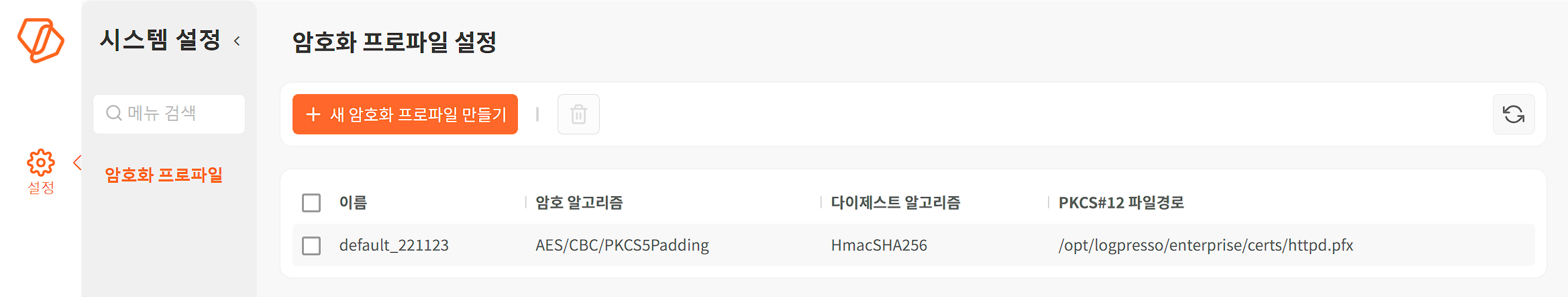
### 암호화 프로파일

#### 개요

로그프레소는 데이터 원본을 실시간 압축하는 동시에 암호화 및 다이제스트 생성을 통하여 기밀성과 무결성을 보장합니다. 데이터 암호화를 설정하려면 먼저 암호화 프로파일을 만든 후, 테이블 생성 시 crypto 옵션으로 암호화 프로파일을 지정합니다.

로그프레소는 PKCS#12 인증서 파일(일반적으로 확장자가 .pfx인 파일)에서 인증서와 키를 읽어들여 사용합니다. 일자별 데이터 원본 파일(확장자는 .dat)을 생성할 때 일자별 암호키 파일 (확장자는 .key)을 생성합니다. 암호키 파일에는 해당 일자의 데이터 원본 파일을 암호화/HMAC 다이제스트 하는데 사용한 키, 암호 알고리즘, 다이제스트 알고리즘에 대한 정보가 포함됩니다. 암호키 파일은 PKCS#12 공개키를 사용하여 암호화되고 비밀키를 사용하여 복호화되므로, 사용자가 설정한 PKCS#12 인증서 파일이 없으면 로그 원본 데이터 파일이 유출되더라도 임의로 내용을 읽을 수 없습니다.

**설정 > 암호화 프로파일**에서 암호화 프로파일을 관리할 수 있습니다.

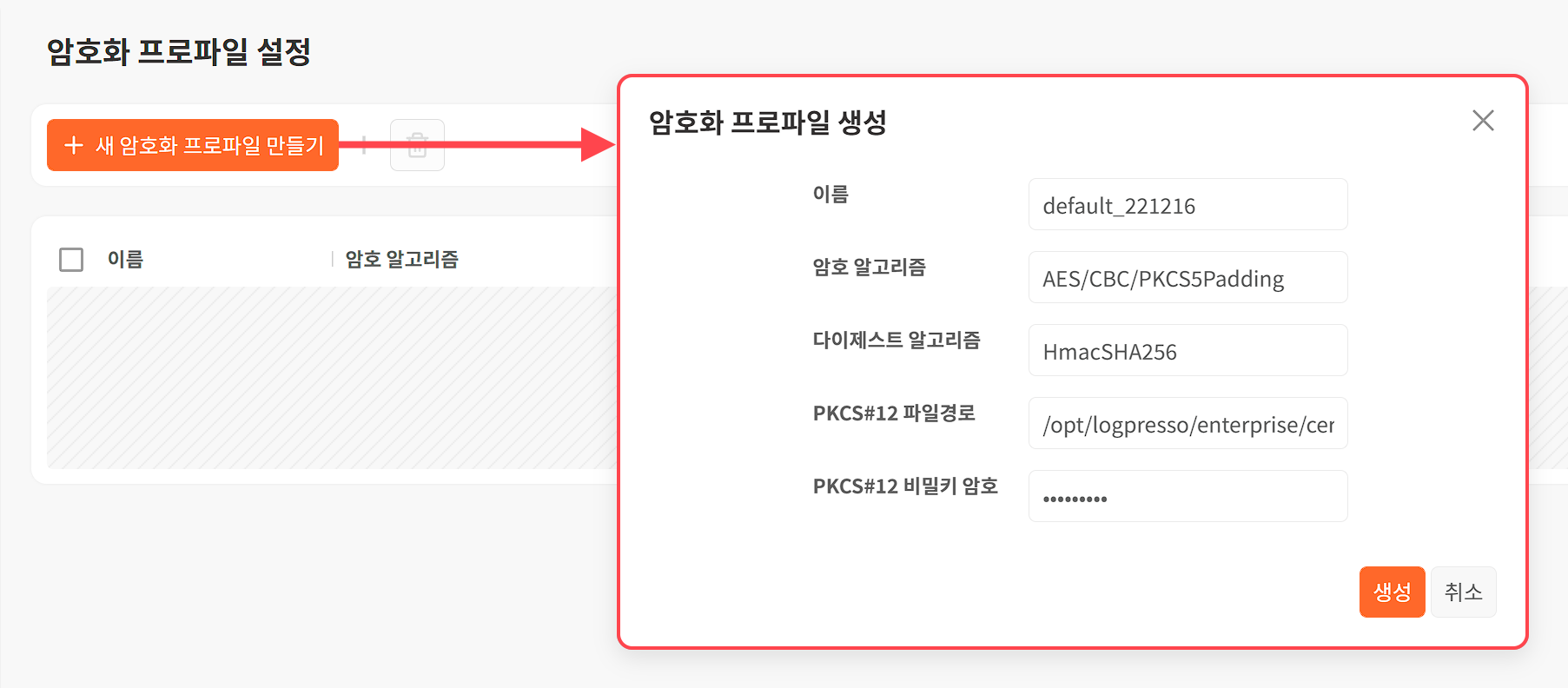


암호화/무결성 프로파일 목록에서 다음과 같은 정보를 확인할 수 있습니다.

* **이름**: 암호화 프로파일의 이름
* **암호 알고리즘**: 암호화 프로파일에 설정된 암호화 알고리즘 슈트
* **다이제스트알고리즘**: 암호화 프로파일에 설정된 무결성 알고리즘 슈트
* **PKCS#12 파일경로**: PKCS#12 인증서 파일의 경로

#### 암호화 프로파일 추가

암호화 프로파일을 추가하는 방법은 다음과 같습니다.



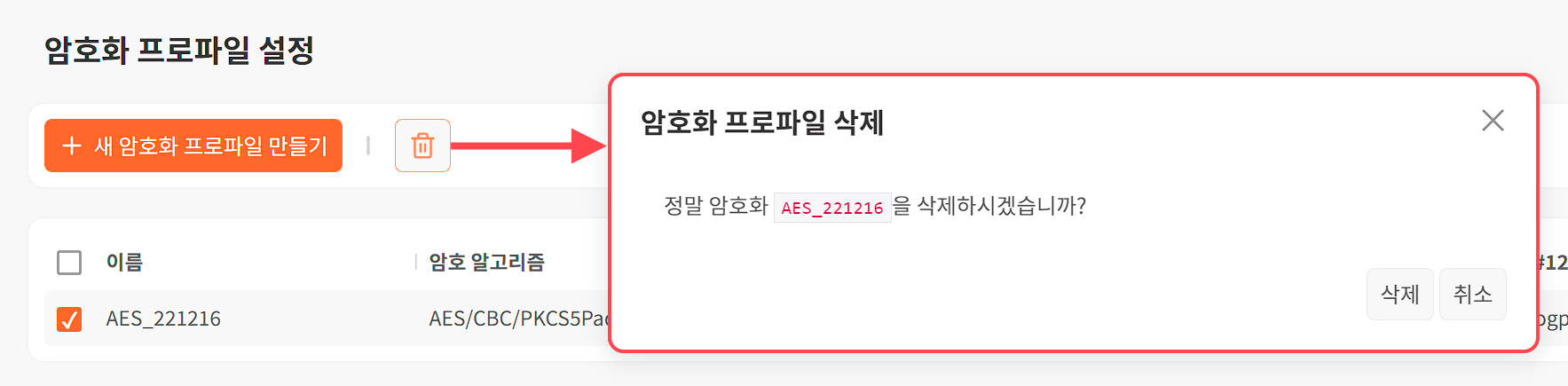
**설정 > 암호화 프로파일**에 있는 도구 모음에서 **+ 새 암호화 프로파일 만들기**를 누릅니다.

암호화 프로파일 구성에 필요한 정보를 입력하고 **생성**을 누릅니다.

* **이름**: 프로파일을 식별하는데 사용할 이름
* **암호 알고리즘**: 암호 알고리즘 방식을 입력(기본값: AES/CBC/PKCS5Padding)
* **다이제스트 알고리즘**: 요약 알고리즘을 입력(기본값: HmacSHA256)
* **PKCS#12 파일경로**: PKCS#12 파일의 경로
* **PKCS#12 비밀키 암호**: PKCS#12 파일의 비밀키 암호

#### 암호화 프로파일 삭제

암호화 프로파일을 삭제하는 방법은 다음과 같습니다.



**설정 > 암호화 프로파일**에서 삭제할 암호화 프로파일을 선택한 다음 도구 모듬에서 휴지통을 누릅니다.

**암호화 프로파일 삭제** 창에서 삭제할 암호화 프로파일을 확인한 다음 **삭제**를 누릅니다.