

# 보안 웹 어플라이언스를 이전 버전으로 되돌리기

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[시작하기 전에](#)

[SWA 준비 및 백업](#)

[1단계. 컨피그레이션 파일 내보내기](#)

[2단계. 암호 해독 인증서 내보내기](#)

[3단계. 사용자 지정 트러스트 루트 인증서 내보내기](#)

[4단계. GUI 인증서 내보내기](#)

[5단계. ISE 인증서 내보내기](#)

[6단계. 라이선스/기능](#)

[7단계. 인증 리디렉션 인증서](#)

[8단계. 고정 경로 내보내기](#)

[9단계. DNS 설정](#)

[SWA 되돌리기](#)

[10단계. SWA 되돌리기](#)

[컨피그레이션이 SWA를 되돌렸습니다.](#)

[11단계. SWA 라이선스 부여](#)

[12단계. 시스템 설정 마법사 실행](#)

[13단계. 사용자 지정 신뢰할 수 있는 루트 인증서 가져오기](#)

[14단계. 구성 파일 가져오기](#)

[15단계. 경로 가져오기](#)

[16단계. DNS 설정 구성](#)

[17단계. SWA를 Active Directory에 가입/재가입](#)

[관련 정보](#)

---

## 소개

이 문서에서는 SWA(Secure Web Appliance)를 이전 버전으로 되돌리는 단계에 대해 설명합니다.

## 사전 요구 사항

## 요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- SWA의 그래픽 사용자 인터페이스(GUI)에 액세스
- SWA에 대한 관리 액세스
- Cisco Software Licensing Portal 또는 SWA 라이선스 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

어플라이언스를 되돌리는 것은 매우 파괴적입니다.

Thia는 프로세스에서 폐기되는 데이터이며 백업해야 합니다.

- 현재 시스템 구성 파일입니다.
- 모든 로그 파일(자세한 내용은 [Access Secure Web Appliance 로그 참조](#))
- 모든 보고 데이터(저장된 예약 및 보관된 보고서 포함)
- 사용자 지정 최종 사용자 알림 페이지

---

 경고: 이전 버전으로 되돌리기 전에 해당 특정 버전에 해당하는 암호화된 컨피그레이션 파일이 있는지 확인하십시오. 현재 구성 파일이 이전 소프트웨어 버전과 호환되지 않을 수 있습니다.

---

## SWA 준비 및 백업

되돌리기 전에 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.

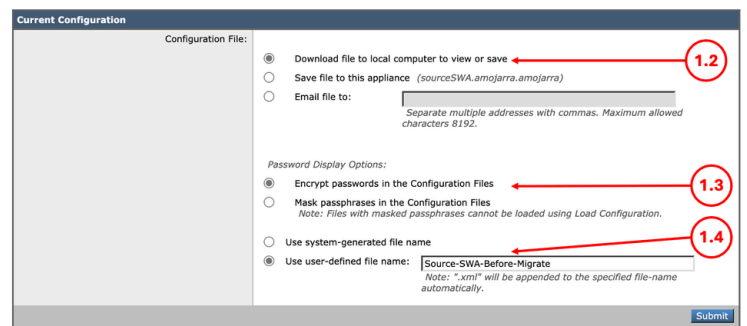
1.2단계. 보거나 저장할 로컬 컴퓨터에 파일 다운로드가 선택되었는지 확인합니다.

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.

#### Configuration File



이미지 - 컨피그레이션 파일 내보내기

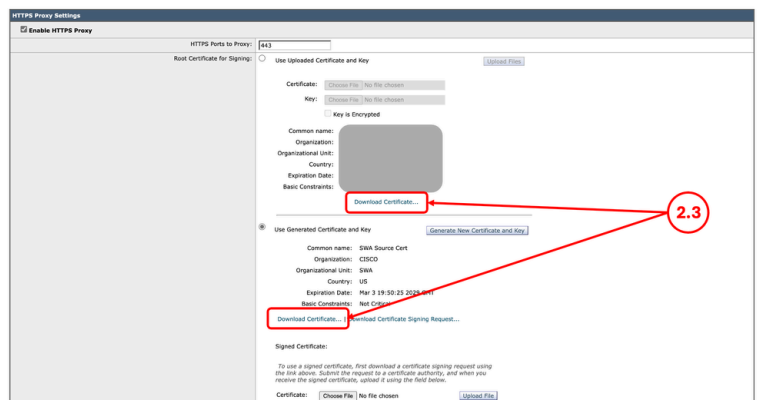
2단계. 암호 해독 인증서 내보내기

 참고: HTTPS 암호 해독이 비활성화된 경우 3단계로 건너뜁니다.


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.



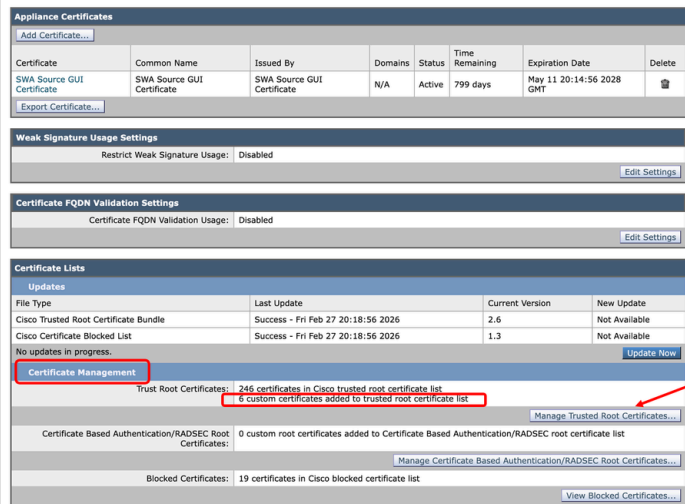
이미지 - HTTPS 암호 해독 인증서

 참고: 이 예에서는 두 가지 유형의 HTTPS 암호 해독 인증서가 모두 표시되어 있습니다. 그러나 네트워크에서는 한 가지 유형만 구축할 수 있습니다.


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.

Certificate Management



Appliance Certificates

Certificate	Common Name	Issued By	Domains	Status	Time Remaining	Expiration Date	Delete
SWA Source GUI Certificate	SWA Source GUI Certificate	SWA Source GUI Certificate	N/A	Active	799 days	May 11 20:14:56 2028 GMT	

Weak Signature Usage Settings

Restrict Weak Signature Usage: Disabled [Edit Settings](#)

Certificate FQDN Validation Settings

Certificate FQDN Validation Usage: Disabled [Edit Settings](#)

Certificate Lists

File Type	Last Update	Current Version	New Update
Cisco Trusted Root Certificate Bundle	Success - Fri Feb 27 20:18:56 2026	2.6	Not Available
Cisco Certificate Blocked List	Success - Fri Feb 27 20:18:56 2026	1.3	Not Available

No updates in progress. [Update Now](#)


**Certificate Management**

Trust Root Certificates: 245 certificates in Cisco trusted root certificate list  
6 custom certificates added to trusted root certificate list [Manage Trusted Root Certificates...](#)

Certificate Based Authentication/RADSEC Root Certificates: 0 custom root certificates added to Certificate Based Authentication/RADSEC root certificate list [Manage Certificate Based Authentication/RADSEC Root Certificates...](#)

Blocked Certificates: 19 certificates in Cisco blocked certificate list [View Blocked Certificates...](#)

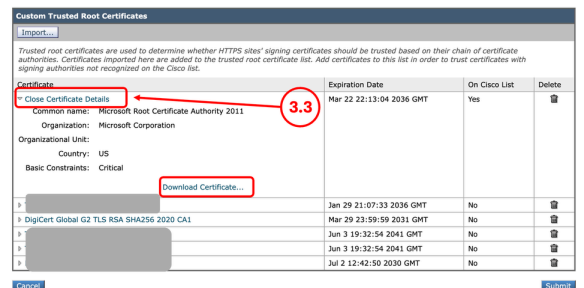
3단계. 사용자 지정 트러스트 루트 인증서 내보내기

 참고: SWA에 추가된 신뢰할 수 있는 사용자 지정 루트 인증서가 없으면 4단계로 건너웁니다.

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

Manage Trusted Root Certificates



Custom Trusted Root Certificates

Trusted root certificates are used to determine whether HTTPS sites' signing certificates should be trusted based on their chain of certificate authorities. Certificates imported here are added to the trusted root certificate list. Add certificates to this list in order to trust certificates with signing authorities not recognized on the Cisco list.

Certificate	Expiration Date	On Cisco List	Delete
Common name: Microsoft Root Certificate Authority 2011 Organization: Microsoft Corporation Country: US Basic Constraints: Critical <a href="#">Download Certificate...</a>	Mar 22 22:13:04 2036 GMT	Yes	
 [Redacted]	Jan 29 21:07:33 2036 GMT	No	
 [Redacted]	Mar 29 23:59:59 2031 GMT	No	
 [Redacted]	Jun 3 19:32:54 2041 GMT	No	
 [Redacted]	Jun 3 19:32:54 2041 GMT	No	
 [Redacted]	Jul 2 12:42:50 2030 GMT	No	


[Cancel](#) [Submit](#)

클릭합니다.

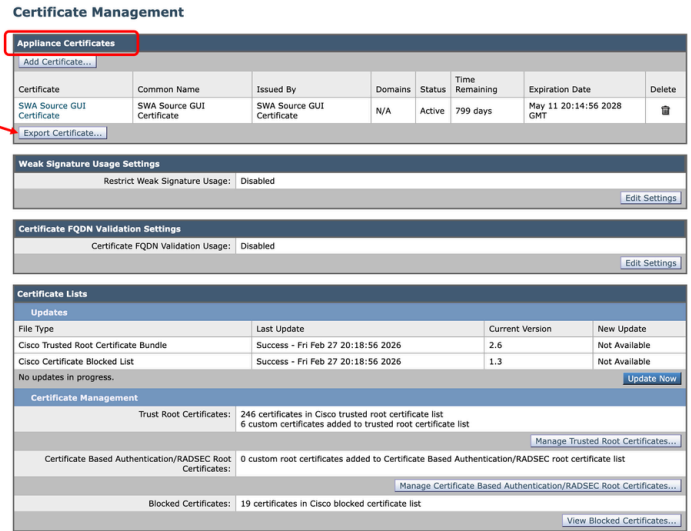
이미지 - 신뢰할 수 있는 루트 인증서 다운로드

4단계. GUI 인증서 내보내기

4.1단계. GUI에서 Network(네트워크)로 이동하고 Certificate Management(인증서 관리)를 클릭합니다.


 참고: 내장 GUI 인증서를 사용하는 경우 5단계로 건너뛩니다.

4.2단계. Appliance Certificates(어플라이언스 인증서) 섹션에서 Export Certificate(인증서 내보내기)를 클릭합니다.

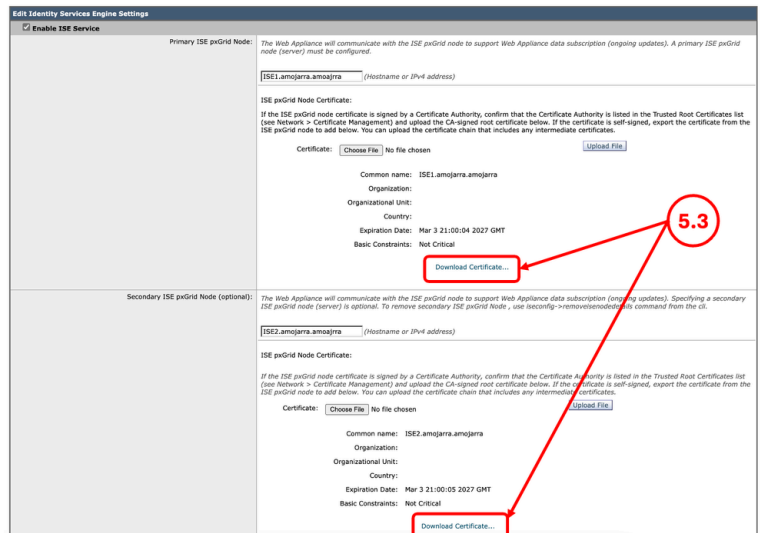


이미지 - GUI 인증서 내보내기

5단계. ISE 인증서 내보내기

 참고: SWA, ISE 통합이 없는 경우 6단계로 건너뛩니다.

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

6단계. 라이선스/기능

6.1단계. GUI에서 System Administration(시스템 관리)으로 이동하고 Licenses(라이선스) 또는 Features(기능)를 클릭하면 사용 중인 라이선스 유형에 따라 달라

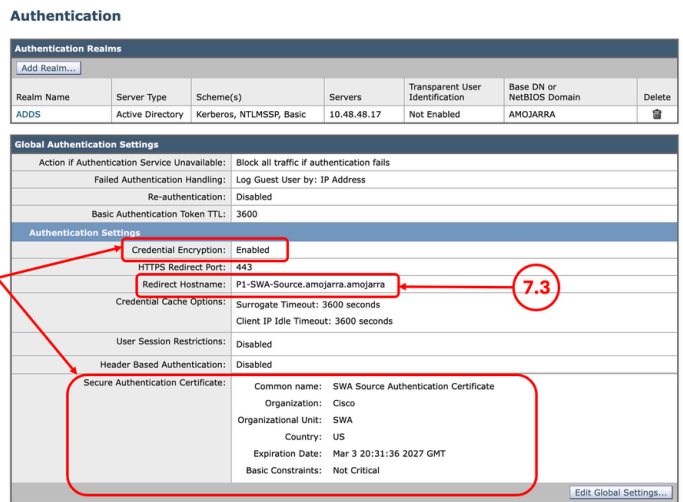
집니다.

6.2단계. 라이선스/기능의 스크린샷을 찍습니다.

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.



7단계. 인증 리디렉션 인증서

이미지 - 인증 인증서



참고: GUI에서 인증 인증서를 다운로드할 수 없습니다.

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.

#### Routes


Route Name	Destination	Gateway	All
10.1.1.0	10.1.1.0/24	10.62.131.1	<input type="checkbox"/>
10.3.3.0	10.3.3.0/24	10.62.131.1	<input type="checkbox"/>
10.4.4.0	10.4.4.0/24	10.62.131.1	<input type="checkbox"/>
10.2.2.0	10.2.2.0/24	10.62.131.1	<input type="checkbox"/>
Default Route	All Others	10.62.131.1	<input type="checkbox"/>

8단계. 고정 경로 내보내기



참고: 대상 SWA에 동일한 네트워크 컨피그레이션 및 IP 주소를 사용하려는 경우 10단계로 건너뜁니다.




이미지 - 라우팅 테이블 내보내기

9단계. DNS 설정	9.1단계. GUI에서 Network(네트워크)로 이동하고 DNS를 클릭합니다.
 참고: 대상 SWA에 동일한 네트워크 컨피그레이션 및 IP 주소를 사용하려는 경우 10단계로 건너뜁니다.	9.2단계. DNS 컨피그레이션의 스크린샷을 찍습니다.

## SWA 되돌리기

10단계. SWA 되돌리기	<p>10.1단계. CLI에 연결합니다.</p> <p>10.2단계. revert를 입력하고 Enter 키를 누릅니다.</p> <p>10.3단계.Y를 입력하고 Enter 키를 눌러 "계속하시겠습니까? [N]&gt; "</p> <p>10.4단계.Y를 입력하고 Enter 키를 눌러 "계속하시겠습니까? [N]&gt;"</p> <p>10.5단계. 목록에서 되돌릴 버전과 연결된 번호를 선택하고 Enter를 누릅니다.</p> <pre>SWA_CLI&gt; revert</pre> <p>This command will revert the appliance to a previous version of AsyncOS.</p> <p>Warning: Reverting the appliance is extremely destructive. The following data will be destroyed in the process and should be backed up:</p> <ul style="list-style-type: none"> <li>- current system configuration file</li> <li>- all log files</li> <li>- all reporting data (including saved scheduled and archived reports)</li> <li>- any custom end user notification pages</li> </ul> <p>This command will try to preserve the current network settings.</p> <p>Reverting the device will cause a reboot to take place. After rebooting, the appliance reinitializes itself and reboots again to the desired version, with the earlier system configuration.</p> <pre>Do you want to continue? [N]&gt; Y Are you sure you want to continue? [N]&gt; Y</pre> <pre> Available versions ===== 1. 12.5.1-011 Please select an AsyncOS version: 1 You have selected "12.5.1-011". The system will now reboot to perform the revert operation.</pre>
----------------	--

컨피그레이션이 SWA를 되돌렸습니다.

<p>11단계. SWA 라이선스 부여</p>	<p>11.1단계. 자세한 내용은 Configure <a href="#">Secure Web Appliance Initial Setup</a>을 참조하십시오.</p>
<p>12단계. 시스템 설정 마법사 실행</p>	<p>12.1단계. 자세한 내용은 Configure <a href="#">Secure Web Appliance Initial Setup</a>을 참조하십시오.</p>
<p>13단계. 사용자 지정 신뢰할 수 있는 루트 인증서 가져오기</p> <hr/> <p> 참고: 사용자 지정 신뢰할 수 있는 루트 인증서를 사용하지 않는 경우 14단계로 건너뛩니다.</p> <hr/> <p> 주의: 루트 및 중간 인증서를 모두 사용할 수 있는 경우 루트 CA 인증서를 업로드하는 것부터 시작합니다. 변경 사항을 제출하고 커밋한 후 중간 인증서를 가져옵니다.</p>	<p>13.1단계. GUI에서 Network(네트워크)로 이동하고 Certificate Management(인증서 관리)를 클릭합니다.</p> <p>13.2단계. Certificate Management(인증서 관리) 섹션에서 Manage Trusted Root Certificates(신뢰할 수 있는 루트 인증서 관리)를 클릭합니다.</p> <p>13.3단계. Import(가져오기)를 클릭합니다.</p> <p>13.4단계. 이전에 3단계에서 다운로드한 인증서를 업로드합니다.</p>
<p>14단계. 구성 파일 가져오기</p> <hr/> <p> 주의: 1단계에서 내보낸 컨피그레이션 파일이 아니라 현재 버전에 해당하는 컨피그레이션 파일을 가져와야 합니다.</p>	<p>14.1단계. GUI에서 System Administration(시스템 관리)으로 이동하고 Configuration File(컨피그레이션 파일)을 선택합니다.</p> <p>14.2단계. [구성 로드] 섹션에서 [로컬 컴퓨터에서 구성 파일 로드]를 선택합니다.</p> <p>14.3단계. 파일 선택을 클릭하고 현재 버전과 관련된 XML 구성 파일을 선택합니다.</p> <p>14.4단계(선택 사항) 되돌리기에서 IP 주소 및 네트워크 컨피그레이션을 제거한 경우 Load Network Settings(네트워크 설정 로드) 확인란을 선택합니다. 그렇지 않으면 이 옵션을 선택하지 않습니다.</p> <p>14.5단계. Load(로드)를 클릭합니다.</p> <p>14.6단계. Confirm Load Configuration(컨피그레이션 로드 확인) 팝업에서 Continue(계속)를 클릭합니다.</p>

	 <p>이미지 - 이전 컨피그레이션 파일 로드</p> <p>14.7단계. 변경 사항을 커밋합니다.</p>
<p>15단계. 경로 가져오기</p> <p> 참고: 컨피그레이션을 가져오는 동안 네트워크 설정을 로드하는 경우 17단계로 건너뛩니다.</p>	<p>15.1단계. GUI에서 Network(네트워크)로 이동하고 Routes(경로)를 클릭합니다.</p> <p>15.2단계. 각 라우팅 테이블에 대해 Load Route Table(경로 테이블 로드)을 클릭합니다.</p> <p>15.3단계. 8단계에서 내보낸 파일을 선택합니다.</p> <p>15.4단계. 제출을 클릭합니다.</p> <p>15.5단계. 변경 사항을 커밋합니다.</p>
<p>16단계. DNS 설정 구성</p> <p> 참고: 컨피그레이션을 가져오는 동안 네트워크 설정을 로드하는 경우 17단계로 건너뛩니다.</p>	<p>16.1단계. GUI에서 Network(네트워크)로 이동하고 DNS를 클릭합니다.</p> <p>16.2단계. [설정 편집]을 클릭합니다.</p> <p>16.3단계. 9단계의 스크린샷 사용</p> <p>16.4단계. Submit(제출)을 클릭합니다.</p> <p>16.5단계. 변경 사항을 커밋합니다.</p>
<p>17단계. SWA를 Active Directory에 가입/재가입</p>	<p>17.1단계. GUI에서 Network(네트워크)로 이동하고 Authentication(인증)을 클릭합니다.</p> <p>17.2단계. 인증 영역 이름의 이름을 누릅니다.</p> <p> <b>팁:</b> SWA에 새 IP 주소 및 호스트 이름이 할당된 경우 Active Directory DNS 서비스에 필요한 DNS 레코드가 생성되었는지 확인합니다.</p>

17.3단계. Join Domain(도메인 참여)을 클릭하고 자격 증명을 입력합니다.

**Add Realm**

Authentication Realm

Realm Name: ADDS

Authentication Server Type and Scheme(s): Active Directory (Kerberos, NTLMSSP or Basic Authentication)

Active Directory Authentication

Active Directory Server: Specify up to three Active Directory servers:

Set Source Interface

Source Interface: Management

10.48.48.17

hostname or IP address

Active Directory Account: Active Directory Domain: amojarra.amojarra

Computer Account: Computers

Location: Computers (Example: Computers/BusinessUnit/Department/Servers)

Enable Trusted Domain Lookup

Join Domain...

Status: Computer account fordwsa125\$ not yet created.

이미지 - Active Directory에 가입

17.4단계. Submit(제출)을 클릭합니다.

17.5단계. 자격 증명 암호화가 사용하도록 설정된 경우 보안 인증 인증서를 가져옵니다.

17.6단계. 리디렉션 호스트 이름이 올바른지 확인합니다.

**Authentication**

Authentication Realms

Realm Name	Server Type	Scheme(s)	Servers	Transparent User Identification	Base DN or NetBIOS Domain	Delete
ADDS	Active Directory	Kerberos, NTLMSSP, Basic	10.48.48.17	Not Enabled	AMOJARRA	

Global Authentication Settings

Action if Authentication Service Unavailable: Block all traffic if authentication fails

Failed Authentication Handling: Log Guest User by: IP Address

Re-authentication: Disabled

Basic Authentication Token TTL: 3600

Authentication Settings

Credential Encryption: Disabled

Redirect Hostname: ws-source.cisco.local

Credential Cache Options: Surrogate Timeout: 3600 seconds  
Client IP Idle Timeout: 3600 seconds

User Session Restrictions: Disabled

Header Based Authentication: Enabled

이미지 - 인증 설정

17.7단계. 변경 사항을 커밋합니다.

## 관련 정보

- [AsyncOS 15.2 for Cisco Secure Web Appliance 사용 설명서](#)
- [Secure Web Appliance 초기 설정](#)

- [Secure Web Appliance 모범 사례 사용](#)
- [Secure Web Appliance 로그 액세스](#)

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.