

セキュアなWebアプライアンスのGUI証明書の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[Webユーザインターフェイス証明書](#)

[Webインターフェイス証明書を変更する手順](#)

[コマンドラインからの証明書のテスト](#)

[一般的なエラー](#)

[無効なPKCS#12形式のエラー](#)

[日数は整数でなければなりません](#)

[証明書の検証エラー](#)

[Invalid Password](#)

[証明書はまだ有効ではありません](#)

[CLIからのGUIサービスの再起動](#)

[関連情報](#)

はじめに

このドキュメントでは、Secure Web Appliance(SWA)管理Webインターフェイスの証明書を設定する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- SWA管理。

Cisco では次の前提を満たす推奨しています。

- 物理または仮想SWAがインストールされている。
- SWAグラフィカルユーザインターフェイス(GUI)への管理アクセス。
- SWAコマンドラインインターフェイス(CLI)への管理アクセス。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

Webユーザインターフェイス証明書


まず、SWA管理Webユーザインターフェイス(Web UI)で使用する証明書のタイプを選択する必要があります。

デフォルトでは、SWAは「シスコアプライアンスデモ証明書：」を使用します。

- CN = Cisco Appliance Demo Certificate (シスコアプライアンスデモ証明書)
- O = Cisco Systems, Inc
- L = SAN JOSE
- S =カリフォルニア
- C = US

SWAで自己署名証明書を作成するか、または内部認証局(CA)サーバによって生成された独自の証明書をインポートできます。

SWAは、証明書署名要求(CSR)の生成時のサブジェクト代替名(SAN)の組み込みをサポートしていません。また、SWA自己署名証明書もSAN属性をサポートしていません。SAN属性を持つ証明書を使用するには、証明書を自分で作成して署名し、必要なSANの詳細が含まれていることを確認する必要があります。この証明書を生成したら、使用するSWAにアップロードできます。この方法では、複数のホスト名、IPアドレス、またはその他の識別子を指定できるため、ネットワーク環境の柔軟性とセキュリティが向上します。

 注：証明書には秘密キーが含まれている必要があります。また、秘密キーはPKCS#12形式である必要があります。

Webインターフェイス証明書を変更する手順

ステップ 1：GUIにログインして、トップメニューからNetworkを選択します。

ステップ 2：Certificate Managementを選択します。

ステップ 3：Appliance Certificates で、Add Certificateを選択します。

ステップ 4：Certificate Type(Self Signed CertificateまたはImport Certificate)を選択します。

図 - 証明書タイプの選択

ステップ 5 : 自己署名証明書を選択する場合は、次の手順を使用します。それ以外の場合は、ステップ 6 に進みます。

ステップ5.1:フィールドに入力します。

Add Certificate

Add Certificate	
Add Certificate:	Create Self-Signed Certificate ▾
Common Name:	SelfSignCertificate
Organization:	CiscoLAB
Organizational Unit:	SWA
City (Locality):	City
State (Province):	State
Country:	US
Duration before expiration:	730 days
Private Key Size:	2048

Cancel Next >>

イメージ : 自己署名証明書の詳細

注 : 秘密キーのサイズは2048 ~ 8192の範囲である必要があります。

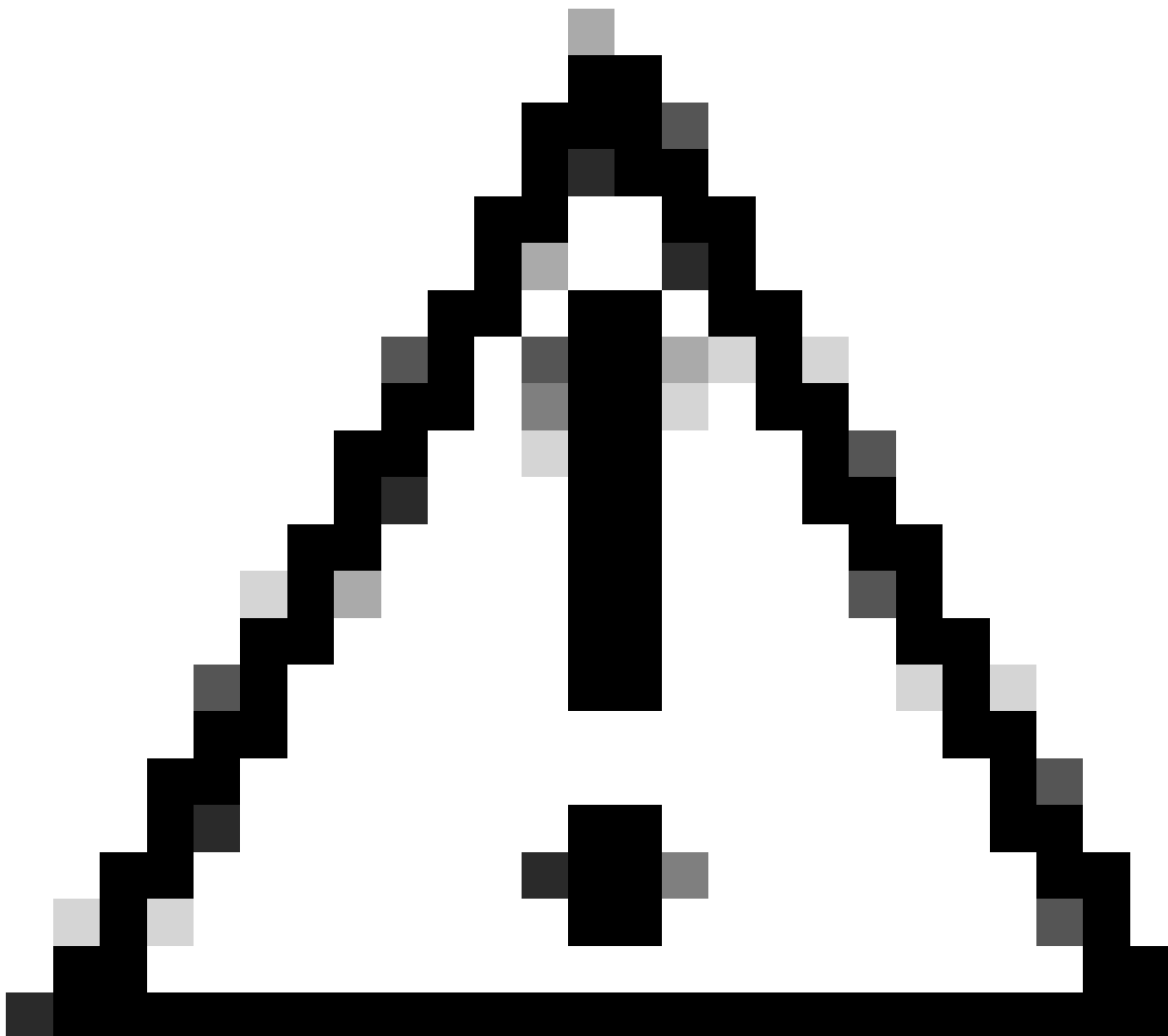
ステップ 5.2 : [Next] をクリックします。

View Certificate SelfSignCertificate

Add Certificate	
Certificate Name:	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 <small>Uploading a new certificate will overwrite the existing certificate.</small>
Intermediate Certificates (optional):	<input type="button" value="Choose File"/> No file chosen

Cancel Submit

ステップ 5.3：（オプション）CSRをダウンロードして組織のCAサーバで署名し、署名付き証明書をアップロードして送信します。



注意: CAサーバを使用してCSRに署名する場合は、署名した証明書を署名またはアップロードする前に、必ずページを送信してコミットしてください。CSR生成プロセスで作成したプロファイルには、秘密キーが含まれています。

ステップ5.4：現在の自己署名証明書が適切な場合は送信します。

ステップ 5.5：ステップ 7 に進みます。

手順 6：Import Certificateを選択します。

ステップ 6.1：証明書ファイルのインポート（PKCS#12形式が必要）。

ステップ 6.2：証明書ファイルのパスワードを入力します。

Add Certificate

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

Cancel Next >>

イメージ：証明書のインポート

ステップ 6.3： [Next] をクリックします。

ステップ 6.4： 変更を送信します。


手順 7： 変更を確定します。

ステップ 8： CLIにログインします。

ステップ 9： certconfigと入力してEnterキーを押します。

ステップ 10： SETUPと入力します。


ステップ 11Yと入力して、Enterキーを押します。

 注：証明書を変更すると、現在Webユーザインターフェイスにログインしている管理ユーザに接続エラーが発生し、未送信の変更が失われる可能性があります。これは、証明書がブラウザによって信頼できるとマークされていない場合にのみ発生します。

ステップ 12 2を選択して、使用可能な証明書のリストから選択します。

ステップ 13 GUIで使用する証明書の数を選択します。

ステップ 14： 中間証明書があり、それを追加する場合はYと入力し、それ以外の場合はN と入力します。

 注：中間証明書を追加する必要がある場合は、中間証明書をPEM形式で貼り付け、「.」（ドットのみ）で終了する必要があります。

```
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.

ステップ 15 : commitと入力して、変更を保存します。

コマンドラインからの証明書のテスト

opensslコマンドを使用して証明書を確認できます。

```
openssl s_client -connect
```

:

この例では、ホスト名はSWA.cisco.comで、管理インターフェイスはデフォルト (TCPポート 8443) に設定されています。

出力の2行目で、証明書の詳細を確認できます。

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

一般的なエラー

GUI証明書を作成または変更しようとしたときに発生する可能性がある一般的なエラーを次に示します。

無効なPKCS#12形式のエラー

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"/>

イメージ：無効なPKCS#12形式

このエラーには、次の2つの原因が考えられます。

1. 証明書ファイルが壊れていて無効です。

証明書を開いてみてください。開くときにエラーが発生した場合は、証明書を再生成するか、もう一度ダウンロードできます。

2. 以前に生成されたCSRが無効になっている。

CSRを生成する場合は、必ずSubmitを実行し、変更をコミットしてください。これは、ログアウトまたはページの変更の際にCSRが保存されなかったためです。CSRを生成したときに作成したプロファイルには、証明書を正常にアップロードするために必要な秘密キーが含まれています。このプロファイルがなくなると、秘密キーはなくなります。そのため、別のCSRを生成して、もう一度CAに送信する必要があります。

日数は整数でなければなりません

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 <small>PKCS#12 format is required. Days must be an integer from 1 to 1825.</small>
Enter Password: (required)	<input type="text"/>

イメージ - 日数は整数エラーである必要があります

このエラーは、アップロードされた証明書の有効期限が切れているか、0日間の有効性が保たれていることが原因です。

この問題を解決するには、証明書の有効期限を確認し、SWAの日付と時刻が正しいことを確認してください。

証明書の検証エラー

このエラーは、ルートCAまたは中間CAがSWAの信頼されたルート証明書リストに追加されていないことを意味します。ルートCAと中間CAの両方を使用している場合、この問題を解決するには、次の手順を実行します。

1. ルートCAをSWAにアップロードし、Commitを実行します。
2. 中間CAをアップロードし、変更をコミットします。
3. GUI証明書をアップロードします。



注：ルートCAまたは中間CAをアップロードするには、GUIから「Network」を選択します。Certificate Managementセクションで、Manage Trusted Root Certificatesの順に選択します。Custom Trusted Root Certificatesで、Importをクリックして、CA証明書をアップロードします。

Invalid Password

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 >>

イメージ – 無効なパスワード

このエラーは、PKCS#12証明書パスワードが正しくないことを示します。エラーを解決するには、正しいパスワードを入力するか、証明書を再生成します。

証明書はまだ有効ではありません

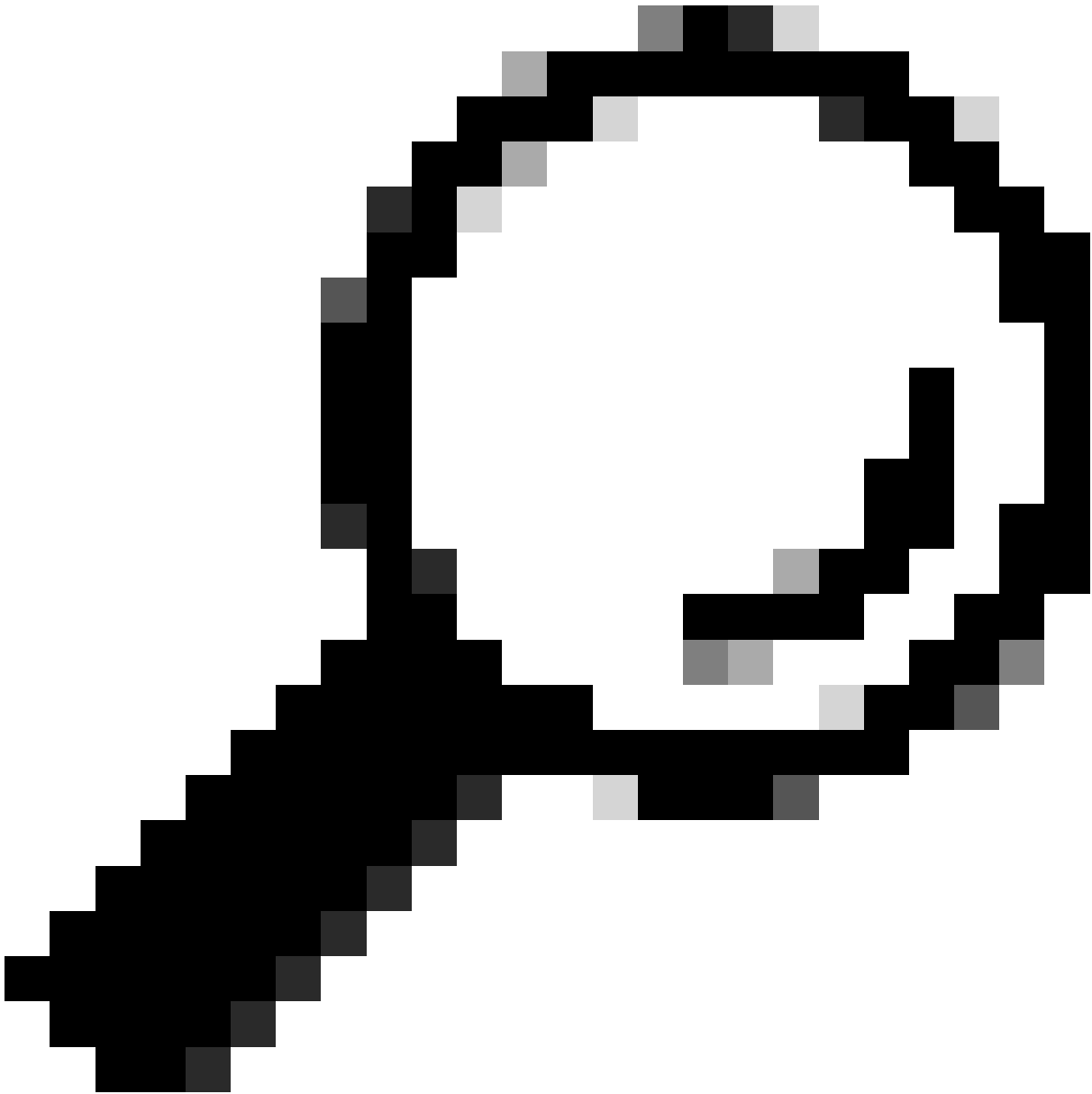
Add Certificate

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"/>

図 – 証明書がまだ有効ではない

1. SWAの日付と時刻が正しいことを確認します。
2. 証明書の日付を確認し、「Not Before」の日付と時刻が正しいことを確認します。



ヒント：証明書を生成したばかりの場合は、1分待ってから証明書をアップロードしてください。

CLIからのGUIサービスの再起動

WebUIサービスを再起動するには、CLIから次の手順を使用できます。

ステップ 1：CLIにログインします。

ステップ 2：diagnosticと入力します(これは隠しコマンドであり、Tabを押すと自動的に入力されません)。

ステップ 3：SERVICESを選択します。

ステップ 4 : WEBUIを選択します。

ステップ 5 : RESTARTを選択します。

関連情報

- [AsyncOS 15.0 for Cisco Secure Web Appliance ユーザガイド – GD\(General Deployment\) – ポリシーアプリケーションのエンドユーザの分類 \[Cisco Secure Web Appliance\] – シスコ](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。