

Konfigurieren des GUI-Zertifikats der sicheren Web-Appliance

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Zertifikat für die Webbenutzeroberfläche](#)

[Schritte zum Ändern des Webschnittstellenzertifikats](#)

[Testen des Zertifikats über die Befehlszeile](#)

[Häufige Fehler](#)

[Fehler: Ungültiges PKCS#12-Format](#)

[Tage müssen eine ganze Zahl sein.](#)

[Fehler bei der Zertifikatsvalidierung](#)

[Ungültiges Kennwort](#)

[Das Zertifikat ist noch nicht gültig.](#)

[GUI-Dienst von CLI neu starten](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden die Schritte zum Konfigurieren von Zertifikaten für die Webschnittstelle der Secure Web Appliance (SWA) für die Verwaltung beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- SWA-Verwaltung.

Cisco empfiehlt Folgendes:

- Installiertes physisches oder virtuelles SWA.
- Administrator-Zugriff auf die grafische Benutzeroberfläche (GUI) von SWA
- Administrator-Zugriff auf die SWA-Befehlszeilenschnittstelle (CLI)

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

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 möglichen Auswirkungen aller Befehle kennen.

Zertifikat für die Webbenutzeroberfläche


Zuerst müssen wir den Zertifikatstyp auswählen, den wir in der SWA-Verwaltungs-Webbenutzeroberfläche (Webbenutzeroberfläche) verwenden möchten.

Standardmäßig verwendet SWA das "Cisco Appliance Demo Certificate:".

- CN = Cisco Appliance Demo-Zertifikat
- O = Cisco Systems, Inc.
- L = San Jose
- S = Kalifornien
- C = USA

Sie können ein selbstsigniertes Zertifikat in SWA erstellen oder Ihr eigenes Zertifikat importieren, das von Ihrem CA-Server (Internal Certificate Authority) generiert wurde.

Der SWA unterstützt beim Generieren einer Zertifikatssignierungsanforderung (Certificate Signing Request, CSR) nicht die Integration alternativer Subjektnamen (Subject Alternative Names, SAN). Darüber hinaus unterstützen die selbstsignierten SWA-Zertifikate auch keine SAN-Attribute. Um Zertifikate mit SAN-Attributen zu verwenden, müssen Sie das Zertifikat selbst erstellen und signieren, um sicherzustellen, dass es die erforderlichen SAN-Details enthält. Sobald Sie dieses Zertifikat generiert haben, können Sie es zur Verwendung in die SWA hochladen. Mit diesem Ansatz können Sie mehrere Hostnamen, IP-Adressen oder andere IDs angeben, wodurch Ihre Netzwerkumgebung flexibler und sicherer wird.

 Hinweis: Die Zertifikate müssen den privaten Schlüssel enthalten und im PKCS#12-Format vorliegen.

Schritte zum Ändern des Webschnittstellenzertifikats

Schritt 1: Melden Sie sich bei der GUI an, und wählen Sie im oberen Menü die Option Network (Netzwerk) aus.

Schritt 2: Wählen Sie Zertifikatsverwaltung aus.

Schritt 3: Wählen Sie in Appliance-Zertifikaten die Option Zertifikat hinzufügen aus.

Schritt 4: Wählen Sie Zertifikatstyp aus (selbstsigniertes Zertifikat oder Zertifikat importieren).

Add Certificate

Add Certificate

Add Certificate:
Select an option...

Cancel

Create Self-Signed Certificate
 Import Certificate

Next >>

Bild - Zertifikatstyp auswählen

Schritt 5: Wenn Sie das selbstsignierte Zertifikat auswählen, gehen Sie folgendermaßen vor. Fahren Sie andernfalls mit Schritt 6 fort.

Schritt 5.1. Füllen Sie die Felder aus.

Add Certificate

Add Certificate

Add Certificate:	<input type="text" value="Create Self-Signed Certificate"/>
Common Name:	<input type="text" value="SelfSignCertificate"/>
Organization:	<input type="text" value="CiscoLAB"/>
Organizational Unit:	<input type="text" value="SWA"/>
City (Locality):	<input type="text" value="City"/>
State (Province):	<input type="text" value="State"/>
Country:	<input type="text" value="US"/>
Duration before expiration:	<input type="text" value="730"/> days
Private Key Size:	<input type="text" value="2048"/>

Cancel
Next >>

Bild - Zertifikatdetails zum Selbstsignieren

Hinweis: Die Größe des privaten Schlüssels muss im Bereich von 2048 bis 8192 liegen.

Schritt 5.2: Klicken Sie auf Next (Weiter).

View Certificate SelfSignCertificate

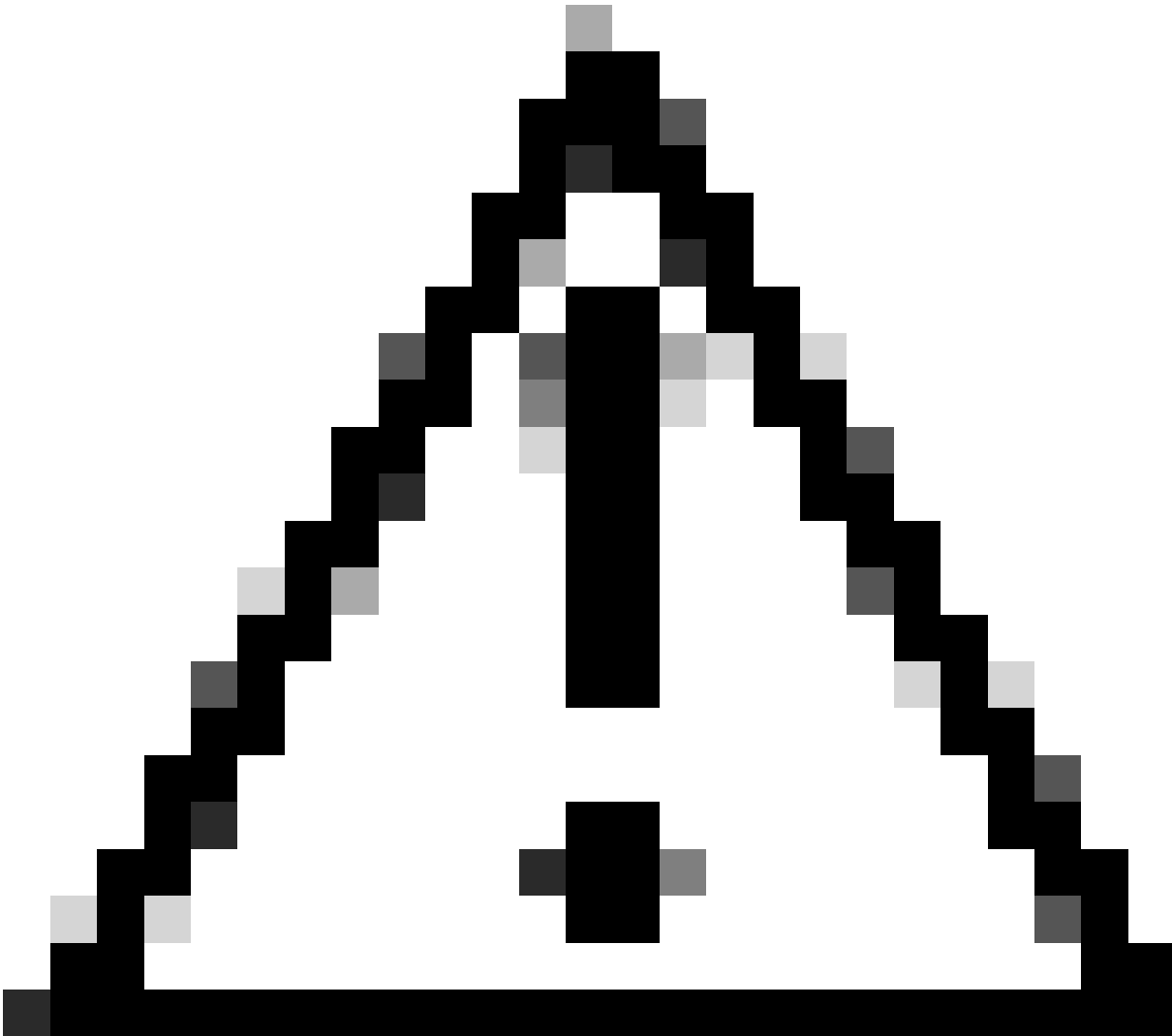
Add Certificate

Certificate Name:	<input type="text" value="SelfSignCertificate"/>
Common Name:	SelfSignCertificate
Organization:	CiscoLAB
Organization Unit:	SWA
City (Locality):	City
State (Province):	State
Country:	US
Signature Issued By:	Common Name (CN): SelfSignCertificate Organization (O): CiscoLAB Organizational Unit (OU): SWA Issued On: Oct 14 11:48:59 2024 GMT Expires On: Oct 14 11:48:59 2026 GMT
	<i>If you would like a globally recognized signed certificate: 1. Download Certificate Signing Request, 2. Submit this to a certificate authority, 3. Once you receive the signed certificate, upload it below.</i>
	Upload Signed Certificate: <input type="button" value="Choose File"/> No file chosen
	<input type="button" value="Download Certificate Signing Request..."/>
<input checked="" type="checkbox"/> Intermediate Certificates (optional):	Upload an Intermediate Certificate: <input type="button" value="Choose File"/> No file chosen

Cancel
Submit

Bild: CSR herunterladen

Schritt 5.3: (Optional) Sie können den CSR herunterladen und mit dem Zertifizierungsstellenserver Ihrer Organisation signieren. Anschließend können Sie das signierte Zertifikat hochladen und einsenden.



Achtung: Wenn Sie den CSR mit Ihrem CA-Server signieren möchten, stellen Sie sicher, dass Sie die Seite einreichen und bestätigen, bevor Sie das signierte Zertifikat signieren oder hochladen. Das Profil, das Sie während der CSR-Erstellung erstellt haben, enthält Ihren privaten Schlüssel.

Schritt 5.4. Senden, wenn das aktuelle selbstsignierte Zertifikat angemessen ist

Schritt 5.5: Fahren Sie mit Schritt 7 fort.

Schritt 6: Wenn Sie Zertifikat importieren auswählen.

Schritt 6.1: Zertifikatsdatei importieren (PKCS#12-Format erforderlich).

Schritt 6.2: Geben Sie das Kennwort für die Zertifikatsdatei ein.

Add Certificate

Add Certificate:	Import Certificate
Import Certificate:	Choose File No file chosen PKCS#12 format is required.
Enter Password: (required)	

Cancel Next >>

Bild - Zertifikat importieren

Schritt 6.3: Klicken Sie auf Next (Weiter).

Schritt 6.4: Änderungen übermitteln.


Schritt 7. Änderungen bestätigen.

Schritt 8: Melden Sie sich bei der CLI an.

Schritt 9. Geben Sie certconfig ein, und drücken Sie die Eingabetaste.

Schritt 10. Geben Sie SETUP ein.


Schritt 11. Geben Sie Y ein, und drücken Sie die Eingabetaste.

 Hinweis: Bei einer Änderung des Zertifikats kann es bei Administratoren, die derzeit an der Webbenutzeroberfläche angemeldet sind, zu einem Verbindungsfehler kommen, sodass nicht übermittelte Änderungen verloren gehen können. Dies ist nur der Fall, wenn das Zertifikat vom Browser noch nicht als vertrauenswürdig markiert wurde.

Schritt 12: Wählen Sie 2 aus, um ein Zertifikat aus der Liste der verfügbaren Zertifikate auszuwählen.

Schritt 13: Wählen Sie die Anzahl der Zertifikate aus, die für die GUI verwendet werden sollen.

Schritt 14: Wenn Sie ein Zwischenzertifikat besitzen und dieses hinzufügen möchten, geben Sie Y else ein, und geben Sie N ein.

 Hinweis: Wenn Sie das Zwischenzertifikat hinzufügen müssen, fügen Sie das Zwischenzertifikat im PEM-Format ein und enden mit '.' (Nur Punkt).

```
SWA_CLI> certconfig
```

Choose the operation you want to perform:

- SETUP - Configure security certificate and key.
- OCSPVALIDATION - Enable OCSP validation of certificates during upload

```
- RESTRICTCERTSIGNATURE - Enable restricted signature validation of certificates during upload
- OCSPVALIDATION_FOR_SERVER_CERT - Enable OCSP validation for server certificates
- FQDNVALIDATION - FQDN validation for certificate
[ ]> SETUP
```

Currently using the demo certificate/key for HTTPS management access.

When the certificate is changed, administrative users who are currently logged in to the web user interface occurs only if the certificate is not already marked as trusted by the browser.

```
Do you want to continue? [Y]> Y
```

```
Management (HTTPS):
```

```
Choose the operation you want to perform:
```

1. PASTE - Copy paste cert and key manually
 2. SELECT - select from available list of certificates
- ```
[1]> 2
```

```
Select the certificate you want to upload
```

1. SelfSignCertificate
  2. SWA\_GUI.cisco.com
- ```
[1]> 1
```

```
Do you want add an intermediate certificate? [N]> N
```

Successfully updated the certificate/key for HTTPS management access.

Schritt 15: Geben Sie commit ein, um die Änderungen zu speichern.

Testen des Zertifikats über die Befehlszeile

Sie können das Zertifikat mit dem Befehl openssl überprüfen:

```
openssl s_client -connect
```

```
:
```

In diesem Beispiel lautet der Hostname SWA.cisco.com, und die Verwaltungsschnittstelle ist als Standard festgelegt (TCP-Port 8443).

In der zweiten Zeile der Ausgabe sehen Sie die Zertifikatdetails:

```
openssl s_client -connect SWA.cisco.com:8443
CONNECTED(00000003)
depth=0 C = US, CN = SelfSignCertificate, L = City, O = CiscoLAB, ST = State, OU = SWA
```

Häufige Fehler

Hier sind einige häufige Fehler, denen Sie beim Erstellen oder Ändern Ihres GUI-Zertifikats begegnen können.

Fehler: Ungültiges PKCS#12-Format

Add Certificate

Error — Invalid PKCS#12 format

Add Certificate	
Add Certificate:	Import Certificate ▾
Import Certificate:	<input type="button" value="Choose File"/> No file chosen <i>PKCS#12 format is required.</i> Invalid PKCS#12 format
Enter Password: (required)	<input type="password"/>

Bild - Ungültiges PKCS#12-Format

Dieser Fehler kann auf zwei Ursachen zurückzuführen sein:

1. Die Zertifikatsdatei ist beschädigt und ungültig.

Versuchen Sie, das Zertifikat zu öffnen. Wenn beim Öffnen ein Fehler auftritt, können Sie das Zertifikat erneut generieren oder herunterladen.

2. Die zuvor generierte CSR ist nicht mehr gültig.

Wenn Sie eine CSR-Anfrage erstellen, müssen Sie sicherstellen, dass Sie Ihre Änderungen einreichen und bestätigen. Der Grund dafür ist, dass Ihr CSR nicht gespeichert wurde, als Sie sich abgemeldet oder Seiten geändert haben. Das Profil, das Sie beim Generieren des CSR erstellt haben, enthält den privaten Schlüssel, der für das erfolgreiche Hochladen des Zertifikats erforderlich ist. Sobald dieses Profil gelöscht wurde, ist der private Schlüssel verschwunden. Aus diesem Grund muss eine weitere CSR-Anfrage generiert und dann erneut an Ihre CA gesendet werden.

Tage müssen eine ganze Zahl sein.

Add Certificate

Error — Days must be an integer from 1 to 1825.

Add Certificate	
Add Certificate:	Import Certificate ▾
Import Certificate:	<input type="button" value="Choose File"/> No file chosen <i>PKCS#12 format is required.</i> Days must be an integer from 1 to 1825.
Enter Password: (required)	<input type="text"/>

Bild - Tage müssen eine ganze Zahl sein

Dieser Fehler ist darauf zurückzuführen, dass das hochgeladene Zertifikat abgelaufen ist oder eine Gültigkeit von 0 Tagen hat.

Um das Problem zu lösen, überprüfen Sie bitte das Ablaufdatum des Zertifikats und vergewissern Sie sich, dass Ihr SWA-Datum und Ihre SWA-Zeit korrekt sind.

Fehler bei der Zertifikatsvalidierung

Dieser Fehler bedeutet, dass die Stammzertifizierungsstelle oder die intermediäre Zertifizierungsstelle nicht der Liste vertrauenswürdiger Stammzertifikate in SWA hinzugefügt werden. Um das Problem zu beheben, wenn Sie sowohl die Stammzertifizierungsstelle als auch die mittlere Zertifizierungsstelle verwenden:

1. Laden Sie die Root-Zertifizierungsstelle in SWA hoch, und klicken Sie anschließend auf Bestätigen.
2. Laden Sie die Zwischen-CA hoch, und bestätigen Sie die Änderungen erneut.
3. Laden Sie Ihr GUI-Zertifikat hoch.



Hinweis: So laden Sie die Stamm- oder Zwischen-CA über die GUI hoch: Netzwerk. Wählen Sie im Abschnitt Zertifikatsverwaltung die Option Vertrauenswürdige Stammzertifikate verwalten aus. Klicken Sie unter Benutzerdefinierte vertrauenswürdige Stammzertifikate auf Importieren, um Ihre Zertifizierungsstellenzertifikate hochzuladen.

Ungültiges Kennwort

Add Certificate

Error — Invalid PKCS#12 password

Add Certificate	
Add Certificate:	Import Certificate ▾
Import Certificate:	<input type="button" value="Choose File"/> No file chosen <i>PKCS#12 format is required.</i>
Enter Password: (required)	<input type="password"/> Invalid PKCS#12 password

Cancel

Next >>

Bild - Ungültiges Kennwort

Dieser Fehler zeigt an, dass das PKCS#12-Zertifikatkennwort falsch ist. Um den Fehler zu beheben, geben Sie das richtige Kennwort ein, oder generieren Sie das Zertifikat neu.

Das Zertifikat ist noch nicht gültig.

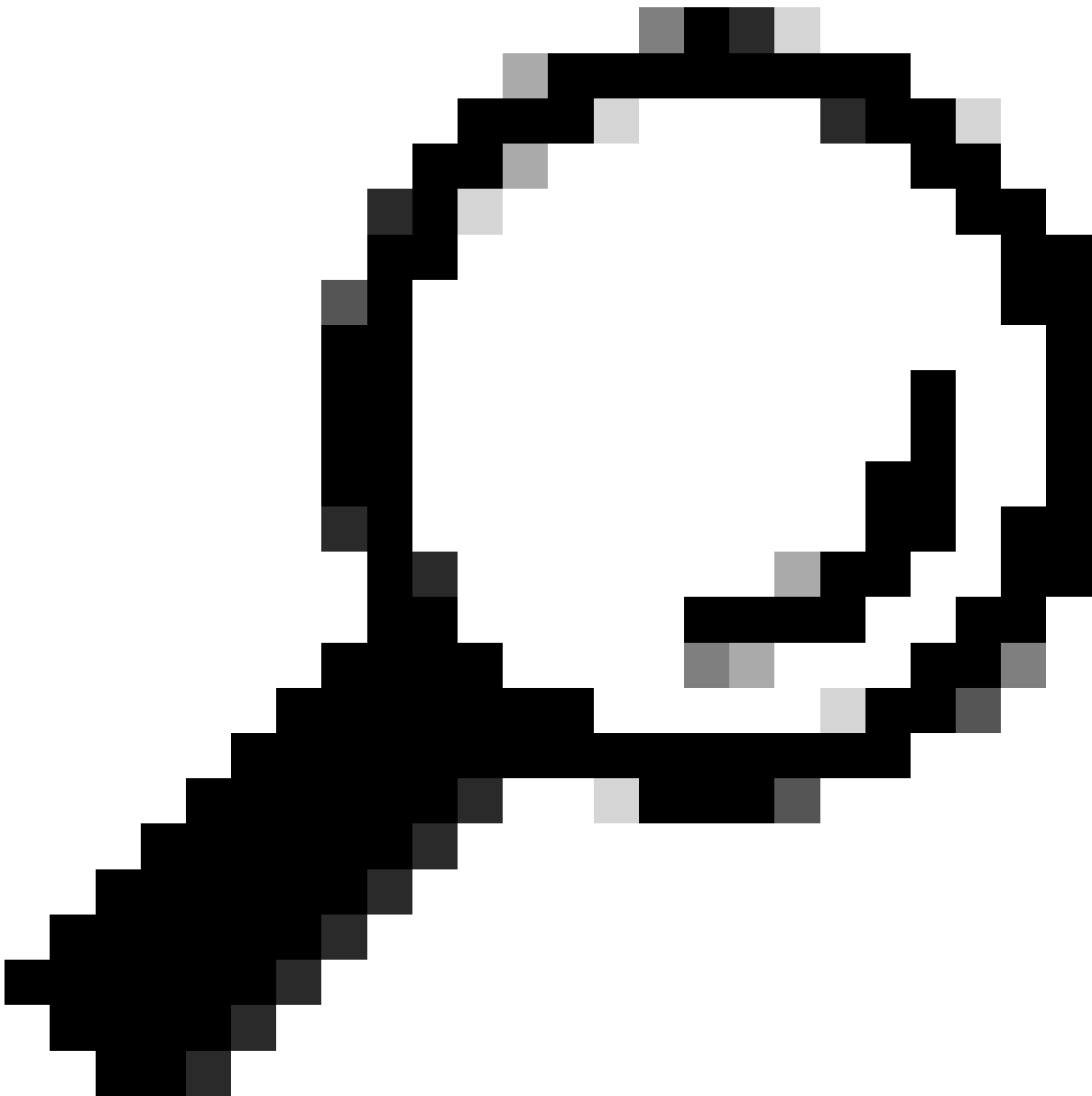
Add Certificate

Error — The certificate is Not Yet Valid.

Add Certificate	
Add Certificate:	Import Certificate ▾
Import Certificate:	<input type="button" value="Choose File"/> No file chosen <i>PKCS#12 format is required.</i> The certificate is Not Yet Valid.
Enter Password: (required)	<input type="password"/>

Bild: Das Zertifikat ist noch nicht gültig.

1. Stellen Sie sicher, dass Datum und Uhrzeit der SWA korrekt sind.
2. Überprüfen Sie das Datum des Zertifikats, und vergewissern Sie sich, dass Datum und Uhrzeit "Nicht vor" korrekt sind.



Tipp: Wenn Sie das Zertifikat gerade generiert haben, warten Sie eine Minute und laden Sie es hoch.

GUI-Dienst von CLI neu starten

Um den WebUI-Dienst neu zu starten, können Sie die folgenden Schritte über die CLI ausführen:

Schritt 1: Melden Sie sich bei der CLI an.

Schritt 2: Geben Sie `diagnostic` (Dies ist ein ausgeblendeter Befehl, der nicht automatisch mit TAB eingegeben wird) ein.

Schritt 3: Wählen Sie `SERVICES`.

Schritt 4: Wählen Sie WEBUI aus.

Schritt 5: Wählen Sie RESTART.

Zugehörige Informationen

- [Benutzerhandbuch für AsyncOS 15.0 für Cisco Secure Web Appliance - GD\(Allgemeine Bereitstellung\) - Endbenutzer für Richtlinienanwendung klassifizieren \[Cisco Secure Web Appliance\] - Cisco](#)

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.