범용

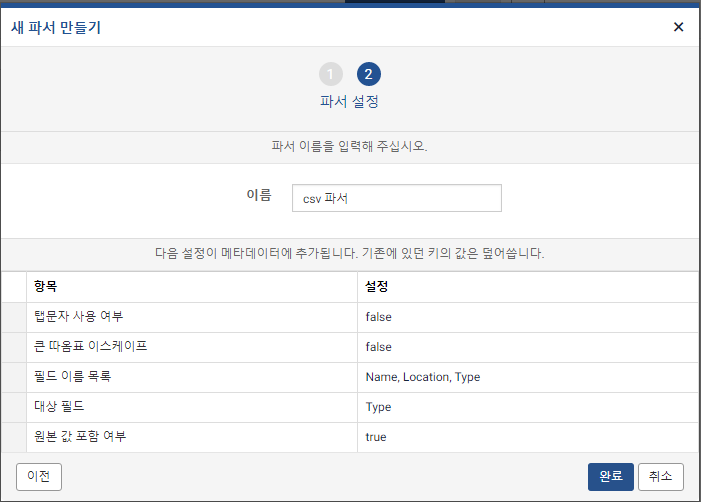
**CEF 파서**

CEF (Common Event Format) 형식의 로그를 파싱합니다. 아크사이트 등 ESM이나 SIEM 시스템과 연동에 사용되는 규격으로 별도로 설정할 매개변수 항목은 없습니다.

**CSV 파서**

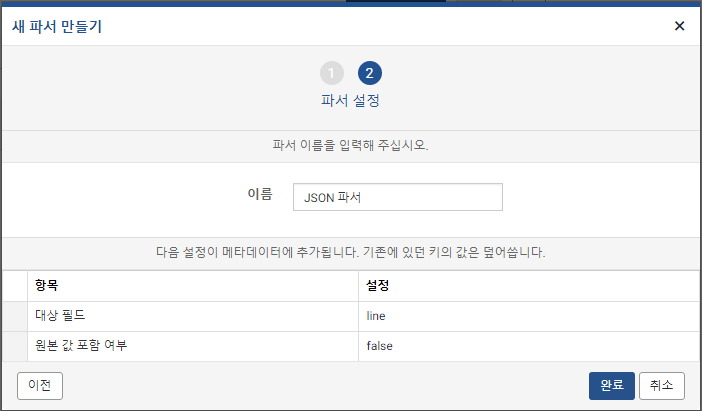
CSV 형식으로 구분된 각 토큰에 대하여 설정된 필드 이름들을 순서대로 적용하여 파싱합니다.

* 탭문자 사용 여부: 구분자로 탭문자를 사용할 지 결정합니다. true 혹은 false를 입력합니다.
* 큰 따옴표 사용 여부: 특수문자를 구분하기 위한 이스케이프 문자를 큰 따옴표로 사용합니다. true 혹은 false를 입력합니다.
* 필드 이름 목록: 파싱된 결과 필들드 이름들을 입력합니다.
* 대상 필드: 파싱할 대상 필드 이름을 입력합니다.
* 원본 값 포함 여부: CSV로 파싱된 결과 외에 원본 필드 값도 포함할 지 여부를 설정합니다. true 혹은 false를 입력합니다.



**JSON 파서**

JSON 형식의 문자열을 파싱합니다.



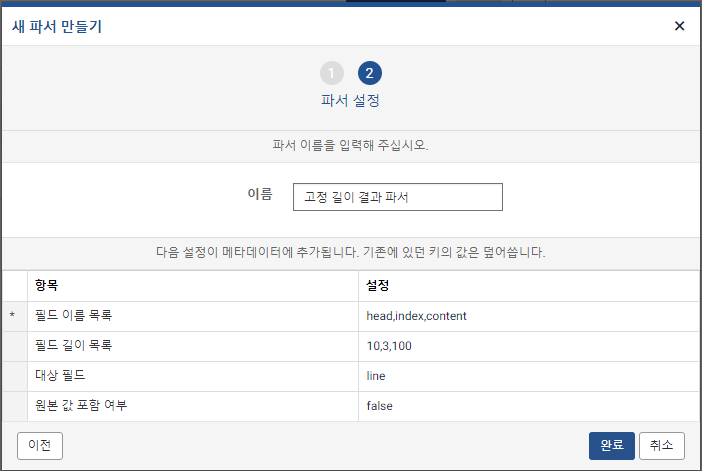
**WELF 포맷 파서**

WELF 파서는 WELF (WebTrends Enhanced Log Format) 형식의 데이터를 파싱합니다. 별도의 설정 매개변수는 없으며 키/값 쌍의 나열을 파싱할 수 있습니다.

**고정 길이 필드 파서**

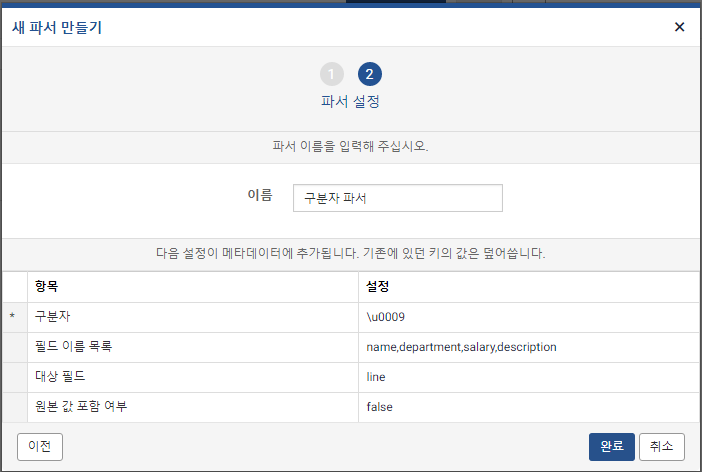
설정된 필드 이름들에 대하여 입력한 고정길이로 로그를 파싱합니다.

* 필드 이름 목록: 쉼표로 구분 된 필드 이름 목록을 입력합니다.
* 필드 길이 목록: 필드 별 길이를 입력합니다.
* 대상 필드: 파싱할 대상 필드 이름을 입력합니다.
* 원본 값 포함 여부: 구분자로 파싱된 결과 외에 원본 필드 값도 포함할 지 여부를 설정합니다. true 혹은 false를 입력합니다.



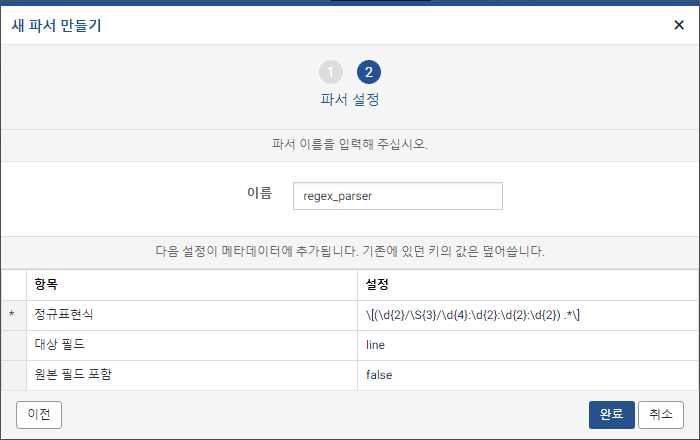
**구분자 파서**

* 구분자로 구분된 각 토큰에 대하여 설정된 필드 이름들을 순서대로 적용하여 파싱합니다.
* 구분자: 하나의 아스키 구분자 혹은 4자리 유니코드 이스케이프 시퀀스를 입력합니다. (예: 0x0d)
* 필드 이름 목록: 쉼표로 구분 된 필드 이름 목록을 입력합니다.
* 대상 필드: 구분자로 파싱할 대상 필드 이름을 입력합니다.
* 원본 값 포함 여부: 구분자로 파싱된 결과 외에 원본 필드 값도 포함할 지 여부를 설정합니다. true 혹은 false를 입력합니다.



**정규표현식 파서**

* 정규표현식을 이용하여 로그를 파싱합니다.
* 정규 표현식: 파서로 사용할 정규 표현식을 입력합니다.
* 대상필드: 파서를 적용할 필드명을 입력합니다.
* 원본필드포함: 원본필드를 표현할지 true, false로 입력합니다.



**쿼리 기반 파서**

쿼리를 이용하여 파싱을 수행합니다. 쿼리 문법을 그대로 사용할 수 있으므로 다른 파서에 비해 상대적으로 복잡하고 정교한 파싱을 수행할 수 있습니다.

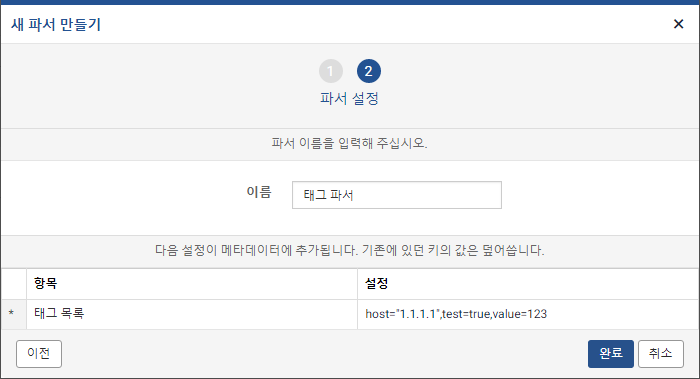
* 쿼리: 로그 파싱에 사용할 쿼리문을 입력합니다. 쿼리 문자열, 입력 로그와 쿼리 결과가 일대일로 매핑되는 쿼리 커맨드를 파이프로 연결한 쿼리를 설정할 수 있습니다.



**태그 파서**

지정된 태그를 추가하여 파싱합니다.

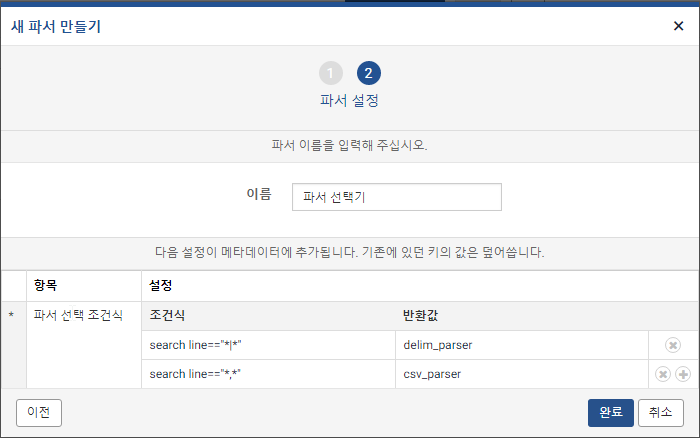
* 태그 목록: 쉼표로 구분된 키=값 형태의 태그 목록



**파서 선택기**

표현식 조건과 일치하는 첫번째 파서를 선택하여 파싱을 수행합니다.

* 조건: 파서를 선택할 조건 쿼리를 입력합니다. 여러 조건을 만족할 경우 가장 첫 번째 조건에 해당하는 파서를 선택합니다.
* 반환값: 조건을 만족할 경우 사용할 파서 값을 입력합니다.
* 여러 조건을 입력할 경우 + 버튼을 클릭하여 새 조건을 생성합니다.



**파서 체인**

여러개 파서를 조합하여 만든 체인을 이용하여 파싱합니다.

* 파서 이름 목록: 쉼표로 구분된 파서 이름 목록을 입력합니다. 입력한 순서대로 파서가 동작합니다.



**필드 이름 변경 파서**

필드 이름을 변경합니다.

* 필드 이름 변환 목록: 쉼표로 구분되는 원본필드=변경필드 형식의 이름 목록을 입력합니다.

