

AD 인증서 서비스를 사용하여 Umbrella 사용자 지정 루트 인증서 만들기

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[개요](#)

[인증서 문자열 인코딩](#)

[1단계: AD 인증서 서비스 템플릿 준비](#)

[2단계: 템플릿 발행](#)

[3단계: CSR 다운로드 및 서명](#)

[4단계: 서명된 CSR\(및 공용 루트 인증서\) 업로드](#)

소개

이 문서에서는 Microsoft Windows AD(Active Directory) 인증서 서비스를 사용하여 사용자 지정 루트 인증서를 만드는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 현재 Microsoft에서 지원하는 Microsoft Windows Server 버전
- Windows 서버에 설치된 Active Directory 인증서 서비스
- Active Directory 인증서 서비스 및 웹 서비스/웹 등록 서비스 역할이 있는 계정
- UTF-8 인코딩("UTF8STRING")으로 인증서를 발급하도록 구성된 인증서 서비스

사용되는 구성 요소

이 문서의 정보는 Cisco Umbrella를 기반으로 합니다.

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.

개요

이 문서에는 Microsoft Windows Active Directory 인증서 서비스를 사용하여 사용자 지정 루트 인증서(표준 [Cisco Umbrella Root CA](#) 인증서 대신 사용됨)를 생성한 다음 이 루트 인증서를 사용하여 Umbrella의 [고객 CA 서명 CA 인증서 기능](#)에서 CSR(Certificate Signing Request)에 서명하는 방법에 대한 지침이 포함되어 있습니다.

인증서 문자열 인코딩

인증서 서비스가 기본 인코딩("PRINTABLESTRING")을 사용하도록 구성된 경우 생성된 인증서 체인을 특정 웹 클라이언트, 특히 Firefox에서 신뢰할 수 없습니다.

Cisco Umbrella Secure Web Gateway 프록시는 UTF8STRING 인코딩으로 문자열을 인코딩하는 인증서 체인을 사용합니다. Cisco Umbrella Customers CA 중간 인증서를 생성하기 위해 CSR에 서명한 발급 인증서(예: 루트 인증서)가 PRINTABLESTRING으로 인코딩된 경우 Cisco Umbrella Customers CA 인증서의 Subject 필드는 PRINTABLESTRING입니다. 이 인코딩은 Cisco Umbrella R1 CA 중간 인증서의 Issuer 필드의 UTF8STRING 인코딩과 일치할 수 없습니다. 인증서 체인의 다음 필드입니다.

RFC 5280 섹션 4.1.2.6에서는 인증서 체인이 발급된 인증서의 Issuer 필드와 발급된 인증서의 Subject 필드 간에 동일한 문자열 인코딩을 유지해야 합니다.

"인증서의 주체가 CA인 경우 주체 필드는 주체 CA가 발급한 모든 인증서의 발급자 필드(섹션 4.1.2.4)에 인코딩되는 것과 동일한 방식으로 인코딩되어야 합니다."

많은 브라우저가 이 요구 사항을 적용하지 않지만 일부(특히 Firefox)는 이를 적용합니다. 그 결과 Firefox와 같은 웹 클라이언트는 신뢰할 수 없는 사이트 오류를 생성하고 고객 CA 서명 CA 인증서 기능이 있는 SWG(Secure Web Gateway)를 사용할 때 웹 사이트를 로드하지 않을 수 있습니다.

이 문제를 해결하려면 RFC 5280의 요구 사항을 적용하지 않는 Chrome과 같은 브라우저를 사용하십시오.

1단계: AD 인증서 서비스 템플릿 준비

1. 시작 > 실행 > MMC로 이동하여 Active Directory 인증 기관 MMC를 엽니다.
2. 파일 > 스냅인 추가/제거를 선택하고 인증서 템플릿 및 인증 기관 스냅인을 추가합니다. 확인을 선택합니다.
3. 인증서 템플릿을 확장하고 하위 인증 기관을 마우스 오른쪽 단추로 누릅니다. 중복 템플릿을 누릅니다.

이제 Umbrella 설명서에 나열된 요구 사항을 준수하기 위해 사용자 지정 인증서 템플릿을 생성할 수 있습니다.

이러한 요구 사항은 이 문서의 작성 시 자세히 설명 됩니다.

- General(일반) 탭
 - 템플릿에 의미가 있는 이름을 지정합니다.
 - 유효 기간을 35개월로 설정합니다(3년 한 달 미만).
 - 갱신 기간을 20일로 설정합니다.

- 확장 탭
 - Basic Constraints를 두 번 클릭합니다.
 - 이 내선을 중요시하도록 설정이 선택되었는지 확인합니다.
 - Key Usage(키 사용)에서:
 - Certificate Signing(인증서 서명) & CRL Signing(CRL 서명)이 선택되었는지 확인합니다.
 - 디지털 서명을 선택 취소합니다.
 - 이 내선 번호가 중요한지 확인합니다.
- Apply(적용) 및 OK(확인)를 선택합니다

2단계: 템플릿 발행

1. 이전 프로세스의 2단계에서 설정한 MMC로 돌아가서 Certificate Authority(인증 기관) 섹션을 확장합니다.
 2. 새로 확장된 섹션에서 Certificate Templates(인증서 템플릿) 폴더를 마우스 오른쪽 버튼으로 클릭하고 New(새로 만들기) > Certificate Template to Issue(발급할 인증서 템플릿)를 선택합니다.
 3. 신규 창에서 마지막 섹션에서 생성한 인증서 템플릿의 이름을 선택하고 확인을 선택합니다.
- 이제 CA가 요청을 지원할 준비가 되었습니다.

3단계: CSR 다운로드 및 서명

1. Umbrella 대시보드(<https://dashboard.umbrella.com>)에 로그인합니다.
2. Deployments(구축) > Configuration(구성) > Root Certificate(루트 인증서)로 이동합니다.
3. 모서리에 있는 추가(+) 아이콘을 선택하고 새 창에서 CA의 이름을 지정합니다.
4. CSR(Certificate Signing Request)을 다운로드합니다.
5. 새 브라우저 탭에서 Active Directory 인증서 서비스의 웹 서비스로 이동합니다. (로컬 시스템을 사용하는 경우 127.0.0.1/certsrv/ 또는 이와 비슷합니다.)
6. 신규 페이지에서 인증서 요청을 선택합니다.
7. 고급 인증서 요청을 선택합니다.
8. Saved Request(저장된 요청)에서 4단계에서 다운로드한 CSR의 내용을 복사하여 붙여넣습니다 (텍스트 편집기를 사용하여 열어야 함).
9. Certificate Template(인증서 템플릿) 아래에서 "Preparing AD Certificate Services Template(AD 인증서 서비스 템플릿 준비) 섹션"에서 생성한 인증서 템플릿의 이름을 선택하고 Submit(제출)을 선택합니다.
10. Base64 Encoded(Base64 인코딩)를 선택하고 Download Certificate(인증서 다운로드)를 선택한 다음 .cer 파일 위치를 기록해 둡니다.

4단계: 서명된 CSR(및 공용 루트 인증서) 업로드

1. Umbrella Dashboard에서 Deployment(구축) > Configuration(컨피그레이션) > Root Certificate(루트 인증서)로 이동합니다.
2. 이전 섹션의 단계 3에서 생성한 루트 인증서를 선택합니다.
3. 라인의 오른쪽 하단 모서리에 있는 CA 업로드*를 선택합니다.
4. 상위 찾아보기 버튼(Certificate Authority (Signed CSR))을 선택합니다.
5. 이전 섹션에서 생성한 .cer 파일의 위치로 이동하여 저장을 선택합니다.
6. 다음을 선택하고 (Cisco 루트 인증서 대신) 인증서를 사용할 컴퓨터/사용자 그룹을 선택한 후 저장을 선택합니다.

*선택적으로 CA 인증서를 업로드할 수도 있습니다. 인증 기관 서버의 웹 인터페이스 (<http://127.0.0.1/certsrv/>)에서 검색한 다음 CA 인증서, 인증서 체인 또는 CRL 다운로드를 선택합니다. Base 64에서 "CA 인증서 다운로드"라는 화면 프롬프트를 완료합니다.

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.