Advanced Certificate Manager

Transport Layer Security(TLS)로 인증서 수명 관리 오버헤드를 줄이면서 애플리케이션을 보호하세요.

TLS를 통해 팀의 업무량을 줄이면서 웹 애플리케이션을 보호하세요

Advanced Certificate Manager로 인증서가 자동으로 관리되므로 복잡한 TLS 요건에 대응할 유연성이 생깁니다

TLS는 인터넷 개인정보 보호 및 데이터 보안의 중추로, 최종 사용자가 신용 카드 정보나 기타 중요한 데이터를 노출하지 않고 비공개로 인터넷을 탐색할 수 있도록 합니다. **Advanced Certificate Manager**는 다음과 같은 방식으로 조직에서 TLS로 웹 애플리케이션을 보호할 수 있도록 지원합니다.

- TLS 인증서 발급, 관리, 갱신을 Cloudflare에 위임. 자동 관리로 팀 생산성이 향상됩니다.
- 새로 생성한 모든 도메인에서 자동 암호화로 보안 상태를 강화하세요. 조직의 요구와 규제 요구에 맞게 사용자 지정이 가능합니다.

어떤 솔루션이 적합할까요?	
Universal SSL 인증서가 적합한 경우:	**고급 인증서 또는 사용자 지정 인증서가 적합한 경우:**
• 인증서 수명 주기 관리 오버헤드를 줄이려면 무료 SSL/TLS 솔루션이 필요함 • 하위 도메인이 한 수준뿐임 • 만능 솔루션이 필요함	• 모든 호스트 이름에 완전한 TLS 커버리지를 원함 • SSL/TLS 인증서의 호스트 이름에 대한 특정 요구 사항이 있는 조직 • 기본 설정인 90일보다 짧은 유효 기간을 선호함 • 선호하는 인증 기관이 있음 • 맞춤형 암호 제품군을 설정하고 싶음

인증서 관리 간소화

Cloudflare에서는 고객을 대신해 TLS 인증서를 자동으로 발급하고 갱신하여 오버헤드를 줄입니다.

TLS 배포 사용자 지정

인증서의 호스트 이름을 사용자 지정하고, 유효 기간을 조정하며, 자체 인증 기관(CA) 및 암호 제품군을 선택하고, 자체 인증서를 가져오는 등의 작업을 수행하세요.

규제 준수 보장

최신 암호화 기술로 업계, 규제기관, 조직의 규제 준수 요구 사항을 최신 상태로 유지합니다.

Advanced Certificate Manager의 주요 기능

Cloudflare에서는 사용자가 생성한 모든 새로운 도메인에 대해 인증서를 자동 발급합니다

조직이 성장함에 따라 새로운 호스트 이름과 새로운 제품 라인 또는 웹 사이트의 현지화된 버전과 같은 새로운 웹 자산이 필요하게 될 가능성이 아주 큽니다. 새 호스트 네임이 생성될 때마다 자동으로 발급되므로 새로 만든 도메인에 보안 또는 개인정보 보호 공백이 생기지 않습니다. 웹 사이트를 새로 시작하는 것은 어려운 일이므로, Cloudflare에서 TLS를 처리하도록 위임하세요.

두 수준 이상의 하위 도메인 암호화

고객이 웹 사이트에서 더 많은 하위 도메인을 생성하면 Cloudflare에서는 항상 고객을 대신해 인증서를 발급하고 유효 기간이 끝나면 이를 갱신합니다.

선호하는 인증 기관(CA)을 선택하세요

일부 조직에서는 특정 CA를 선택하여 작업하는 것을 선호할 수 있습니다. Advanced Certificate Manager를 사용하면 인증서를 발급할 CA를 선택할 수 있습니다. 현재 CA 목록을 참조하세요.

Cloudflare에서 개인 키를 관리하는 동안, 인증서 서명 요청(CSR)을 생성하여 Cloudflare에서 선택한 CA에서 사용자 지정 인증서를 발급받으면 됩니다. CSR과 연계된 개인 키는 Cloudflare에서 생성하며, Cloudflare 네트워크를 벗어나지 않습니다.

인증서 유효 기간 사용자 지정

인증서는 일반적으로 표준 유효 기간이 90일이지만, Advanced Certificate Manager를 사용하면 기간을 더 짧게 설정하여 보안을 더 강력하게 보장하고 유출 발생 시 피해 범위를 줄일 수 있습니다.

선호하는 TLS 버전의 요청만 수락

TLS 1.1 또는 1.2 등 이전 버전의 TLS는 TLS 1.3보다 연결 속도가 느리고 보안이 취약할 수 있습니다. 요청을 수락할 최소 TLS 버전을 설정하도록 선택할 수 있습니다. 예를 들어, TLS를 1.2 이상으로 설정하면 웹 사이트에서는 TLS 1.2 및 1.3을 사용하는 클라이언트로부터의 연결을 허용합니다.

TLS용 암호 제품군 제어

Advanced Certificate Manager를 사용하면 Cloudflare와 클라이언트(예: 방문자의 브라우저) 간의 연결을 제한하여 특정 암호 제품군의 연결만 허용할 수 있습니다.

업계의 특정 권장 사항을 따르거나, 약하거나 오래된 암호 제품군을 비활성화하거나, 규제 또는 조직 요구 사항을 준수하기 위해 이를 수행할 수 있습니다.

"Advanced Certificates Manager 덕분에 저희가 보유한 여러 도메인에 걸쳐 인증서를 관리하는 방식이 간소화되지만, 아울러 엄격한 보안 요건도 충족할 수 있습니다. 암호 제품군을 관리하고 우리 파라미터 내에서 자동 갱신되는 기능을 활용하여 사용 가능하고 안전한 환경이 만들어집니다."

Colin Henderson
OneTrust 엔지니어링 이사

OneTrust

