두 SWA 간 컨피그레이션 마이그레이션

목차

소개

이 문서에서는 SWA(Secure Web Appliance)에서 다른 어플라이언스로 컨피그레이션을 복원하는 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- SWA의 그래픽 사용자 인터페이스(GUI)에 액세스

- SWA에 대한 관리 액세스
- SMA(Security Management Appliance)에 대한 관리 액세스
- Cisco Software Licensing Portal 또는 SWA 라이센스 파일에 액세스
- Active Directory는 SWA를 도메인에 가입시키고 DNS 레코드를 생성하기 위해 사용자 액세스 권한을 부여했습니다.

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.

시작하기 전에

이 문서에서는 소스 SWA에서 대상 SWA로 마이그레이션하는 단계를 간략하게 설명합니다. 이 표에는 각 시스템의 사양이 나열되어 있습니다.

	소스 SWA	대상 SWA
모델	S396	S100v
버전	15.5.0-710	15.5.0-710
라이선스	Smart 라이센스	Smart 라이센스
액티브 디렉토리	조인됨	조인됨
ISE(Identity Services Engine)와 통합	예	예
NIC(Network Interface Card) 수	5	5

HTTPS 암호 해독	자체 서명 인증서를 사용하여 활성화됨	자체 서명 인증서를 사용하여 활성화됨
투명 리디렉션	WCCP	WCCP
SMA에서 관리	예	예
외부 로그 서버	SCP 푸시	SCP 푸시
고가용성	활성화됨	활성화됨

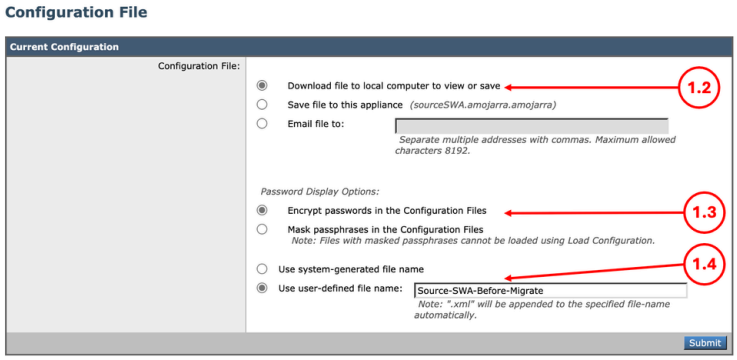
참고: 새 가상 SWA를 설치할 때는 항상 Cisco에서 권장하는 모든 네트워크 인터페이스가 VM(가상 머신)에 존재하고 구성되어 있는지 확인합니다. 인터페이스는 연결을 끊은 상태로 유지할 수 있지만 VM 내에서 사용 가능해야 합니다.

한 디바이스에서 다른 디바이스로 SWA를 마이그레이션할 때 가능한 시나리오는 두 가지입니다.
[시나리오-1] 기존 SWA 교체: 원래 SWA가 해제되고 대상 SWA의 IP 주소가 소스 SWA와 동일합니다.
[시나리오-2] 새 SWA 추가: 원래 SWA는 새 SWA가 구성되는 동안 계속 사용 중입니다.

소스 SWA 준비 및 백업

소스 SWA에서 필요한 파일 및 컨피그레이션을 수집하려면 다음 단계를 수행합니다.

1단계. 컨피그레이션 파일 내보내기	1.1단계. GUI에서 System Administration(시스템 관리)으로 이동하고 Configuration File(컨피그레이션 파일)을 선택합니다. 1.2단계. 보거나 저장할 로컬 컴퓨터에 파일 다운로드가 선택되었는지 확인합니다. 1.3단계. Encrypt passwords in the Configuration Files(컨피그레이션 파일에서 비밀번호 암호화)를 선택합니다 1.4단계. (선택 사항) 컨피그레이션 파일의 이름을 선택합니다. 1.5단계. Submit(제출)을 클릭합니다.

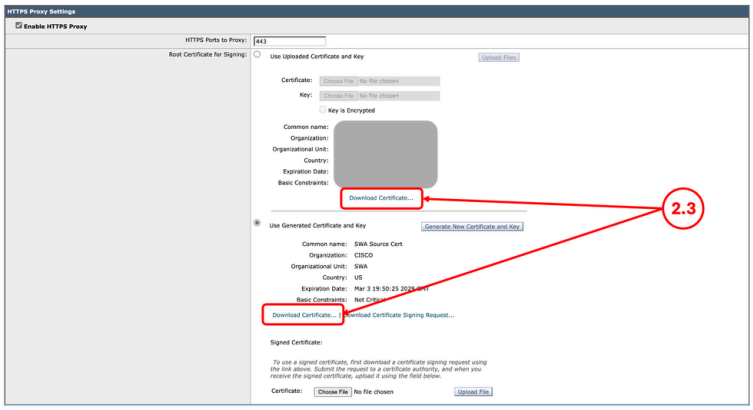
<table>
<tr>
<td></td>
<td> 

이미지 - 컨피그레이션 파일 내보내기</td>
</tr>
<tr>
<td>2단계. 암호 해독 인증서 내보내기

참고: HTTPS 암호 해독이 비활성화된 경우 3단계로 건너뜁니다.</td>
<td>2.1단계. GUI에서 Security Services(보안 서비스)로 이동하고 HTTPS Proxy(HTTPS 프록시)를 클릭합니다.

2.2단계. 설정 편집을 클릭합니다.

2.3단계. Download Certificate..(인증서 다운로드...)를 클릭하여 HTTPS 암호 해독 인증서를 다운로드합니다. 링크를 클릭합니다.

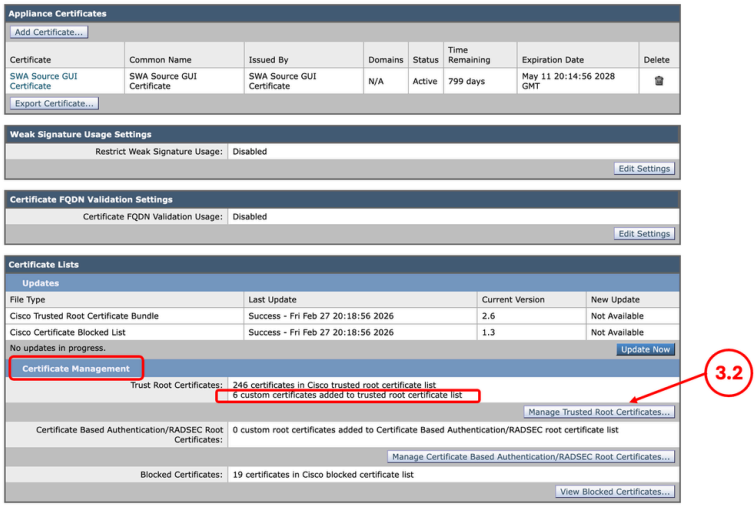
 

이미지 - HTTPS 암호 해독 인증서

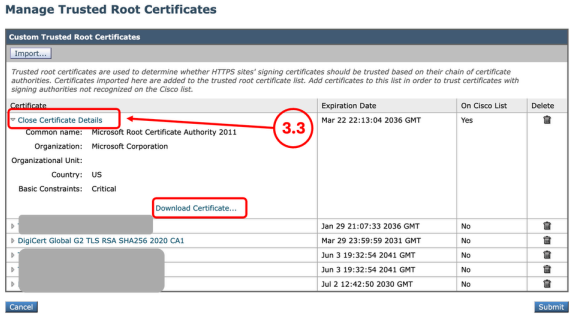
참고: 이 예에서는 두 가지 유형의 HTTPS 암호 해독 인증서가 모두 표시되어 있습니다. 그러나 네트워크에서는 한 가지 유형만 구축할 수 있습니다.</td>
</tr>
<tr>
<td>3단계. 사용자 지정 트러스트 루트 인증서 내보내기

참고: SWA에 추가된 신뢰할 수 있는 사용자 지정 루트 인증서가 없으면 4단계로 건너뜁니다.</td>
<td>3.1단계. GUI에서 Network(네트워크)로 이동하고 Certificate Management(인증서 관리)를 클릭합니다.

3.2단계. Certificate Management(인증서 관리) 섹션에서 Manage Trusted Root Certificates(신뢰할 수 있는 루트 인증서 관리)를 클릭합니다.</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>
Certificate Management


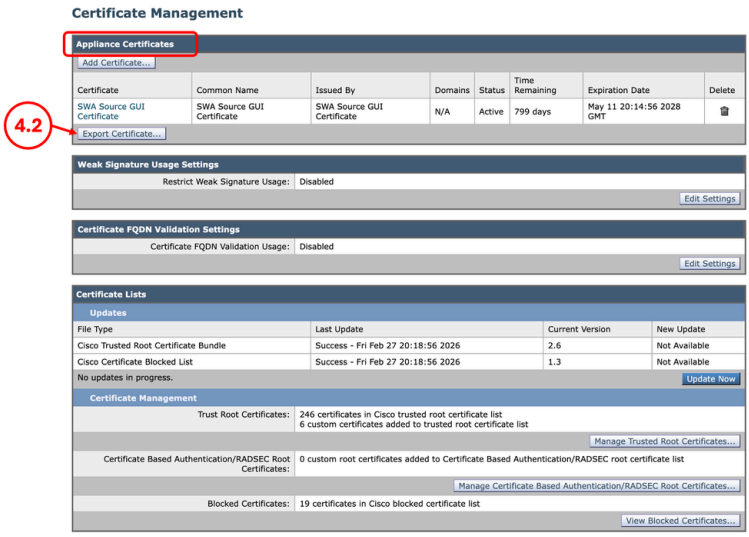
이미지 - 신뢰할 수 있는 루트 인증서 관리

3.3단계. 각 Custom Trusted Root Certificates(사용자 지정 신뢰할 수 있는 루트 인증서)의 이름을 클릭하여 확장하고 Download Certificate(인증서 다운로드)...를 클릭합니다.


이미지 - 신뢰할 수 있는 루트 인증서 다운로드
</td>
</tr>
<tr>
<td>
4단계. GUI 인증서 내보내기

참고: 내장 GUI 인증서를 사용하는 경우 5단계로 건너뜁니다.
</td>
<td>
4.1단계. GUI에서 Network(네트워크)로 이동하고 Certificate Management(인증서 관리)를 클릭합니다.

4.2단계. Appliance Certificates(어플라이언스 인증서) 섹션에서 Export Certificate(인증서 내보내기)를 클릭합니다.
</td>
</tr>
</table>

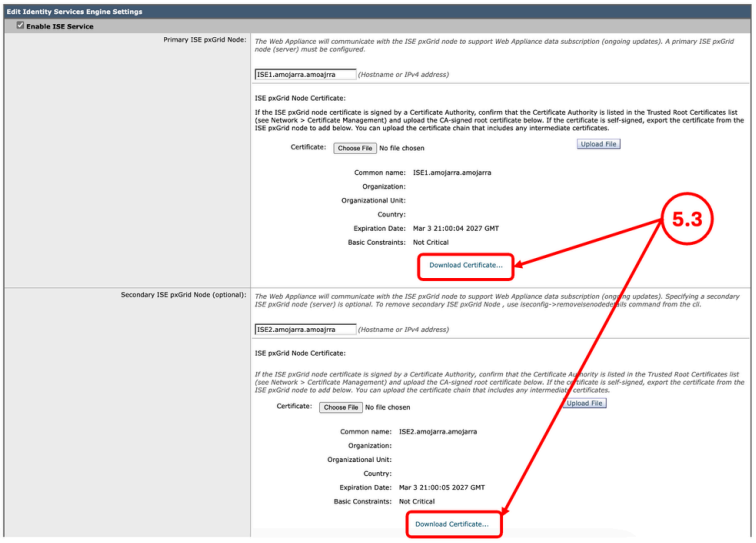
<table>
<tr><td></td><td> 

이미지 - GUI 인증서 내보내기</td></tr>
<tr><td>5단계. ISE 인증서 내보내기

참고: SWA, ISE 통합이 없는 경우 6단계로 건너뜁니다.</td><td>5.1단계. GUI에서 Network(네트워크)로 이동하고 Identity Services Engine(Identity Services 엔진)을 클릭합니다.

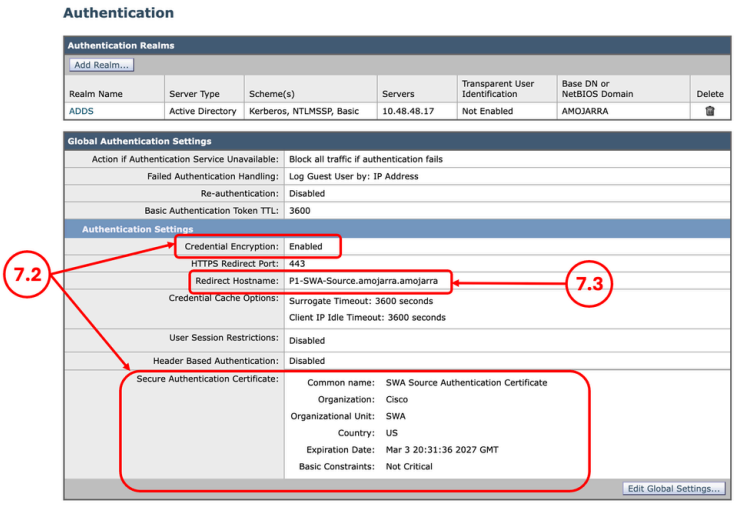
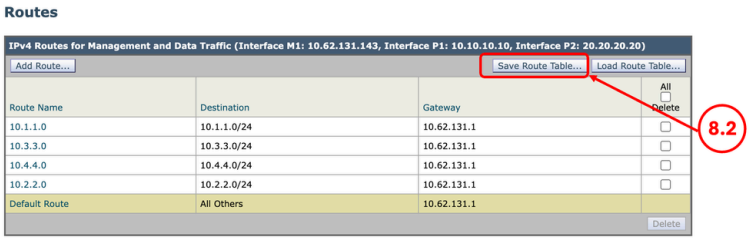
5.2단계. 설정 편집을 클릭합니다.

5.3단계. 사용 가능한 모든 인증서를 다운로드합니다.

이미지 - ISE 인증서 다운로드</td></tr>
<tr><td>6단계. 라이센스/기능</td><td>6.1단계. GUI에서 System Administration(시스템 관리)으로 이동하고 Licenses(라이센스) 또는 Features(기능)를 클릭하면 사용 중인 라이센스 유형에 따라 달라집니다.

6.2단계. 라이센스/기능의 스크린샷을 찍습니다.</td></tr>
</table>

7단계. 인증 리디렉션 인증서	7.1단계. GUI에서 Network(네트워크)로 이동하고 Authentication(인증)을 클릭합니다. 7.2단계. 자격 증명 암호화가 활성화된 경우 인증서 및 키가 있는지 확인합니다. 7.3단계. 현재 컨피그레이션을 스크린샷합니다.  이미지 - 인증 인증서 참고: GUI에서 인증 인증서를 다운로드할 수 없습니다.
8단계. 고정 경로 내보내기 참고: 대상 SWA에 동일한 네트워크 컨피그레이션 및 IP 주소를 사용하려는 경우 10단계로 건너뜁니다.	8.1단계. GUI에서 Network(네트워크)로 이동하고 Routes(경로)를 클릭합니다. 8.2단계. 각 라우팅 테이블에 대해 Save Route Table(경로 테이블 저장)을 클릭합니다.  이미지 - 라우팅 테이블 내보내기
9단계. DNS 설정 참고: 대상 SWA에 동일한 네트워크 컨피그레이션 및 IP 주소를 사용하려	9.1단계. GUI에서 Network(네트워크)로 이동하고 DNS를 클릭합니다. 9.2단계. DNS 컨피그레이션의 스크린샷을 찍습니다.

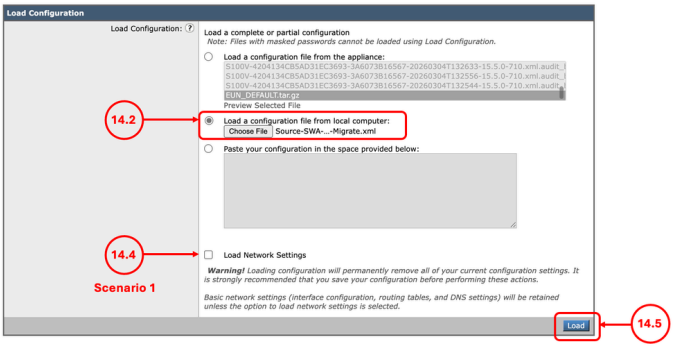
는 경우 10단계로 건너뜁니다.	

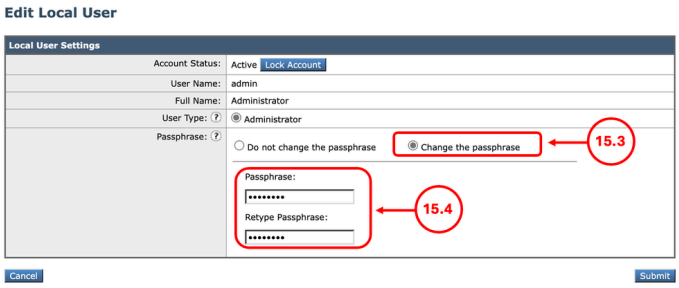
대상 SWA 준비

10단계. 가상 SWA 설치 참고: 대상 SWA가 물리적이면 11단계로 건너뛸 수 있습니다.	10.1단계. 다음 가이드를 사용하여 가상 SWA를 설치합니다. • Vmware ESXi에 보안 웹 어플라이언스 설치 • Microsoft Hyper-V에 Secure Web Appliance 설치 10.2단계. 새 SWA에 권장 네트워크 액세스 권한이 있는지 확인합니다. • Secure Web Appliance용 방화벽 구성
11단계. 초기 SWA 설정	11.1단계. IP 주소를 구성합니다. 11.2단계. 기본 게이트웨이를 구성합니다. 11.3단계. DNS 서버를 구성합니다. 11.4단계. 어플라이언스 라이센스. 11.5단계. 기능을 활성화합니다. 11.6단계. 시스템 설정 마법사를 실행합니다. 이 문서에서 자세한 단계를 찾을 수 있습니다. Secure Web Appliance 초기 설정
12단계. 구성 파일 삭제 참고: ISE를 SWA와 통합하지 않을 경우 13단계로 건너뛸 수 있습니다.	12.1단계 XML 백업 파일에서 ISE 인증서 컨피그레이션을 제거하려면 이 문서의 Fixing Errors(오류 수정) 섹션을 검토합니다.

대상 SWA에 컨피그레이션 파일 가져오기

13단계. 사용자 지정 신뢰할 수 있는 루트 인증서 가져오기	13.1단계. GUI에서 Network(네트워크)로 이동하고 Certificate Management(인증서 관리)를 클릭합니다.

참고: 사용자 지정 신뢰할 수 있는 루트 인증서를 사용하지 않는 경우 14단계로 건너뜁니다.	13.2단계. Certificate Management(인증서 관리) 섹션에서 Manage Trusted Root Certificates(신뢰할 수 있는 루트 인증서 관리)를 클릭합니다. 13.3단계. Import(가져오기)를 클릭합니다. 13.4단계. 이전에 3단계에서 다운로드한 인증서를 업로드합니다. 주의: 루트 및 중간 인증서를 모두 사용할 수 있는 경우 루트 CA 인증서를 업로드하는 것부터 시작합니다. 변경 사항을 제출하고 커밋한 후 중간 인증서를 가져옵니다.
14단계. 구성 파일 가져오기	14.1단계. GUI에서 System Administration(시스템 관리)으로 이동하고 Configuration File(컨피그레이션 파일)을 선택합니다. 14.2단계. [구성 로드] 섹션에서 [로컬 컴퓨터에서 구성 파일 로드]를 선택합니다. 14.3단계. 파일 선택을 클릭하고 XML 구성 파일을 선택합니다. 14.4단계 마이그레이션이 시나리오 1과 일치하고 이전 IP 주소를 새 SWA에서 사용해야 하는 경우 Load Network Settings(네트워크 설정 로드) 확인란을 선택합니다. 그렇지 않으면 이 옵션을 선택하지 않습니다. 14.5단계. Load(로드)를 클릭합니다. 14.6단계. Confirm Load Configuration(컨피그레이션 로드 확인) 팝업에서 Continue(계속)를 클릭합니다.  이미지 - 컨피그레이션 가져오기

15단계. 관리자 비밀번호 변경 참고: Source SWA admin(소스 SWA 관리자) 비밀번호가 있는 경우 16단계로 건너뜁니다.	15.1. GUI에서 System Administration(시스템 관리)으로 이동하고 Users(사용자)를 선택합니다. 15.2. admin 사용자 이름을 클릭합니다. 15.3. 암호 변경을 선택합니다. 15.4. 비밀번호를 입력합니다. 15.5. Submit(제출)을 클릭합니다.  이미지 - 관리자 비밀번호 변경
16단계. 커밋	16.1단계. 이제 변경 사항을 커밋할 수 있습니다.
17단계. 경로 가져오기 참고: 컨피그레이션을 가져오는 동안 네트워크 설정을 로드하는 경우 19단계로 건너뜁니다.	17.1단계. GUI에서 Network(네트워크)로 이동하고 Routes(경로)를 클릭합니다. 17.2단계. 각 라우팅 테이블에 대해 Load Route Table(경로 테이블 로드)을 클릭합니다. 17.3단계.8단계에서 내보낸 파일을 선택합니다. 17.4단계. 제출을 클릭합니다. 17.5단계. 변경 사항을 커밋합니다.
18단계. DNS 설정 구성 참고: 컨피그레이션을 가져오는 동안 네트워크 설정을 로드하는 경우 19단계로 건너뜁니다.	18.1단계. GUI에서 Network(네트워크)로 이동하고 DNS를 클릭합니다. 18.2단계. Edit Settings(설정 편집)를 클릭합니다. 18.3단계. 9단계의 스크린샷 사용 18.4단계. Submit(제출)을 클릭합니다. 18.5단계. 변경 사항을 커밋합니다.

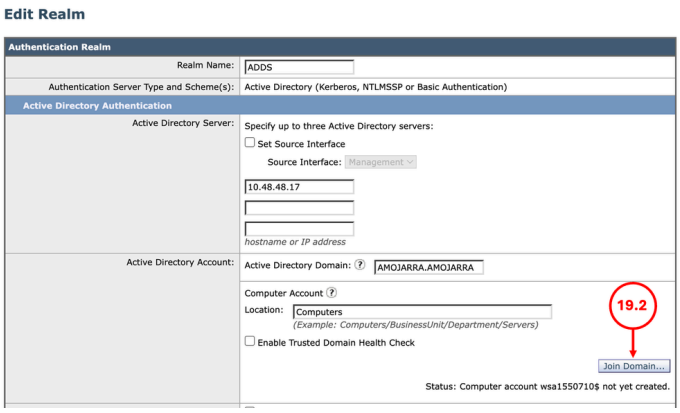
19단계. SWA를 Active Directory에 가입/재가입

19.1단계. GUI에서 Network(네트워크)로 이동하고 Authentication(인증)을 클릭합니다.

19.2단계 인증 영역 이름의 이름을 클릭합니다.

팁: SWA에 새 IP 주소 및 호스트 이름이 할당된 경우 Active Directory DNS 서비스에 필요한 DNS 레코드가 생성되었는지 확인합니다.

19.2단계. Join Domain(도메인 조인)을 클릭하고 자격 증명을 입력합니다.

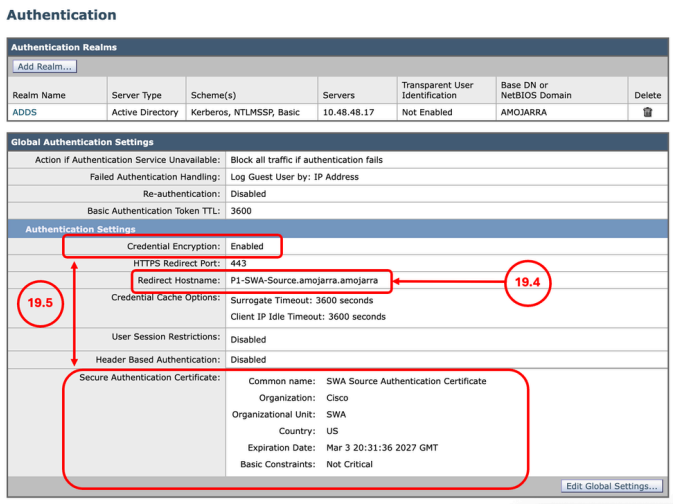


이미지 - Active Directory 도메인에 가입

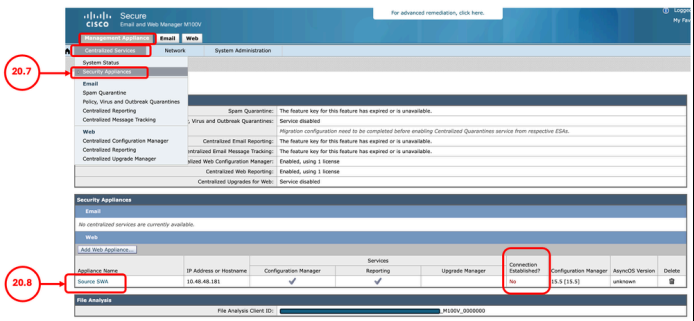
19.3단계. Submit(제출)을 클릭합니다.

19.4단계. 리디렉션 호스트 이름이 올바른지 확인합니다.

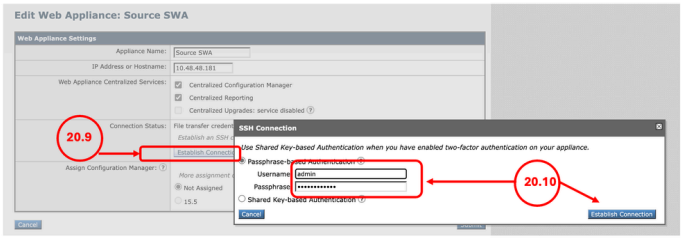
19.5단계. 자격 증명 암호화가 활성화된 경우 보안 인증 인증서가 올바른지 확인합니다.



이미지 - 인증 설정

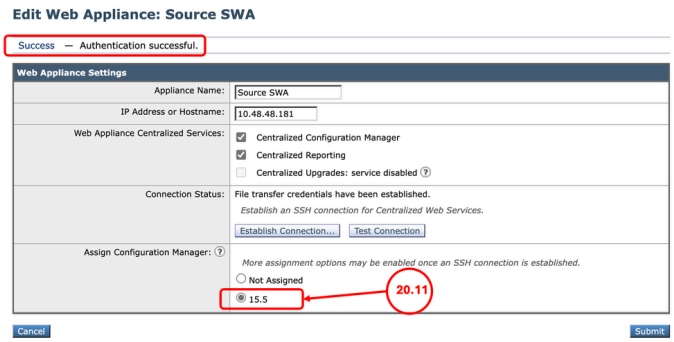
	19.6단계. 변경 사항을 커밋합니다.
20단계. SMA에 다시 참가 참고: SMA에서 SWA를 관리하지 않는 경우 이 단계를 건너뜁니다.	참고: 기존 SWA(Scenario-2)를 교체하지 않았고 마이그레이션된 SWA에 새 IP 주소가 있는 경우 SWA를 새 디바이스로 SMA에 추가하고 20단계를 건너뜁니다. 20.1단계. SMA의 CLI에 연결합니다. 20.2단계. logconfig를 실행합니다. 20.3단계. HOSTKEYCONFIG를 입력합니다. 20.4단계. DELETE를 입력하고 Enter 키를 누릅니다. 20.5단계. 최근에 마이그레이션된 SWA와 관련된 번호를 입력하고 마법사가 완료될 때까지 Enter 키를 누릅니다. 20.6단계. commit을 입력하고 Enter를 눌러 변경 사항을 저장합니다. 20.7단계. SMA GUI에서 Management Appliance로 이동합니다. Centralized Services를 선택하고 Security Appliances를 클릭합니다. 20.8단계. 최근에 마이그레이션된 SWA의 이름을 클릭합니다. 팁: Connection Established(연결 설정됨) 열이 No(아니요)로 설정된 것을 확인할 수 있습니다.  이미지 - SMA Security Appliance 상태 20.9단계. Establish Connection(연결 설정)을 클릭합니다.

20.10단계. 사용자 이름과 암호를 입력하고 Establish Connection(연결 설정)을 클릭합니다.



이미지 - SWA에 대한 연결 설정

20.11단계. Configuration Manager를 할당합니다.



이미지 - Configuration Manager 할당

20.12단계. 변경 사항을 제출 및 커밋합니다.

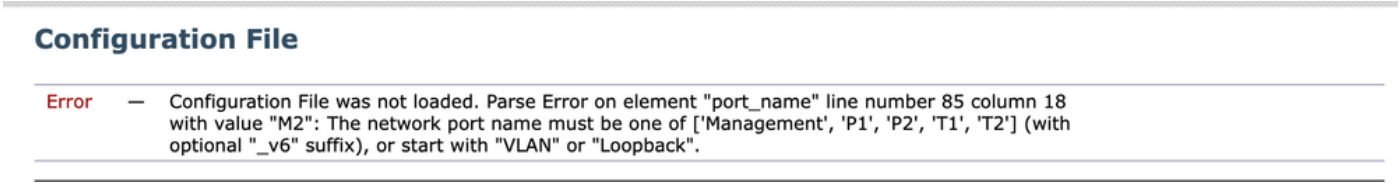
20.13단계(선택 사항) SWA에 컨피그레이션을 게시하여 테스트할 수 있습니다.

팁: SMA는 이전 SWA의 모든 보고 및 추적 데이터를 유지합니다.

오류 수정

port_name 요소 구문 분석 오류

네트워크 포트 이름은 ['Management', 'P1', 'P2', 'T1', 'T2'] 중 하나여야 합니다.



이미지 - 네트워크 인터페이스 이름 지정 오류

```
Error    –    Configuration File was not loaded. Parse Error on element "port_name" line number 85 colu
```

이 오류는 물리적 SWA에서 가상으로 마이그레이션할 때 발생합니다. 가상 SWA에는 5개의 NIC만 있으며 M2 인터페이스가 잘못되었습니다. 오류를 수정하려면 텍스트 편집기에서 XML 구성 파일을 편집하고 다음 행을 제거합니다.

```
        M2
```

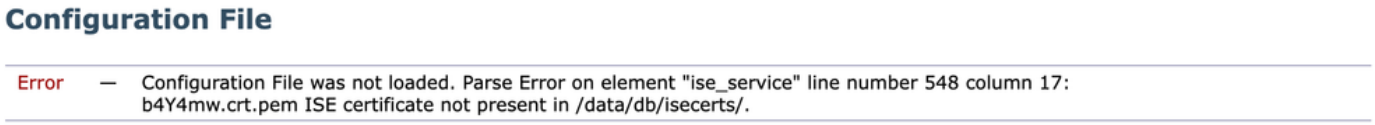
```
         M2
```

```
        M2
```

```
        autoselect
```

aa:bb:cc:00:00:00

요소 ise_service에 대한 구문 분석 오류



이미지 - ISE 인증서 오류

```
Error - Configuration File was not loaded. Parse Error on element "ise_service" line number 548 column
```

ISE 인증서는 SWA 컨피그레이션 내보내기에 포함되지 않으며 디바이스에서 직접 업로드되므로 XML 파일에서 인증서 컨피그레이션을 제거하고 가져오기에 성공한 후 ISE를 수동으로 구성해야 합니다. 이 문제를 해결하려면 텍스트 편집기에서 XML 컨피그레이션 파일을 편집하고 오류에서 인증서 이름을 검색합니다(이 예에서는 AA11AA 검색). 그런 다음 컨피그레이션 파일에서 삭제합니다.

Before:

AA11AA

BB22BB

```
After:
```

인증서 이름 이외에 웹 어플라이언스 클라이언트 인증서 이름도 제거해야 합니다.

이 예에서 웹 어플라이언스 클라이언트 인증서는 자체 서명 인증서입니다.

```
Before:

        1

        xAcK6T

After:

        0
```

새 가상 SWA에서 장애 조치가 작동하지 않음

대상 가상 SWA에서 고가용성(장애 조치)이 작동하지 않는 경우 하이퍼바이저가 올바르게 구성되었는지 확인하십시오. 자세한 내용은 VMware 환경에서 적절한 가상 WSA HA 그룹 기능 확인 을 참조하십시오.

관련 정보

- AsyncOS 15.2 for Cisco Secure Web Appliance 사용 설명서
- Vmware ESXi에 보안 웹 어플라이언스 설치
- Microsoft Hyper-V에 Secure Web Appliance 설치

- Secure Web Appliance 초기 설정
- Cisco Secure Email and Web Virtual Appliance 설치 설명서
- Secure Web Appliance에서 맞춤형 URL 범주 구성 - Cisco
- Secure Web Appliance 모범 사례 사용
- Secure Web Appliance용 방화벽 구성
- Secure Web Appliance에서 암호 해독 인증서 구성
- Secure Web Appliance DNS 서비스 문제 해결
- VMware 환경에서 적절한 가상 WSA HA 그룹 기능 확인

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.