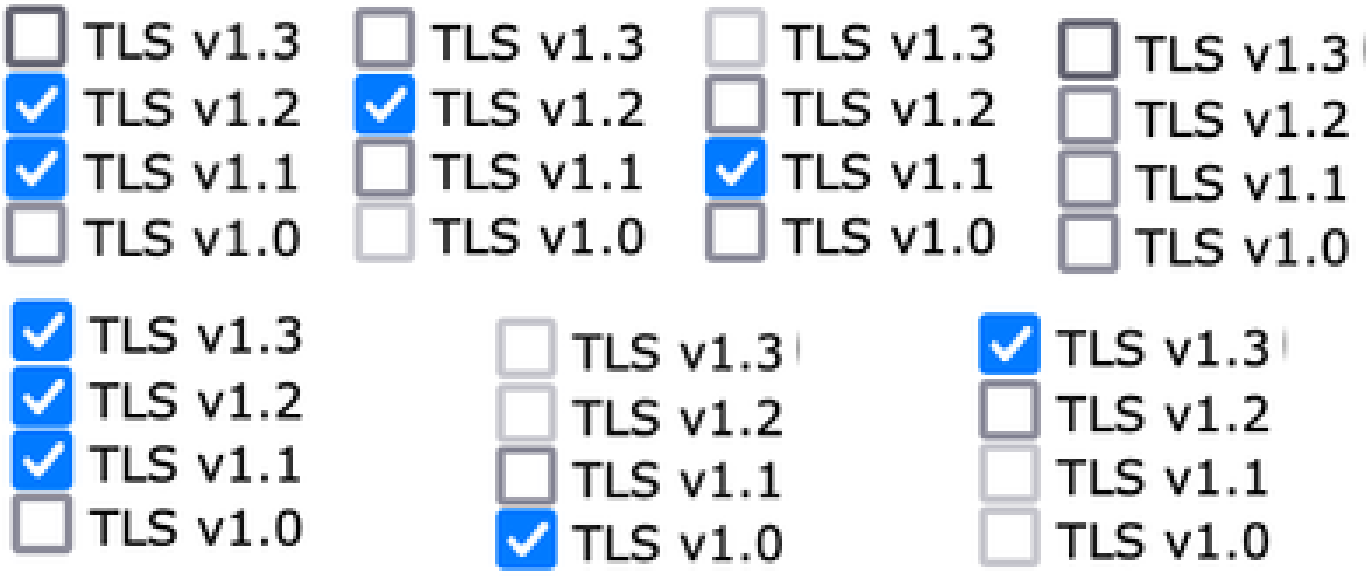
Die Optionen zur Auswahl des TLS-Protokolls für "Web User Interface" umfassen TLS v1.0, TLS v1.1, TLS v1.2 und TLS v1.3.

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

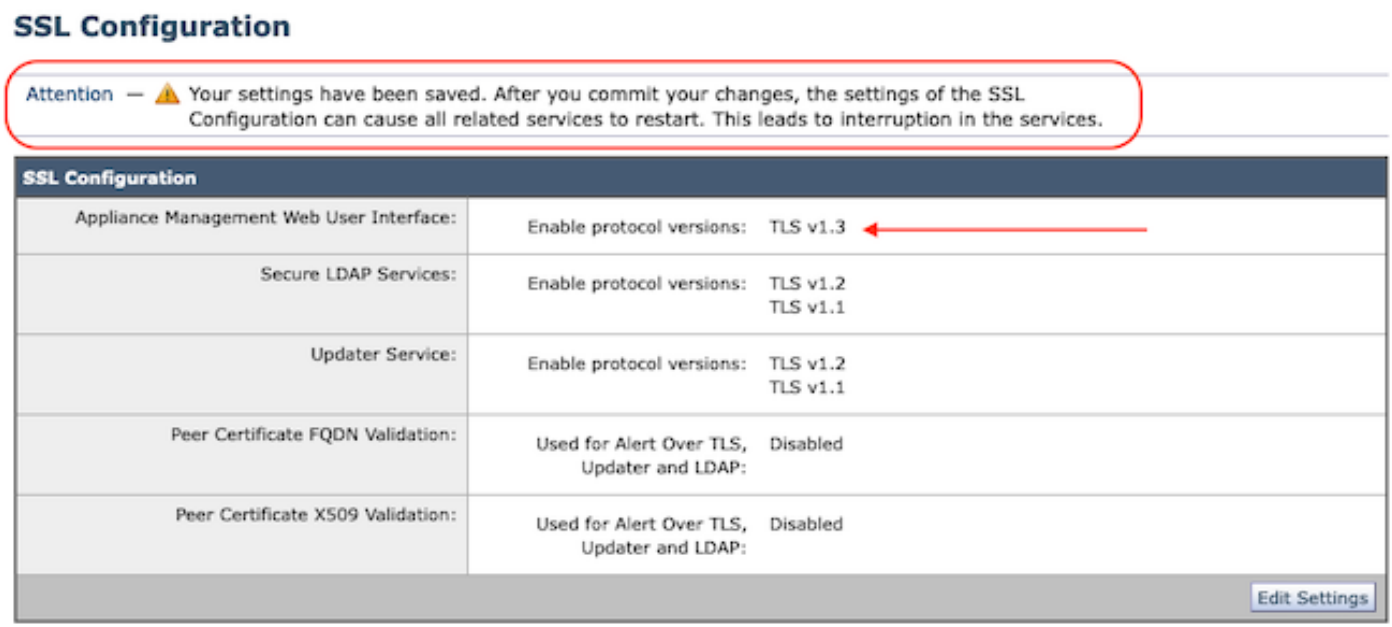


Hinweis: TLS1.0 ist veraltet und daher standardmäßig deaktiviert. TLS v1.0 ist weiterhin verfügbar, wenn der Besitzer die Option aktiviert.

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



Hinweis: Änderungen an der SSL-Konfiguration können dazu führen, dass verwandte Dienste neu gestartet werden. Dies führt zu einer kurzen Unterbrechung des WebUI-Diensts.



Konfiguration über CLI

EWM lässt TLS v1.3 für einen Dienst zu: WebUI

sma1.example.com> sslconfig

Die Deaktivierung von SSLv3 wird aus Sicherheitsgründen empfohlen.

Beachten Sie, dass der SSL/TLS-Dienst auf Remote-Servern sequenzielle TLS-Versionen erfordert. Um Kommunikationsfehler zu vermeiden, wählen Sie immer eine zusammenhängende für jeden Dienst eine Versionsgruppe. Aktivieren Sie beispielsweise nicht TLS 1.0 und 1.2, während TLS 1.1 deaktiviert bleibt.

Wählen Sie den Vorgang aus, den Sie ausführen möchten:
- VERSIONEN - Aktivieren oder Deaktivieren von SSL/TLS-Versionen
- PEER_CERT_FQDN - Validiert die FQDN-Konformität des Peer-Zertifikats für Alert Over TLS, Updater und LDAP.
- PEER_CERT_X509 - Validiert die X509-Kompatibilität des Peer-Zertifikats für Alert Over TLS, Updater und LDAP.
[]> Versionen

Aktivieren oder deaktivieren Sie die SSL/TLS-Version für die Services:

Aktualisierungsdienst
WebUI - Web-Benutzeroberfläche für die Appliance-Verwaltung
LDAPS = Secure LDAP Services (einschließlich Authentifizierung und externer Authentifizierung)

Beachten Sie, dass TLSv1.3 nicht für Updater und LDAPS verfügbar ist, nur WebUI kann mit

TLSv1.3 konfiguriert werden.

Derzeit aktivierte SSL/TLS-Versionen nach Dienst: (J: Aktiviert, N: Deaktiviert)

LDAP-Aktualisierungsmodul für WebUI
TLSv1.0 N N N N
TLSv1.1 Y N J
TLSv1.2 J J J J
TLSv1.3 N/A N/A

Wählen Sie den Service aus, für den SSL/TLS-Versionen aktiviert/deaktiviert werden sollen:

1. Aktualisierungsmodul
2. WebUI
3. LDAPS
4. Alle Dienste
[]> 2

Derzeit aktivierte(s) Protokoll(e) für WebUI sind TLSv1.2.

Wählen Sie eine der folgenden Optionen aus, um die Einstellung für ein bestimmtes Protokoll zu ändern:

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

Die TLSv1.3-Unterstützung für die Web-Benutzeroberfläche der Appliance-Verwaltung ist aktuell deaktiviert. Möchten Sie sie aktivieren? [N]> J

Derzeit aktivierte Protokolle für die WebUI sind TLSv1.3 und TLSv1.2.

Wählen Sie den Vorgang aus, den Sie ausführen möchten:
- VERSIONEN - Aktivieren oder Deaktivieren von SSL/TLS-Versionen
- PEER_CERT_FQDN - Validiert die FQDN-Konformität des Peer-Zertifikats für Alert Over TLS, Updater und LDAP.
- PEER_CERT_X509 - Validiert die X509-Kompatibilität des Peer-Zertifikats für Alert Over TLS, Updater und LDAP.
[]>

sma1.example.com> commit

Warnung: Änderungen an der SSL-Konfiguration verursachen die

diese Prozesse nach Commit neu starten - gui,euq_webui.
Dies führt zu einer kurzzeitigen Unterbrechung des SMA-Betriebs.

Bitte geben Sie Kommentare ein, die Ihre Änderungen beschreiben:
[]> TLS v1.3 aktivieren

Änderungen übernommen: So Jan 28 23:55:40 2024 EST
GUI wird neu gestartet...
GUI neu gestartet
euq_webui wird neu gestartet...
euq_webui neu gestartet

Warten Sie einen Moment, und stellen Sie sicher, dass auf die WebUI zugegriffen werden kann.

Hinweis: Wenn Sie mehrere TLS-Versionen für einen Service auswählen, muss der Benutzer einen Service und eine Protokollversion auswählen und dann die Auswahl eines Service und eines Protokolls wiederholen, bis alle Einstellungen geändert wurden.

Überprüfung

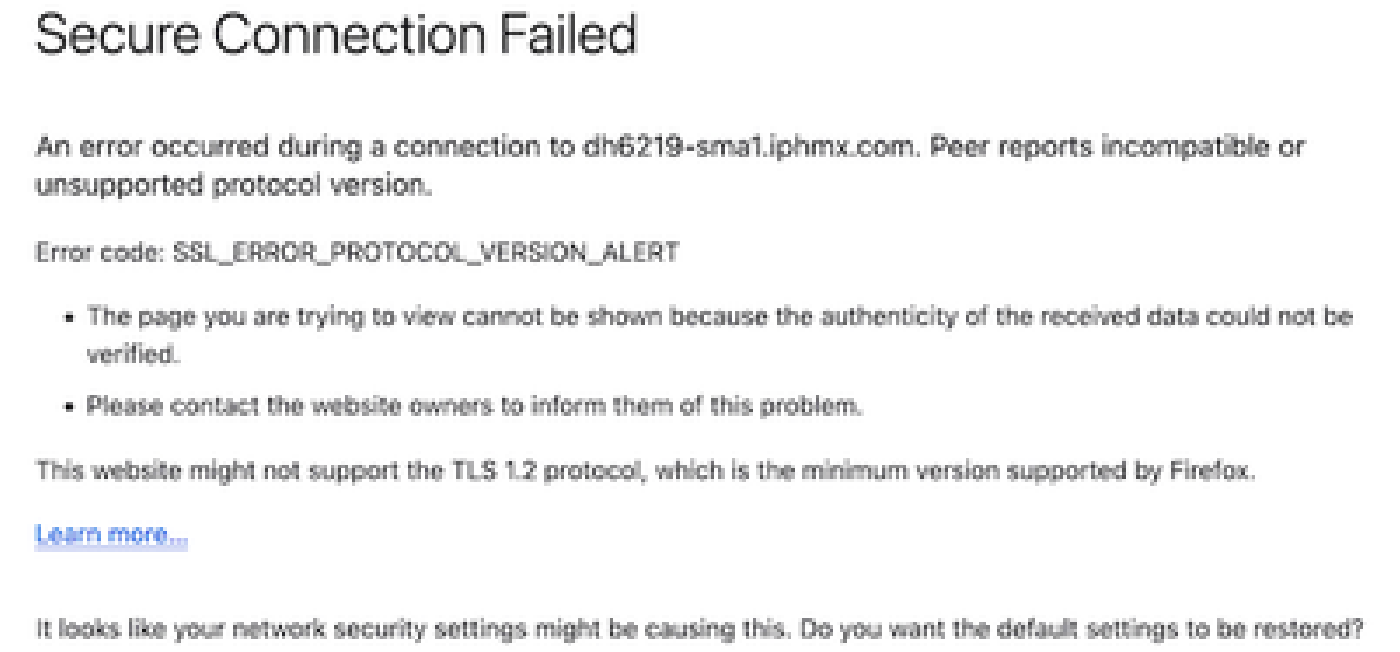
Dieser Abschnitt enthält einige grundlegende Testszenarien und die Fehler, die aufgrund von nicht übereinstimmenden Versionen oder Syntaxfehlern auftreten.

Überprüfen Sie die Browser-Funktionalität, indem Sie eine Webbrowser-Sitzung mit der EWM WebUI oder der NGUI öffnen, die mit TLSv1.3 konfiguriert sind.

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

- Beispiel: Wenn Sie die Browsereinstellung auf Firefox so festlegen, dass die Unterstützung für TLS v1.3 deaktiviert wird, werden Fehler auf der ClassicUI und 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.



TLS v1.3-Webui-Fehler

- Überprüft die Browser-Einstellungen, um sicherzustellen, dass TLSv1.3 enthalten ist. (Dieses Beispiel stammt von Firefox.)

- Beispiel-OpenSSL-Befehl mit einem falsch eingegebenen Verschlüsselungswert würde diese Fehlerausgabe geben: Beispiel-OpenSSL-Verbindungstestfehler aufgrund ungültiger Verschlüsselung: Fehler mit Befehl: "-ciphersuites TLS_AES_256_GCM_SHA386"

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

- Der Beispiel-Curl-Befehl, der an der ng-ui ausgeführt wird, wenn TLS v1.3 deaktiviert ist, erzeugt diesen Fehler.

curl: (35) CURL_SSLVERSION_MAX inkompatibel mit CURL_SSLVERSION

Zugehörige Informationen

- Cisco Content Security Management Appliance - Versionshinweise
- Cisco Content Security Management Appliance - Benutzerhandbücher

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.