### 인증서 관리

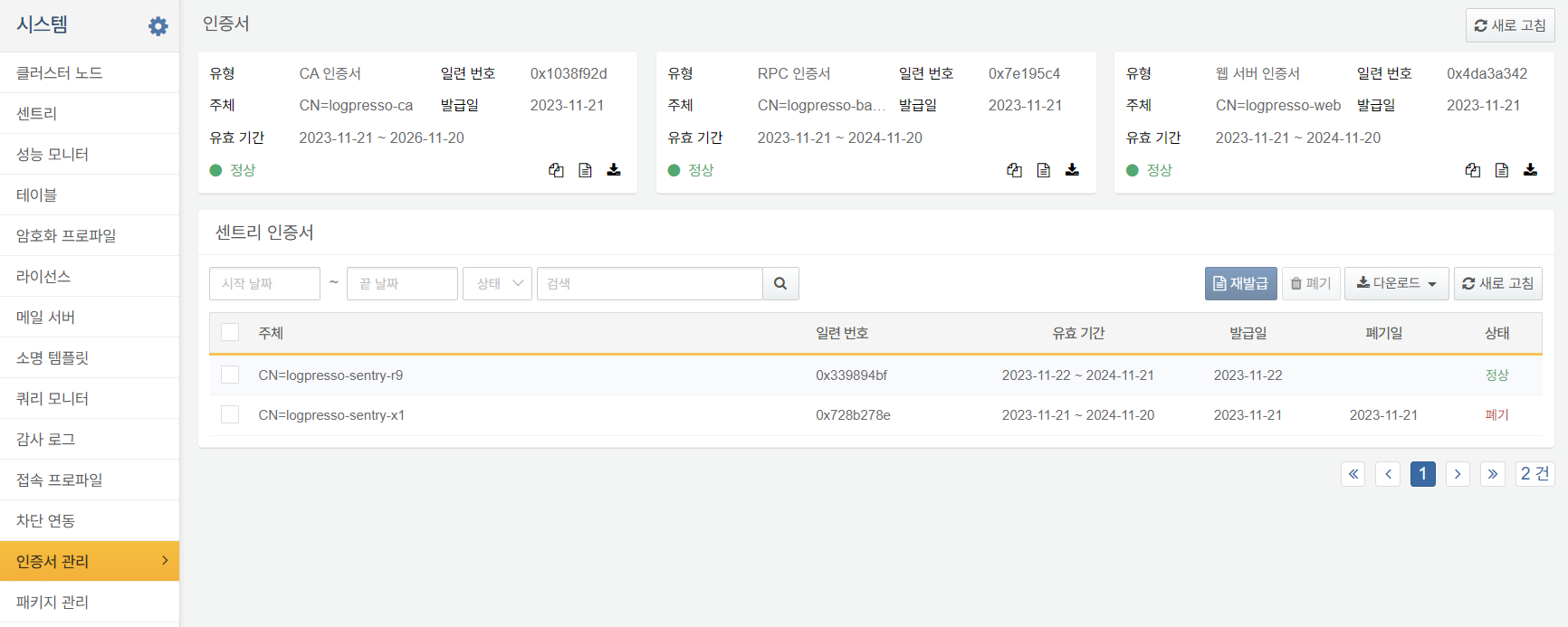
#### 개요

인증서는 현대 암호학과 네트워크 통신에서 통신 상대방의 신뢰성을 보증하거나, 암호화 통신용 키를 교환하는 수단으로 사용됩니다. 인증서의 신뢰성을 보증하는 주체를 CA(Certificate Authority)라 합니다. CA의 역할은 통화체계의 중앙은행과 같습니다. 한국은행이 원화(KRW)를 발행하고 통화량을 조절하듯이, CA는 인증서를 발급하고 신뢰할 수 있음을 보증하는 역할을 수행합니다.

로그프레소 서버의 인증서 체계는 자가 서명 CA(Self-signed Certificate Authority)로서 다음과 같은 인증서를 사용합니다.

* **CA 인증서** - 센트리, 사용자의 웹 브라우저와 공유하는 CA 공개키가 담긴 인증서. CA가 비밀키로 서명한 웹 서버 인증서, RPC 인증서, 센트리 인증서를 검증할 때 사용하는 최상위 인증서
* **웹 서버 인증서** - 로그프레소 서버와 사용자의 웹 브라우저 간 TLS 통신(TCP 443)에 사용
* **RPC 인증서** - 로그프레소 서버와 센트리의 RPC 통신(TCP 7140)에서 서버 인증서로 사용
* **센트리 인증서** - 로그프레소 서버와 센트리의 RPC 통신(TCP 7140)에서 클라이언트 인증서로 사용

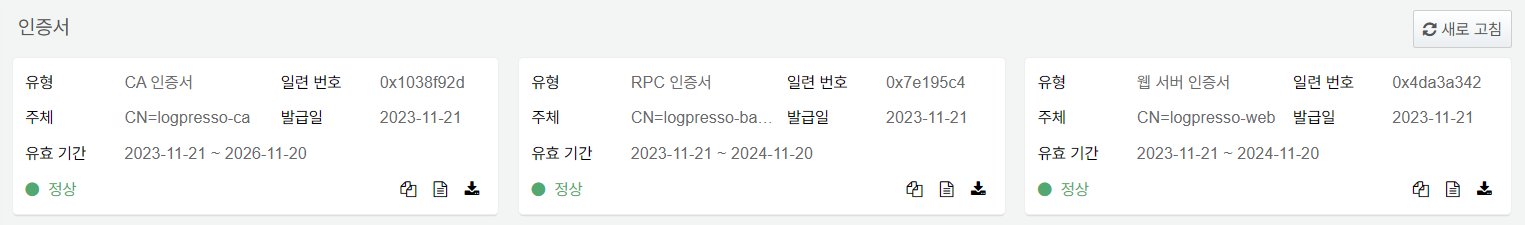
CA 인증서, 웹 서버 인증서, RPC 인증서는 로그프레소 서버를 설치하고 사용자가 처음으로 접속하면 웹 인스톨러가 실행되는 시점에 생성됩니다. 센트리 인증서는 [센트리를 추가](https://docs.logpresso.com/ko/sonar/4.0/ui/section-sentries)하는 시점에 발급됩니다. 이렇게 생성된 인증서는 **시스템 > 인증서 관리**에서 확인할 수 있습니다.



로그프레소 서버는 인증서의 배포에 TCP 44300을 이용합니다.

#### 서버 인증서

로그프레소 서버가 사용하는 인증서는 **CA 인증서**, **RPC 인증서**, **웹 서버 인증서**입니다. **시스템 > 인증서 관리**에서 각 서버 인증서 정보를 확인할 수 있습니다.



* **유형**: 인증서의 종류(CA 인증서, RPC 인증서, 웹 서버 인증서)
* **일련번호**: 인증서를 발행할 때 부여되는 16진수 고유 번호
* **인증서 주체**: 인증서를 사용하는 주체의 식별 정보(CN, Common Name)
* **발급일**: 인증서가 발급된 날짜
* **유효 기간**: 인증서를 사용할 수 있는 기간

각 인증서를 나타내는 카드의 좌하단은 인증서의 상태 정보를 보여줍니다. 인증서가 유효할 때 녹색으로 표시합니다. 인증서 카드의 우하단은 (왼쪽부터) 인증서 정보 복사, 재발급, 인증서 다운로드 버튼이 있습니다.

인증서 정보 복사

복사 아이콘을 클릭하면 인증서의 정보가 클립보드에 복사됩니다. 복사되는 정보로는 **유형**, **일련번호**, **주체**, **유효기간**(시작 시각, 만료 시각)이 있습니다.

재발급

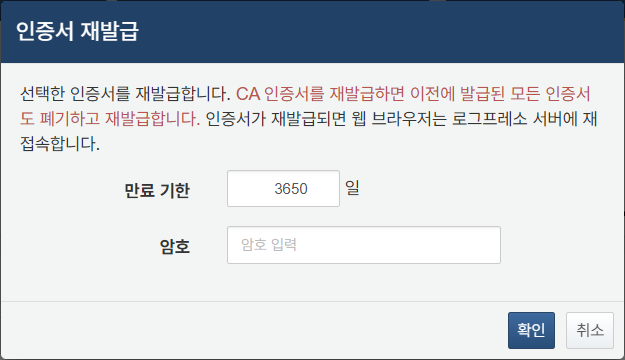
최초의 모든 서버 인증서는 웹 인스톨러 실행 시점에 생성됩니다. 서버 인증서는 센트리와 통신하거나 사용자 웹 브라우저와 서버가 통신할 때 사용되고, 유효 기간이 있습니다. 모든 서버 인증서는 유효 기간이 만료되기 전에 재발급되어야 합니다.

RPC 인증서나 웹 서버 인증서는 재발급 시점에 해당 통신에 사용되는 인증서만 교체됩니다. 그러나, **CA 인증서의 재발급은 모든 서버 인증서와 센트리 인증서의 재발급이 함께 이뤄집니다.**

서버 인증서를 재발급하려면,

재발급할 인증서 카드에서 **재발급** 아이콘을 클릭하세요.

**인증서 재발급** 대화상자에서 **만료 기한**과 인증서의 **암호**를 입력하고 **확인**을 클릭하세요.

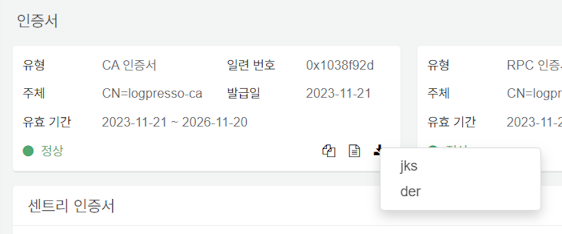


* CA 인증서의 만료 기한 기본값은 3650일(10년)입니다.
* 그 외 서버 인증서의 만료 기한 기본값은 365일(1년)입니다.

인증서를 재발급하면 해당 인증서를 사용하는 통신이 단절되고 새 인증서에 기반하여 재시작됩니다.

인증서 다운로드

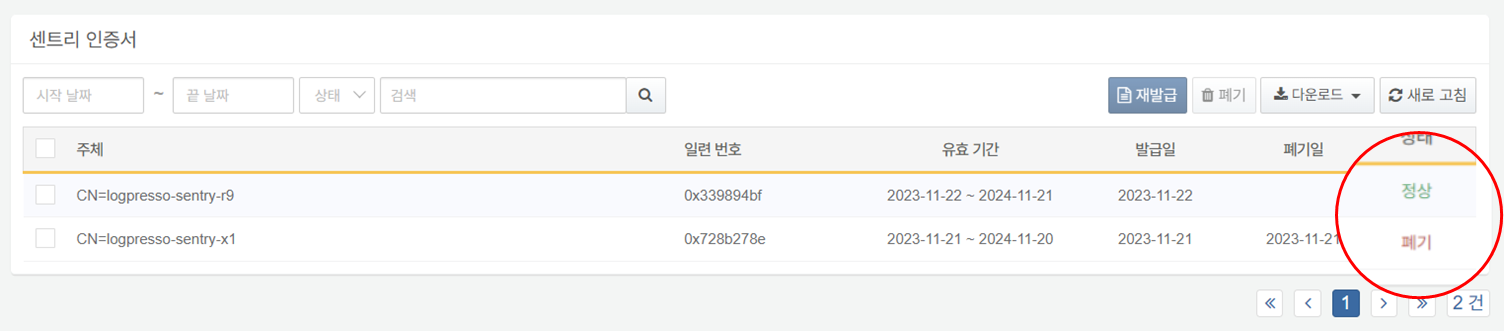
서버 인증서 카드에서 **다운로드** 아이콘을 클릭하면 인증서를 다운로드할 수 있습니다. 서버 인증서의 종류에 따라 파일 형식이 다릅니다. CA 인증서는 JKS 또는 DER 파일, 다른 서버 인증서들은 PFX 파일입니다.



JKS 파일은 자바 키스토어용 인증서 파일입니다. keytool을 이용해 자바 플랫폼의 키 스토어에 인증서를 저장할 수 있습니다. DER인 파일은 X.509 인증서와 개인 키를 DER(Distinguished Encoding Rules) 형식으로 인코딩한 파일입니다. DER 파일은 openssl과 같은 프로그램에서 사용할 수 있습니다.

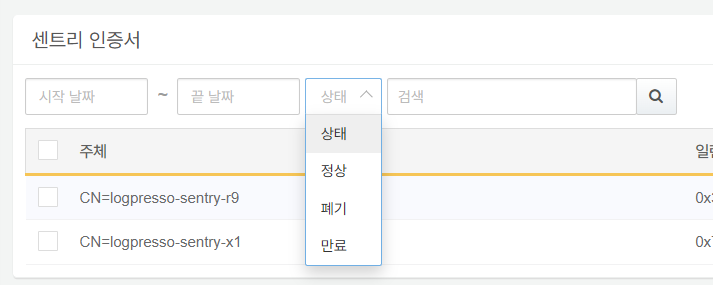
#### 센트리 인증서

로그프레소 서버와 센트리의 RPC 통신은 TLS 채널을 통해 이뤄집니다. 이 때 센트리가 사용할 인증서는 로그프레소 서버에 [센트리를 추가](https://docs.logpresso.com/ko/sonar/4.0/ui/section-sentries)하는 시점에 생성됩니다. 이렇게 생성된 센트리 인증서는 **시스템 > 인증서 관리**에 있는 **센트리 인증서 관리** 목록에서 조회할 수 있습니다. 이 목록은 발행된 인증서와 폐기된 인증서를 모두 보여줍니다.



검색

**센트리 인증서 관리** 도구 모음에서 센트리 인증서를 검색할 수 있습니다.



* **시작 날짜**, **끝 날짜**: 지정된 범위 내에서 만료되는 인증서를 검색합니다.
* **상태**: 인증서의 상태(**정상**, **폐기**, **만료**)
* **검색**: 인증서 주체에서 검색할 키워드

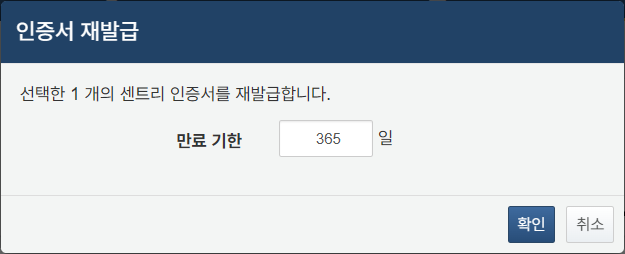
재발급

발급된 인증서를 재발급하려면,

센트리 인증서 관리 목록에서 재발급할 인증서의 체크 박스를 체크하세요.

도구 모음에서 **재발급**을 클릭하세요.

**인증서 재발급** 대화상자에서 **만료 기한**을 입력하세요. 기본값은 365일입니다.



인증서를 재발급하려면 **확인**을, 재발급을 중지하려면 **취소**를 클릭하세요.

* **확인**을 클릭하면 새로 발행된 인증서를 센트리로 전송하고, 기존 인증서는 폐기합니다.
* 새 인증서를 받은 센트리는 재구동됩니다.

**시스템 > 센트리**에서 센트리의 연결 상태를 확인하세요.

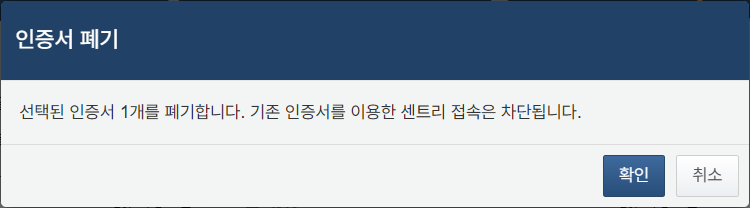
폐기

센트리의 인증서를 사용자가 직접 폐기하려면,

센트리 인증서 관리 목록에서 폐기할 인증서의 체크 박스를 체크하세요.

도구 모음에서 **폐기**를 클릭하세요.

**인증서 폐기** 대화상자가 나타납니다. 폐기를 진행하려면 **확인**을, 폐기를 중지하려면 **취소**를 클릭하세요.



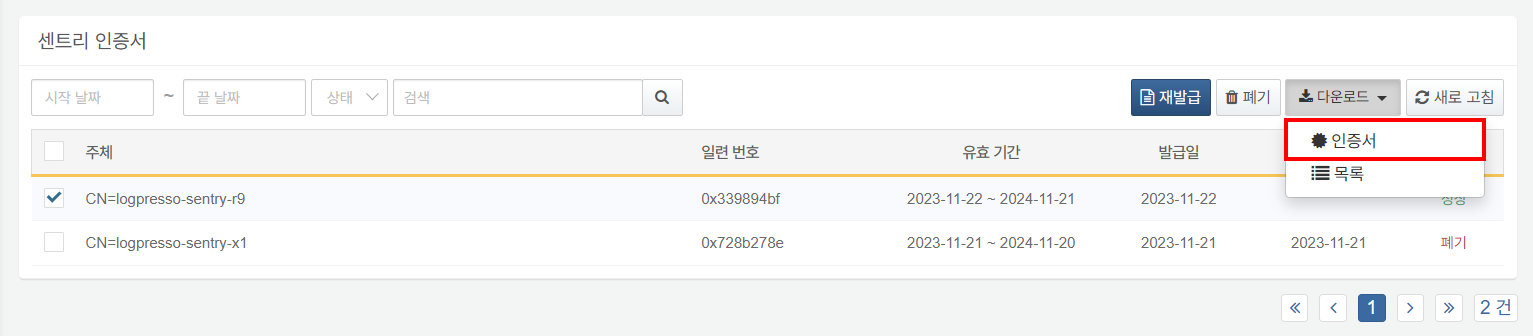
**시스템 > 센트리**에서 센트리의 연결이 해제되었는지 확인하세요. 필요하다면 센트리 목록에서 [센트리를 삭제](https://docs.logpresso.com/ko/sonar/4.0/ui/section-sentries)하세요.

인증서 다운로드

센트리 인증서를 다운로드하려면,

센트리 인증서 관리 목록에서 다운로드할 인증서의 체크 박스를 체크하세요. 목록 최상단에 있는 체크 박스를 체크하면 현재 조회 중인 페이지의 모든 인증서가 선택됩니다.

도구 모음에서 **다운로드 > 인증서**를 클릭하세요.

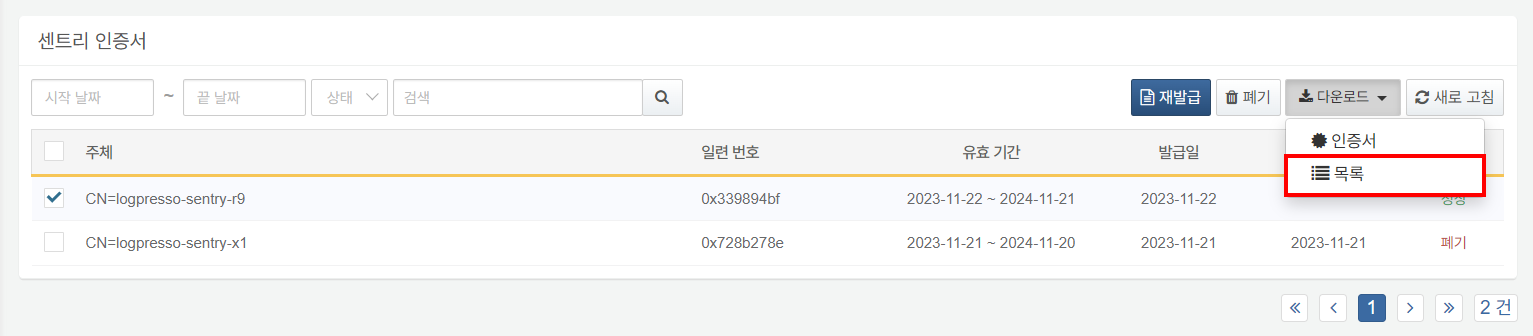


* 사용자에게 전송되는 파일은 센트리 인증서 PFX 파일을 묶은 ZIP 파일입니다.
* 하나의 센트리 인증서만 선택해도 ZIP 파일로 전송됩니다.

인증서 목록 다운로드

센트리 인증서 관리 목록을 다운로드하려면,

도구 모음에서 **다운로드 > 목록**을 클릭하세요.



**센트리 인증서 목록 다운로드** 대화 상자에서 **파일 이름**, **컬럼**, **파일 형식**, **인코딩**, **범위**를 지정하고 **확인**을 클릭하세요.

