# Umbrella 필터링을 사용하는 동안 브라우저 인증서 해지 오류 트러블슈팅

## 목차



## 소개

이 문서에서는 Umbrella 필터링을 사용하는 동안 브라우저 인증서 해지 오류를 해결하는 방법에 대해 설명합니다.

## 문제

Allow-Only Mode(허용 전용 모드) 또는 Limited Category Settings(제한적인 범주 설정)를 사용할 때 사이트가 제대로 로드되기 위해 여러 도메인을 허용 목록에 추가해야 하는 경우가 많습니다.

한 가지 구체적인 문제는 HTTPS/SSL 웹 사이트에 대한 CRL(Certificate Revocation List)을 차단할 수 있다는 것이며, 이는 결국 일부 브라우저에서 오류를 생성합니다. 때때로 이러한 CRL을 차단하면 브라우저가 검증을 시도하는 동안 레이턴시가 발생합니다.

### 원인

CRL(Certificate Revocation List) 및 최신 OCSP(Online Certificate Status Protocol)는 어떤 이유로든 SSL 인증서가 폐기되었는지 인증 기관에 묻는 데 사용됩니다. 이는 일반적으로 HTTPS 웹 사이트에 연결할 때 백그라운드에서 투명하게 발생합니다.

인증서/CA가 손상된 경우 인증서가 폐기되면 브라우저는 사용자가 웹 사이트로 가는 것을 중지합니다. CRL에 대한 액세스를 허용하는 것이 좋습니다.

Allow-Only(허용 전용) 모드에서는 차단을 해제하지 않은 경우 대부분의 CRL이 차단됩니다. 이 기능의 영향은 사용 중인 웹 브라우저에 따라 달라집니다.

- Internet Explorer 7은 아래와 같은 오류와 함께 팝업 경고를 표시합니다. 이 사이트의 보안 인증서에 대한 해지 정보를 사용할 수 없습니다.
- 특정 레지스트리 키 플래그가 설정되지 않은 경우 이후 버전의 Internet Explorer에서는 오류가 표시되지 않습니다.
- Google Chrome은 주소 표시줄 옆에 경고를 표시합니다. 경고를 클릭하면 다음 오류가 표시됩니다. 인증서가 해지되었는지 확인할 수 없습니다.
- about:config에서 security.OCSP.require 설정을 설정하지 않으면 Firefox에서 오류가 표시되

지 않습니다

## 해결

1. 웹 브라우저에서 인증서를 보고 해당 인증서의 CRL을 찾습니다(단계는 브라우저에 따라 다름).
2. 'Details'(세부사항) 탭을 사용하여 다음 정보를 확인하십시오.
    - CRL 배포 지점
    - 권한 액세스 정보
3. URL 정보(아래 예)를 기록해 두고 Umbrella 대시보드의 allow(허용) 목록에 추가합니다.

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.