인증서 관리

대시보드에는 인증서를 가져오고, 보고, 삭제할 수 있는 인증서 섹션이 있습니다. 인증서 행을 클릭하면 인증서 편집기가 열립니다.

인증서 목록
인증서는 정렬 가능한 페이지 매김 표에 표시됩니다 . 목록에는 클라이언트 인증서와 인증 기관 (CA)이 모두 포함됩니다 .

필터

페이지 상단에서 칩 목록을 사용해 필터를 활성화할 수 있습니다. 일부 필터는 상호 배타적입니다 .

전체: 모든 인증서를 표시합니다 .
클라이언트 : 클라이언트 인증서만 표시합니다 .
인증 기관 (CA): CA 인증서만 표시합니다 .
검색: 인증서 이름 또는 가져온 파일 이름으로 검색할 수 있는 텍스트 필드 (레이블 이름 또는 파일 이름)를 표시합니다 .
사용자 없음: 사용자와 연결되지 않은 클라이언트 인증서를 표시합니다 .

표 열

이름
유형
만료
사용자 (클라이언트 인증서에 표시됨)
가져온 파일 이름
가져온 날짜

작업

인증서 열기: 행을 클릭하여 인증서 편집기를 엽니다.
인증서 삭제: 인증서가 사용자 /정책과 연결되어 있지 않고 기기에서 사용되지 않는 경우에만 사용할
수 있습니다. 라이선스가 만료된 경우 이 작업이 비활성화될 수도 있습니다.

다중 행 선택: 여러 인증서를 한 번에 삭제할 수 있도록 다중 행 선택을 활성화할 수 있습니다. 삭제 가능한 인증서만 선택할 수 있습니다.
새로 고침: 인증서 목록을 다시 불러옵니다 .

인증서 가져오기
인증서를 가져오려면 인증서 가져오기 를 클릭하고 하나 이상의 파일을 선택하십시오 . 지원되는 형식은 가져오기 버튼의 도구 설명에 표시됩니다 .

클라이언트

지원 형식: Base64로 인코딩된 PKCS#12(.p12 / .pfx).

클라이언트 인증서는 엔터프라이즈 네트워크에서 사용자 또는 기기를 식별합니다 . 클라이언트 인증서는 특정 사용자와 연결할 수 있습니다.

각 클라이언트 인증서는 선택적으로 특정 사용자에게 할당할 수 있습니다. 이를 통해 동일한 Wi‑Fi EAP 구성을 여러 기기에 배포할 수 있습니다. 정책의 네트워크 구성 섹션에서 사용자의 EAP 자격 증명 옵션을 사용하여 설정할 수 있습니다.

또는 사용자 페이지에서 사용자에게 인증서를 할당할 수 있습니다.

Apple 기기에서는 Apple 정책의 네트워킹 섹션에서 인증서가 설치되며, 여기에서 기기 사용자의 인증서 를 선택할 수도 있습니다. Apple 정책의 네트워킹 페이지를 참조하세요 .

인증 기관 (CA)
지원 형식: Base64로 인코딩된 X.509(.crt / .pem / .cer / .der).

CA 인증서는 인증 기관을 식별하고, CA에서 발급한 모든 인증서를 신뢰해야 한다고 기기에 알립니다. 대시보드는 가져온 X.509 인증서가 CA인지 검증합니다 .

인증서 편집기
인증서를 열면 편집기에 주요 필드와 읽기 전용 인증서 정보 패널이 표시됩니다 .

주요 필드

이름 (필수)
ID(읽기 전용)
유형 (읽기 전용)
만료 (읽기 전용)
가져온 날짜 (읽기 전용)
가져온 파일 이름 (읽기 전용)

사용자 연결 (클라이언트 인증서)
클라이언트 인증서의 경우 편집기에 사용자 필드가 표시됩니다 . 사용자가 할당된 경우 메뉴에서 사용자 열기, 사용자 변경 또는 사용자 연결 해제 를 선택할 수 있습니다. 사용자가 할당되지 않은 경우 사용자 작업 버튼을 사용하여 할당할 수 있습니다.

인증서 삭제

삭제 작업은 인증서가 현재 사용자와 연결되어 있거나 정책에서 사용되는 경우 비활성화됩니다 . 라이선스가 만료된 경우에도 비활성화될 수 있습니다.

Revision #62
Created 2025-12-17 09:34:13 UTC by Admin
Updated 2026-11-12 09:56:21 UTC by Admin