### 암호화/무결성 프로파일

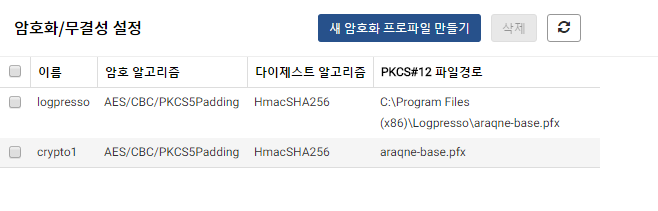
로그프레소는 데이터 원본을 실시간 압축하는 동시에 암호화 및 다이제스트 생성을 통하여 기밀성과 무결성을 보장합니다. 데이터 암호화를 설정하려면 먼저 암호화 프로파일을 만든 후, 테이블 생성 시 crypto 옵션으로 암호화 프로파일을 지정합니다.

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

메뉴는 "시스템 설정" "암호화/무결성 프로파일" 메뉴를 선택하여 사용합니다.

암호화/무결성 프로파일 메뉴는 아래의 항목으로 확인 및 관리됩니다.

* 선택메뉴: 삭제기능을 사용할 경우 선택 기능
* 이름: 프로파일을 이름을 표시.
* 암호알고리즘: 이름 표시
* 다이제스트알고리즘: 이름 표시
* PKCS#12 파일경로: 인증서 경로 표시



#### 암호화 프로파일 생성

유효기간이 만료된 PKCS#12 파일이라도 데이터 암호화 하는데 문제 없이 사용할 수 있습니다. PKCS#12 비밀키를 읽어들이는데 필요한 암호를 입력하고, 이어서 암호 알고리즘과 다이제스트 알고리즘을 입력합니다. 암호알고리즘을 입력하지 않으면 데이터 암호화 없이 다이제스트만 생성하게 됩니다.

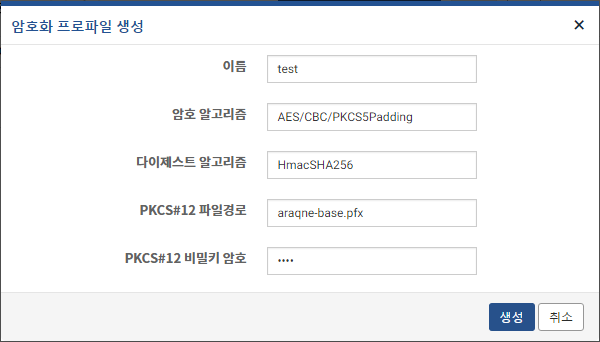
단계 1

새로운 암호화/무결성 프로파일을 생성하기 위하여 새 암호화 프로파일 만들기 메뉴를 선택합니다.



단계 2

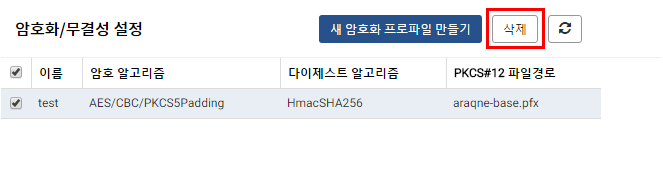
* 설정에 필요한 입력값을 입력한 후 생성 메뉴를 선택합니다.
* 이름: 프로파일을 식별하는데 사용할 유일한 이름을 부여합니다.
* 암호알고리즘: 암호 알고리즘 방식을 입력합니다. 기본값은 AES/CBC/PKCS5Padding 입니다.
* 다이제스트 알고리즘: 요약 알고리즘을 입력합니다. 기본값은 HmacSHA256 입니다.
* PKCS#12 파일경로: 인증서 경로를 입력합니다.
* PKCS#12 비밀키 암호: 인증서 암호를 입력합니다.



#### 암호화 프로파일 삭제

단계 1

암호화/무결성 프로파일 설정 화면에서 등록된 프로파일 이름 중에서 삭제하고자 하는 이름을 선택한 후 삭제 버튼을 클릭합니다.



단계 2

삭제 버튼을 클릭하여 삭제를 완료합니다.