# HTTPS 암호 해독용 WSA 인증서 사용

## 목차



## 소개

이 문서에서는 Cisco WSA(Web Security Appliance)에서 HTTPS 암호 해독에 사용해야 하는 인증서의 유형에 대해 설명합니다.

## 인증서 개요

WSA에는 현재 인증서 및 개인 키를 사용하여 HTTPS 암호 해독에 사용할 수 있습니다.그러나 모든 x.509 인증서가 작동하지는 않으므로 사용해야 하는 인증서 유형에 혼란이 있을 수 있습니다.

인증서에는 두 가지 주요 유형이 있습니다.**서버 인증서** 및 **루트 인증서**.모든 x.509 인증서는 인증서의 유형을 식별하는 Basic Constraints 필드를 포함합니다.

- **Subject Type=End Entity** - 서버 인증서
- **주체 유형=CA** - 루트 인증서

> **참고:**WSA에서 HTTPS 암호 해독에 루트 인증서(CA(Certificate Authority) 서명 인증서라고도 함)를 사용해야 합니다.

### 루트 인증서

서버 인증서를 서명하기 위해 루트 인증서가 특별히 생성됩니다.자체 CA를 생성 및 운영하고 자체 서버 인증서에 서명할 수 있습니다.

> **참고:**루트 인증서는 다른 인증서만 서명하므로 HTTPS 암호화 및 암호 해독을 수행하기 위해 웹 서버에서 사용할 수 없습니다.

HTTPS 암호 해독용 서버 인증서를 능동적으로 생성하려면 WSA에서 루트 인증서를 사용해야 합니다.루트 인증서 사용에는 두 가지 옵션이 있습니다.

- WSA에서 루트 인증서를 생성합니다.WSA는 자체 루트 인증서 및 개인 키를 만들고 이 키 쌍을 사용하여 서버 인증서를 서명합니다.
- 현재 루트 인증서 및 개인 키를 WSA에 업로드할 수 있습니다.루트 인증서의 CN(Common Name) 필드는 서명이 포함된 서버 인증서를 신뢰하는 엔티티(일반적으로 회사 이름)를 식별합니다.

  **참고:**서버 인증서를 신뢰할 수 있으려면 웹 브라우저에 공개 키가 있는 루트 인증서에 의해 서명되어야 합니다.

### 서버 인증서

서버 인증서는 HTTPS 암호화 및 암호 해독에 사용되고 특정 서버의 신뢰성을 확인하기 위해 특별히 생성됩니다.서버 인증서는 CA 루트 인증서를 사용하여 CA에 의해 서명됩니다.CA의 일반적인 예는 VeriSign 또는 Thawte입니다.

**참고:**다른 인증서에 서명하기 위해 서버 인증서를 사용할 수 없습니다.따라서 WSA에 서버 인증서가 설치된 경우 HTTPS 암호 해독이 작동하지 않습니다.

서버 인증서의 CN 필드는 인증서를 사용할 호스트를 지정합니다.예를 들어, **https://www.verisign.com**는 CN이 www.verisign.com인 서버 인증서를 **사용합니다**.

## 관련 정보

- WSA(Web Security Appliance) 인증서 사용(HTTPS 암호 해독, GUI 로그인, 자격 증명 암호화)
- WSA 및 CSR(Certificate Signing Request) 옵션에서 HTTPS 프록시를 활성화하는 단계
- HTTPS 프록시를 (WSA) 및 루트/중간 인증서 업로드 옵션 활성화 단계
- 기술 지원 및 문서 – Cisco Systems