보안 웹 어플라이언스 GUI 인증서 구성

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소

웹 사용자 인터페이스 인증서

웹 인터페이스 인증서 수정 단계

명령줄에서 인증서 테스트

일반 오류

- 오류: 잘못된 PKCS#12 형식
- 일은 정수여야 합니다.
- 인증서 유효성 검사 오류
- 잘못된 암호
- 인증서가 아직 유효하지 않습니다.

CLI에서 GUI 서비스 다시 시작

관련 정보

소개

이 문서는 SWA(Secure Web Appliance) 관리 웹 인터페이스에 대한 인증서를 구성하는 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SWA 관리.

Cisco에서는 다음과 같은 작업을 수행할 것을 권장합니다.

- 물리적 또는 가상 SWA가 설치되었습니다.
- SWA GUI(Graphical User Interface)에 대한 관리 액세스
- SWA CLI(Command Line Interface)에 대한 관리 액세스

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

웹 사용자 인터페이스 인증서

먼저 SWA 관리 웹 사용자 인터페이스(웹 UI)에서 사용할 인증서 유형을 선택해야 합니다.

기본적으로 SWA는 "Cisco Appliance Demo Certificate:"를 사용합니다.

- CN = Cisco Appliance 데모 인증서
- O = Cisco Systems, Inc
- L = 산호세
- S = 캘리포니아
- C = 미국

SWA에서 자체 서명 인증서를 생성하거나 내부 CA(Certificate Authority) 서버에서 생성한 자체 인증서를 가져올 수 있습니다.

SWA는 CSR(Certificate Signing Request)을 생성할 때 SAN(Subject Alternative Name)을 포함할 수 없습니다. 또한 SWA 자체 서명 인증서도 SAN 특성을 지원하지 않습니다. SAN 특성이 있는 인증서를 활용하려면 필요한 SAN 세부 정보를 포함하도록 인증서를 직접 만들고 서명해야 합니다. 이 인증서를 생성한 후에는 사용할 SWA에 업로드할 수 있습니다. 이 접근 방식을 사용하면 여러 호스트 이름, IP 주소 또는 기타 식별자를 지정할 수 있으므로 네트워크 환경에 더 큰 유연성과 보안을 제공할 수 있습니다.

참고: 인증서에는 개인 키가 포함되어야 하며 PKCS#12 형식이어야 합니다.

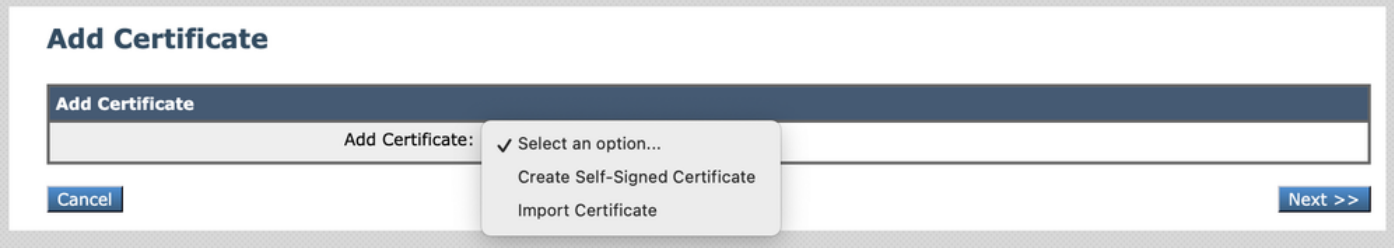
웹 인터페이스 인증서 수정 단계

1단계. GUI에 로그인하고 상단 메뉴에서 Network(네트워크)를 선택합니다.

2단계. Certificate Management(인증서 관리)를 선택합니다.

3단계. Appliance Certificates(어플라이언스 인증서)에서 Add Certificate(인증서 추가)를 선택합니다.

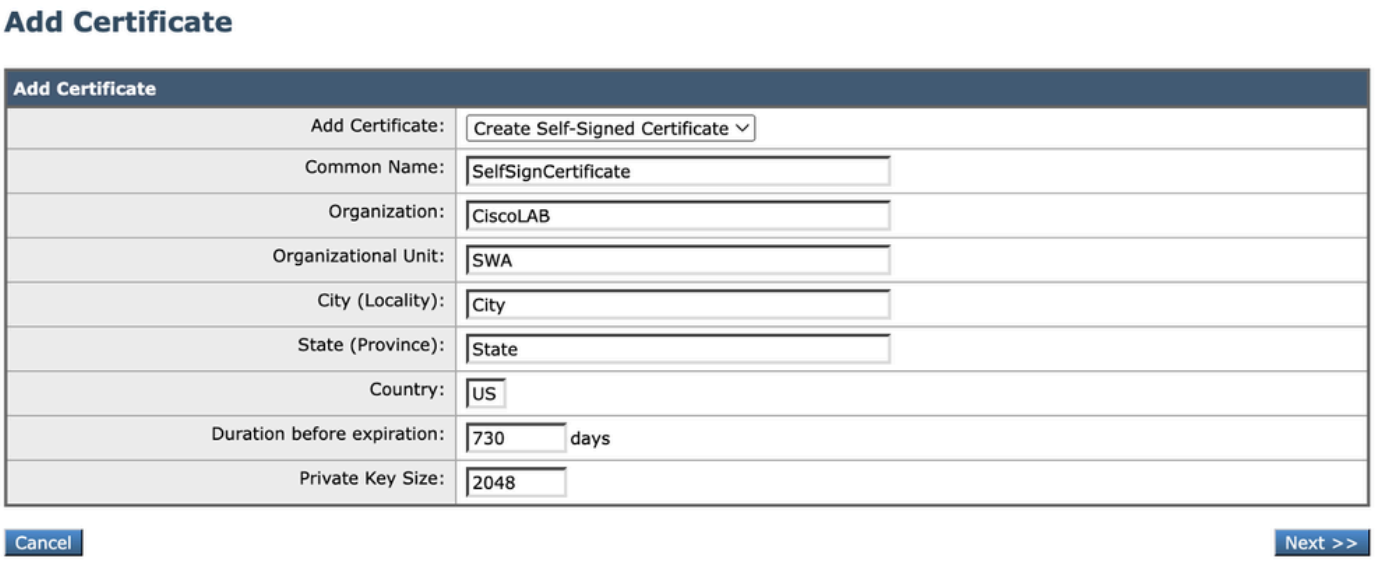
4단계. Certificate Type(인증서 유형)(Self Signed Certificate 또는 Import Certificate)을 선택합니다.



Image(이미지) - Certificate Type(인증서 유형) 선택

5단계. 자체 서명 인증서를 선택하는 경우 다음 단계를 수행합니다. 그렇지 않으면 6단계로 건너뜁니다.

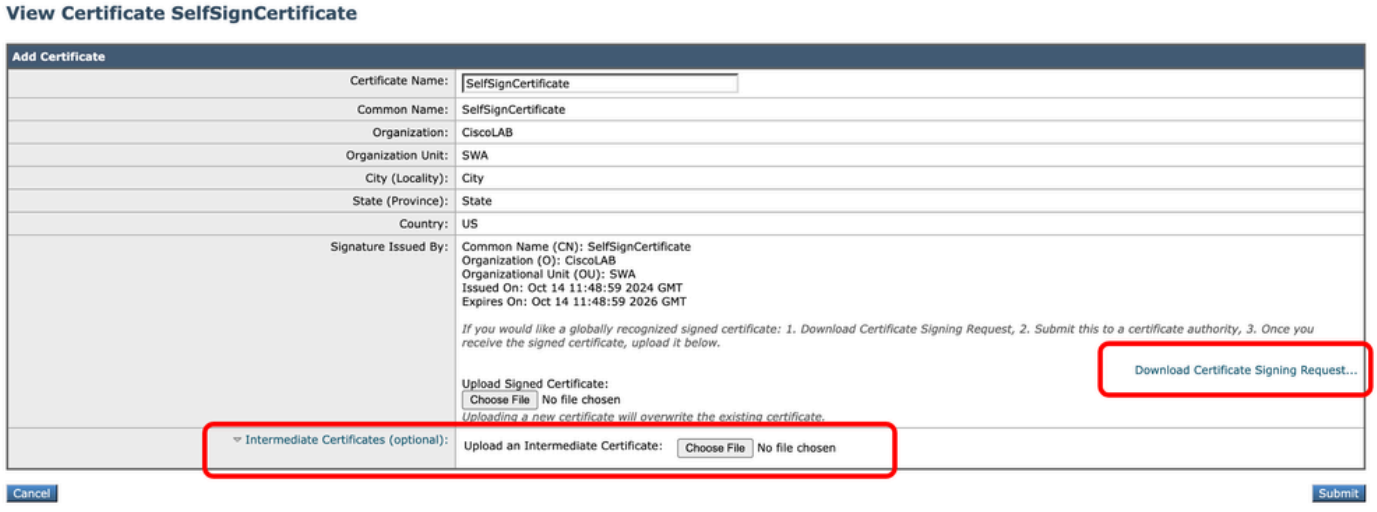
5.1단계. 필드를 완료합니다.



이미지 - 자체 서명 인증서 세부 정보

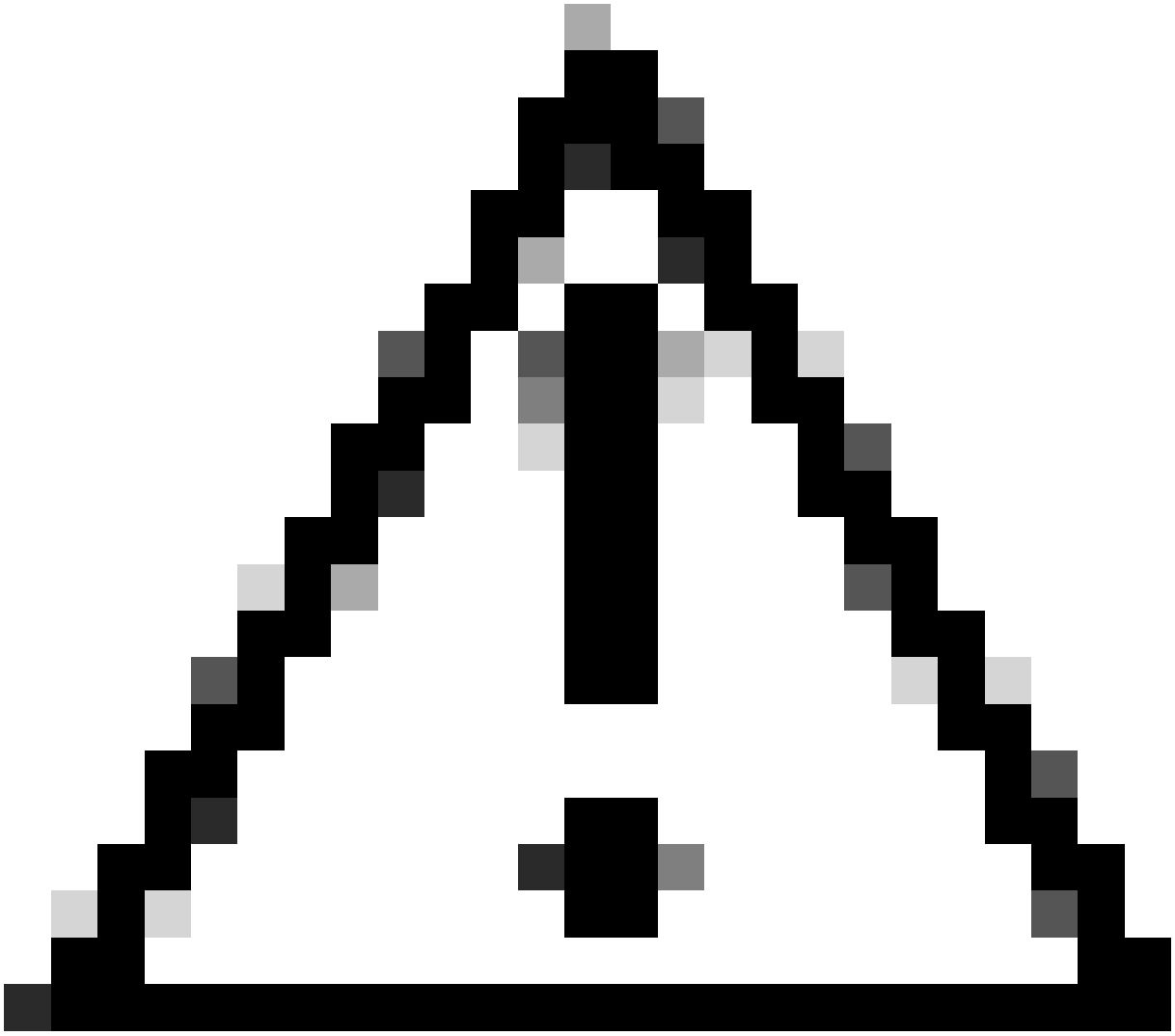
참고: 개인 키 크기는 2048에서 8192 범위에 있어야 합니다.

5.2단계. Next(다음)를 클릭합니다.



이미지 - CSR 다운로드

5.3단계. (선택 사항) CSR을 다운로드하고 조직 CA 서버에 서명한 다음 서명된 인증서를 업로드하고 제출할 수 있습니다.



주의: CA 서버에서 CSR에 서명하려는 경우 서명된 인증서를 서명 또는 업로드하기 전에 Submit and Commit(제출 및 커밋)을 확인하십시오. CSR 생성 프로세스 중에 생성한 프로필에는 개인 키가 포함됩니다.

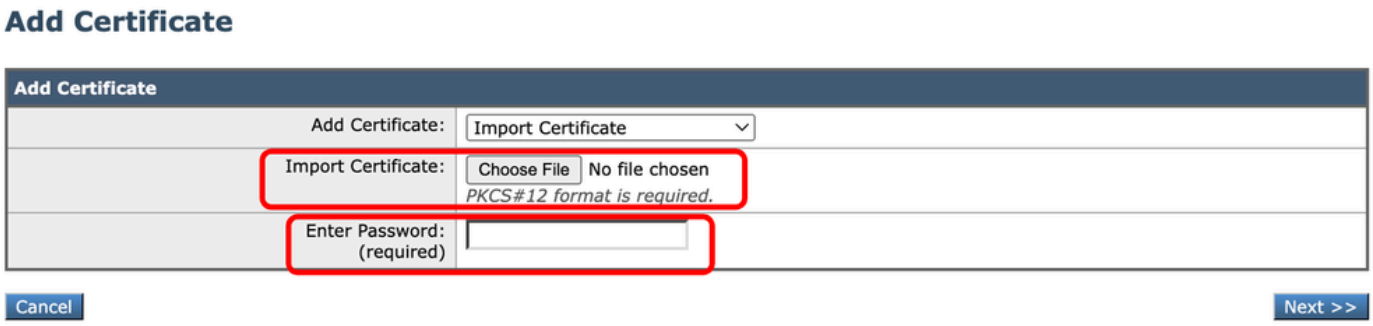
5.4단계. 현재 자체 서명 인증서가 적합한 경우 이를 제출합니다.

5.5단계. 7단계로 건너뜁니다.

6단계. Import Certificate(인증서 가져오기)를 선택한 경우.

6.1단계. 인증서 파일 가져오기(PKCS#12 형식 필요)

6.2단계. 인증서 파일의 암호를 입력 합니다.



이미지 - 인증서 가져오기

6.3단계. Next(다음)를 클릭합니다.

6.4단계. 변경 사항을 제출합니다.

7단계. 변경 사항을 커밋합니다.

8단계. CLI에 로그인합니다.

9단계. certconfig를 입력하고 Enter 키를 누릅니다.

10단계. SETUP을 입력합니다.

11단계. Y를 입력한 다음 Enter 키를 누릅니다.

참고: 인증서가 변경되면 현재 웹 사용자 인터페이스에 로그인한 관리자 사용자에게 연결 오류가 발생할 수 있으며, 제출되지 않은 변경 사항이 손실될 수 있습니다. 이는 인증서가 브라우저에서 신뢰하는 것으로 표시되지 않은 경우에만 발생합니다.

12단계. 사용 가능한 인증서 목록에서 선택하려면 2를 선택합니다.

13단계. GUI에 사용할 원하는 인증서 수를 선택합니다.

14단계. 중간 인증서가 있고 이를 추가하려는 경우 유형 Y 또는 유형 N.

참고: 중간 인증서를 추가해야 하는 경우 PEM 형식으로 중간 인증서를 붙여 넣고 '.'(마침표만)로 끝내야 합니다.

```
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 inter
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.
```

15단계. commit을 입력하여 변경 사항을 저장합니다.

명령줄에서 인증서 테스트

다음과 같이 openssl 명령을 사용하여 인증서를 확인할 수 있습니다.

```
openssl s_client -connect
```

```
:
```

이 예에서 호스트 이름은 SWA.cisco.com이고 관리 인터페이스는 기본값으로 설정됩니다(TCP 포트 8443).

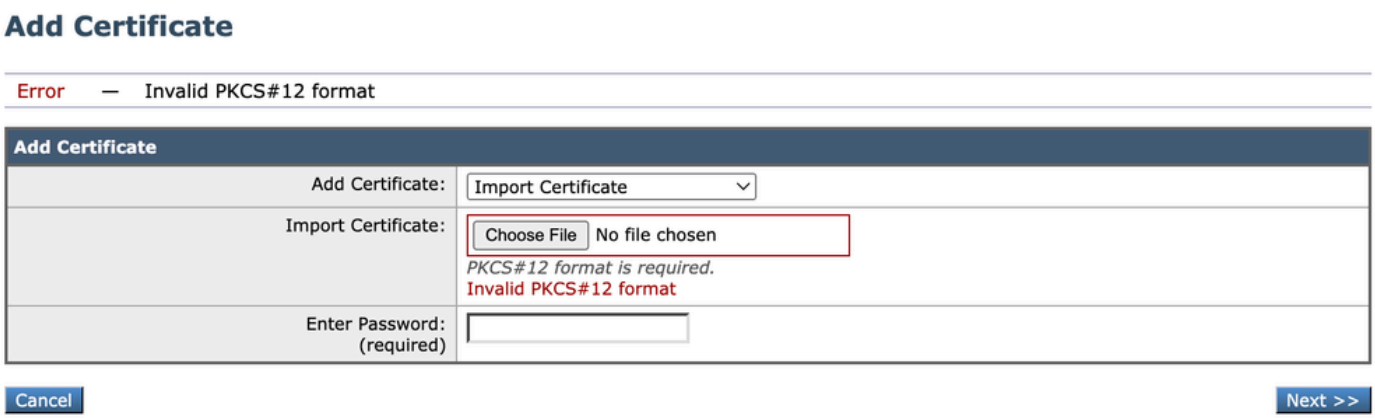
출력의 두 번째 행에서 인증서 세부사항을 볼 수 있습니다.

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

일반 오류

다음은 GUI 인증서를 생성하거나 수정하는 동안 발생할 수 있는 몇 가지 일반적인 오류입니다.

오류: 잘못된 PKCS#12 형식



이미지 - 잘못된 PKCS#12 형식

이 오류의 원인은 두 가지일 수 있습니다.

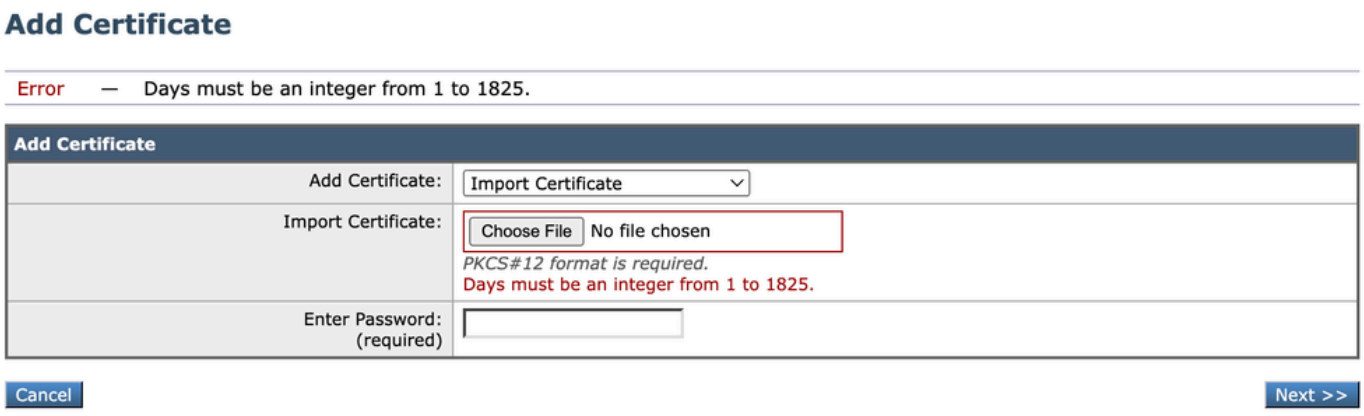
1. 인증서 파일이 손상되어 유효하지 않습니다.

   인증서를 열어 보십시오. 여는 동안 오류가 발생하면 인증서를 다시 생성하거나 다운로드할 수 있습니다.

2. 이전에 생성된 CSR이 더 이상 유효하지 않습니다.

   CSR을 생성할 때 변경 사항을 제출 및 커밋해야 합니다. 그 이유는 로그아웃하거나 페이지를 변경할 때 CSR이 저장되지 않았기 때문입니다. CSR을 생성할 때 생성한 프로필에는 인증서를 성공적으로 업로드하는 데 필요한 개인 키가 포함되어 있습니다. 이 프로필이 사라지면 개인 키가 사라집니다. 따라서 다른 CSR을 생성한 다음 다시 한 번 CA로 가져와야 합니다.

일은 정수여야 합니다.



이미지 - 일은 정수 오류여야 합니다.

이 오류는 업로드된 인증서가 만료되었거나 유효기간이 0일인 경우 발생합니다.

문제를 해결하려면 인증서 만료 날짜를 확인하고 SWA 날짜 및 시간이 올바른지 확인하십시오.

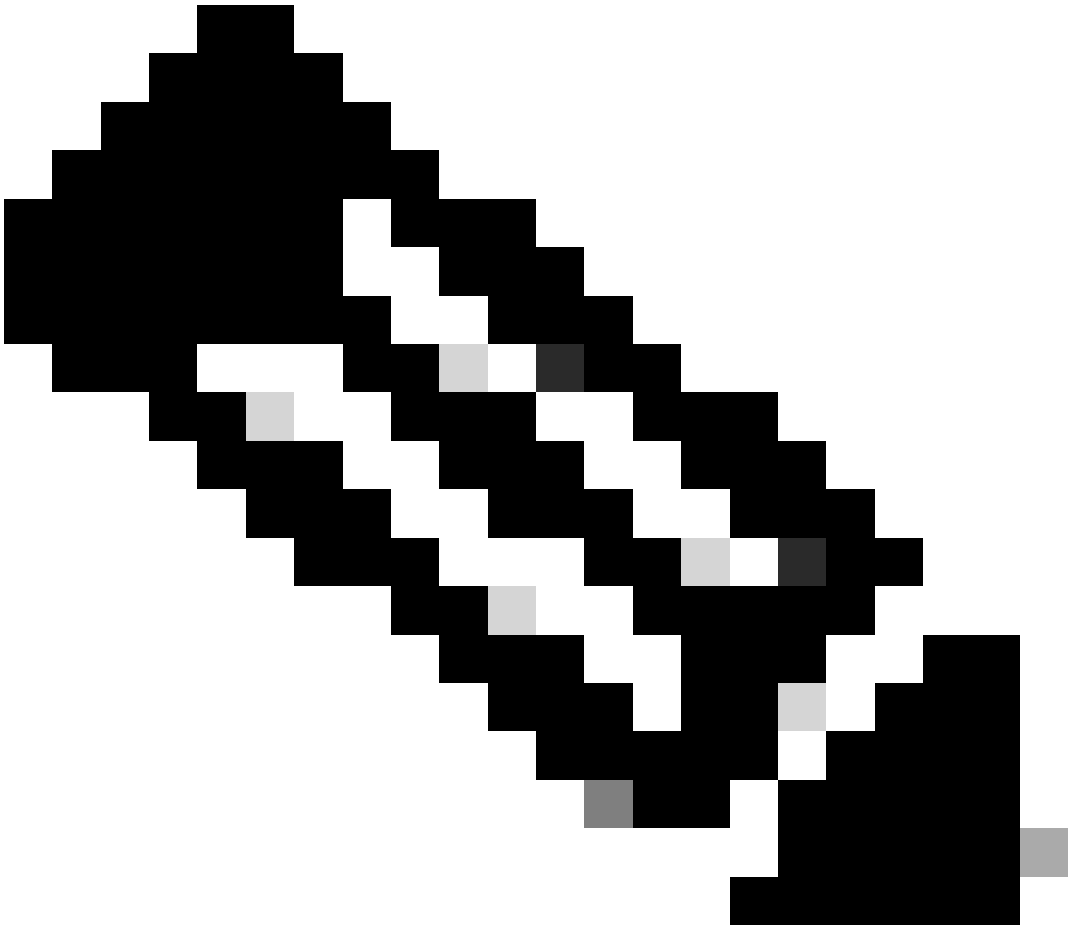
인증서 유효성 검사 오류

이 오류는 루트 CA 또는 중간 CA가 SWA의 신뢰할 수 있는 루트 인증서 목록에 추가되지 않았음을 의미합니다. Root CA 및 Intermediate CA를 모두 사용하는 경우 이 문제를 해결하려면 다음을 수행합니다.

1. SWA에 루트 CA를 업로드한 다음 Commit을 수행합니다.

2. 중간 CA를 업로드한 다음 변경 사항을 다시 커밋합니다.

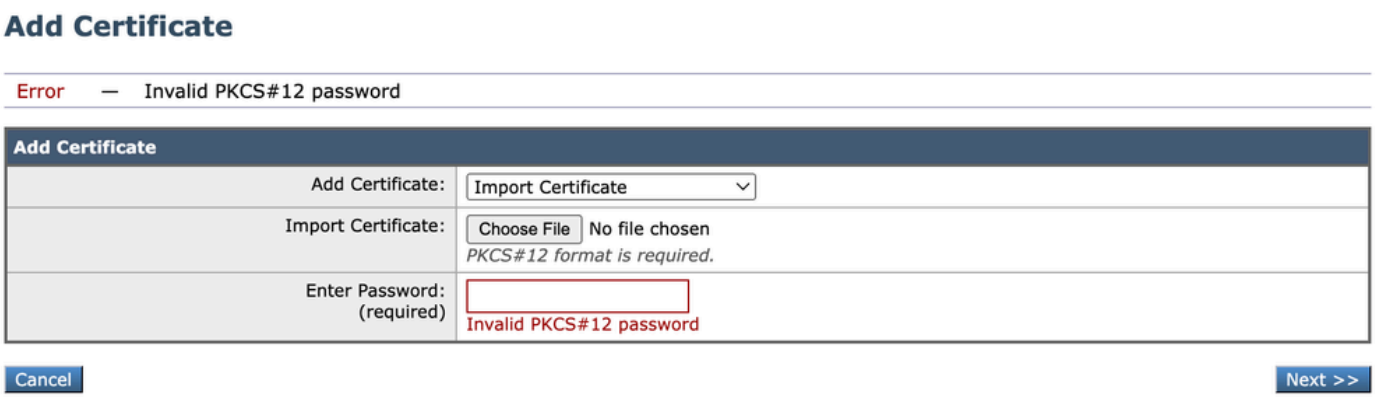
3. GUI 인증서를 업로드합니다.



참고: 루트 또는 중간 CA를 업로드하려면 GUI에서 Network(네트워크)를 선택합니다. Certificate Management(인증서 관리) 섹션에서 Manage Trusted Root Certificates(신뢰할 수 있는 루트 인증서 관리)를 선택합니다. Custom Trusted Root Certificates(맞춤형 신뢰할

수 있는 루트 인증서)에서 Import(가져오기)를 클릭하여 CA 인증서를 업로드합니다.

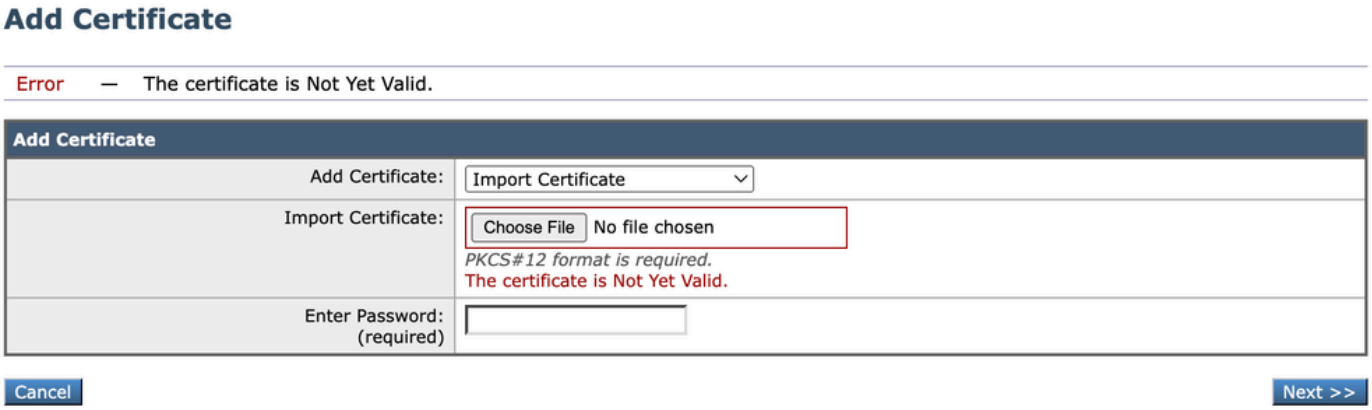
잘못된 암호



이미지 - 잘못된 암호

이 오류는 PKCS#12 인증서 암호가 잘못되었음을 나타냅니다. 오류를 해결하려면 올바른 암호를 입력하거나 인증서를 다시 생성하십시오.

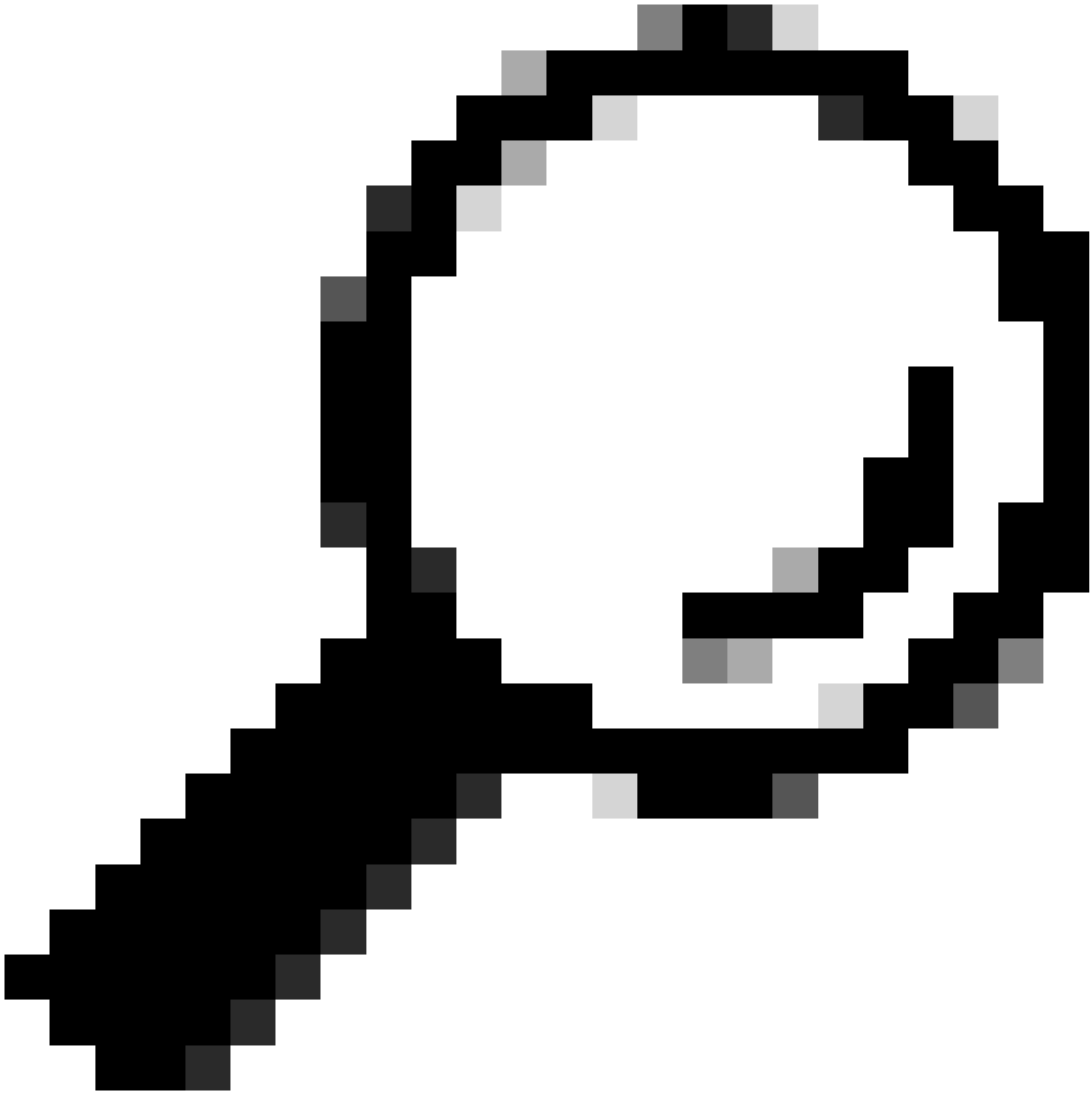
인증서가 아직 유효하지 않습니다.



이미지 - 인증서가 아직 유효하지 않음

1. SWA 날짜 및 시간이 정확한지 확인합니다.

2. 인증서 날짜를 확인하고 "이전 아님" 날짜와 시간이 정확한지 확인합니다.



팁: 방금 인증서를 생성한 경우 잠시 기다렸다가 인증서를 업로드하십시오.

CLI에서 GUI 서비스 다시 시작

WebUI 서비스를 다시 시작하려면 CLI에서 다음 단계를 사용할 수 있습니다.

1단계. CLI에 로그인합니다.

2단계. Type diagnostic(이 명령은 숨겨진 명령이며 TAB을 사용하여 자동으로 입력하지 않음).

3단계. 서비스를 선택합니다.

4단계. WEBUI를 선택합니다.

5단계. RESTART(재시작)를 선택합니다.

관련 정보

- AsyncOS 15.0 for Cisco Secure Web Appliance 사용 설명서 - GD(일반 배포) - 정책 애플리케이션 최종 사용자 분류 [Cisco Secure Web Appliance] - Cisco

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.