#### 범용 파서

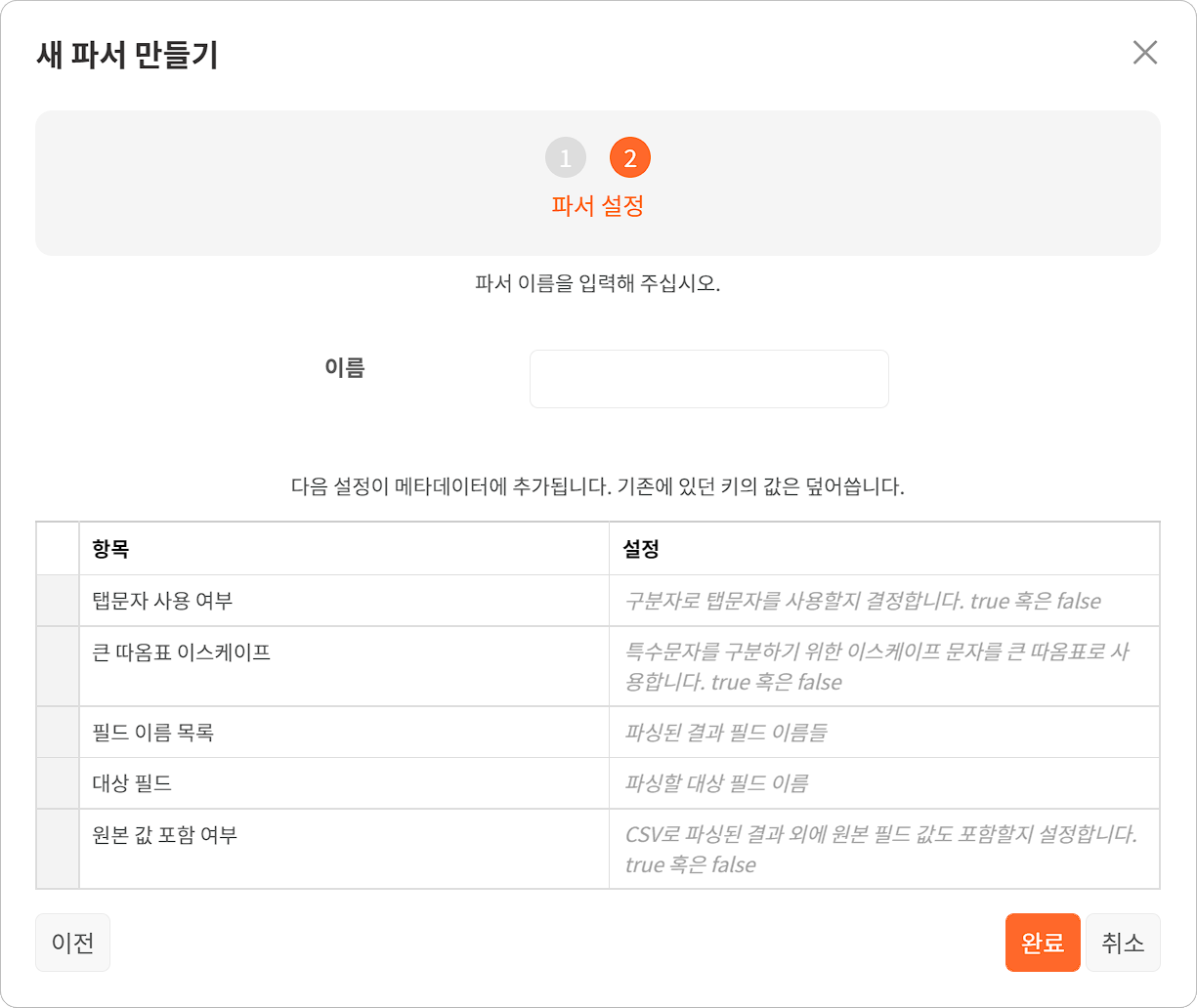
범용 파서는 텍스트 기반 데이터 파일을 다루는 파서들입니다. 여기서는 범용 파서들의 속성을 설명합니다.

CEF 파서

CEF 파서는 CEF(Common Event Format) 형식의 로그를 파싱합니다. ArcSight와 같은 ESM이나 SIEM 시스템과 연동에 사용되는 규격으로, 별도로 설정할 항목이 없습니다.

CSV 파서

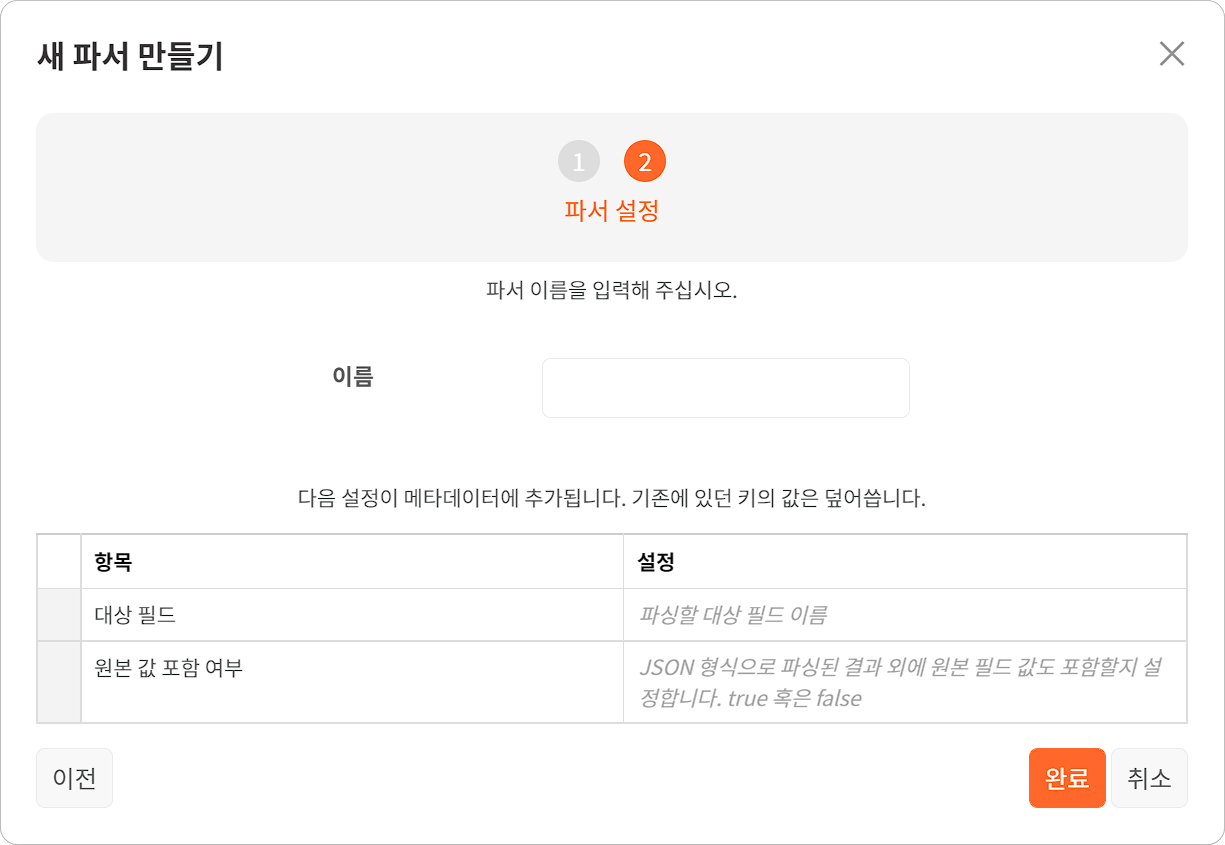
CSV 파서는 CSV(Comma-Separated Values) 또는 TSV(Tab-Separated Values) 형식으로 구분된 각 토큰에 대하여 설정된 필드 이름들을 순서대로 적용하여 파싱합니다.



* **탭문자 사용 여부**: 구분자로 탭 문자의 사용를 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 필드의 이름들 쉼표(,)로 구분해서 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 파서는 JSON 형식의 문자열을 파싱합니다.



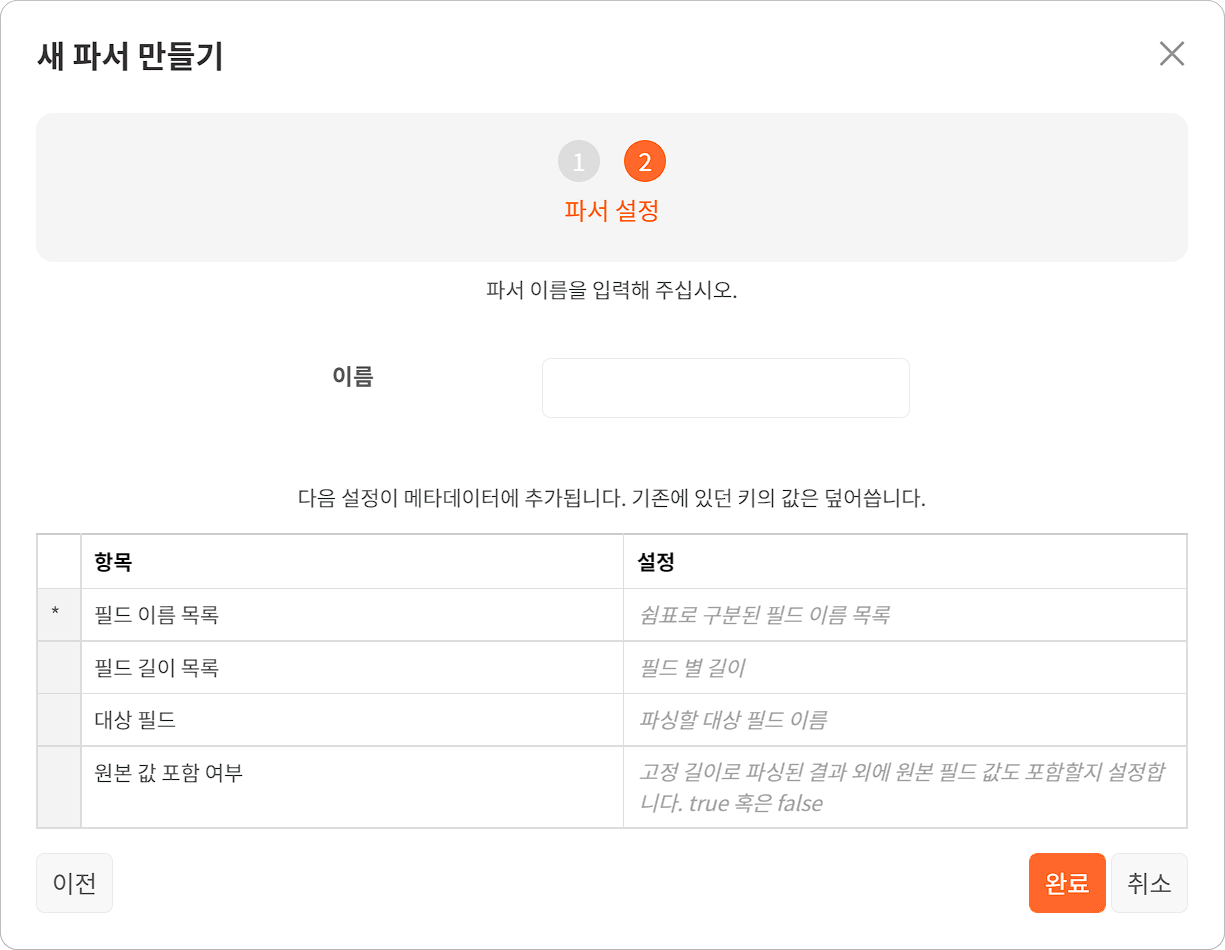
* **대상 필드**: 파싱할 대상 필드 이름을 입력합니다.
* **원본 값 포함 여부**: JSON으로 파싱된 결과 외에 원본 필드 값도 포함할 지 여부를 설정합니다. true 혹은 false를 입력합니다.

WELF 파서

WELF 파서는 WELF(WebTrends Enhanced Log Format) 형식의 데이터를 파싱합니다. WELF 파서는 별도로 설정할 항목이 없습니다.

고정 길이 필드 파서

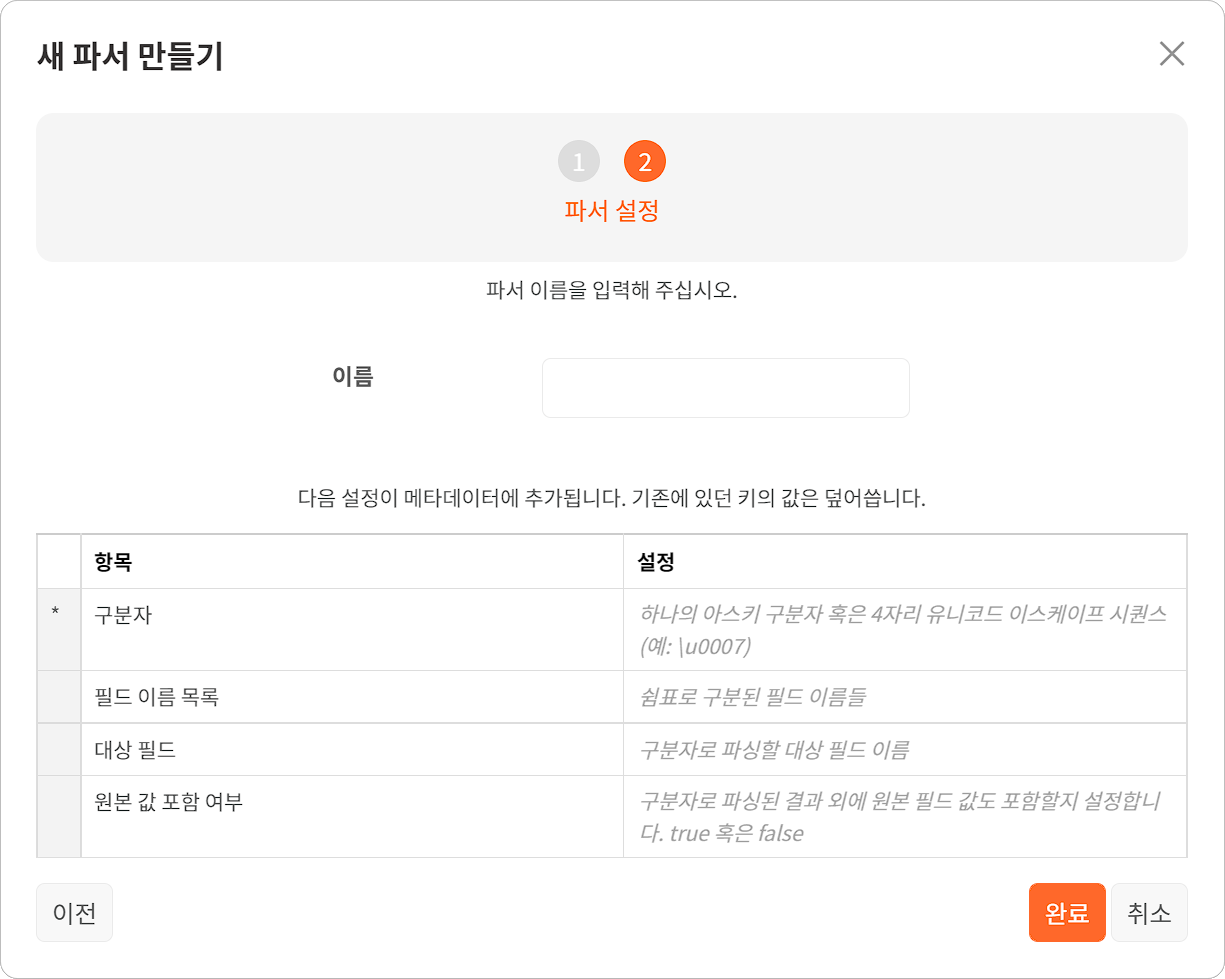
고정 길이 필드 파서는 입력되는 문자열을 고정된 길이 단위로 잘라서 필드에 순서대로 할당하여 파싱합니다.



* **필드 이름 목록**: 필드 이름 목록을 쉼표(,)로 구분해서 입력합니다.
* **필드 길이 목록**: 필드별 길이를 쉼표(,)로 구분해서 파싱할 순서대로 입력합니다.
* **대상 필드**: 파싱할 대상 필드 이름을 입력합니다.
* **원본 값 포함 여부**: 파싱된 결과 외에 원본 필드 값도 출력에 포함할 지 여부를 설정합니다. true 혹은 false를 입력합니다.

구분자 파서

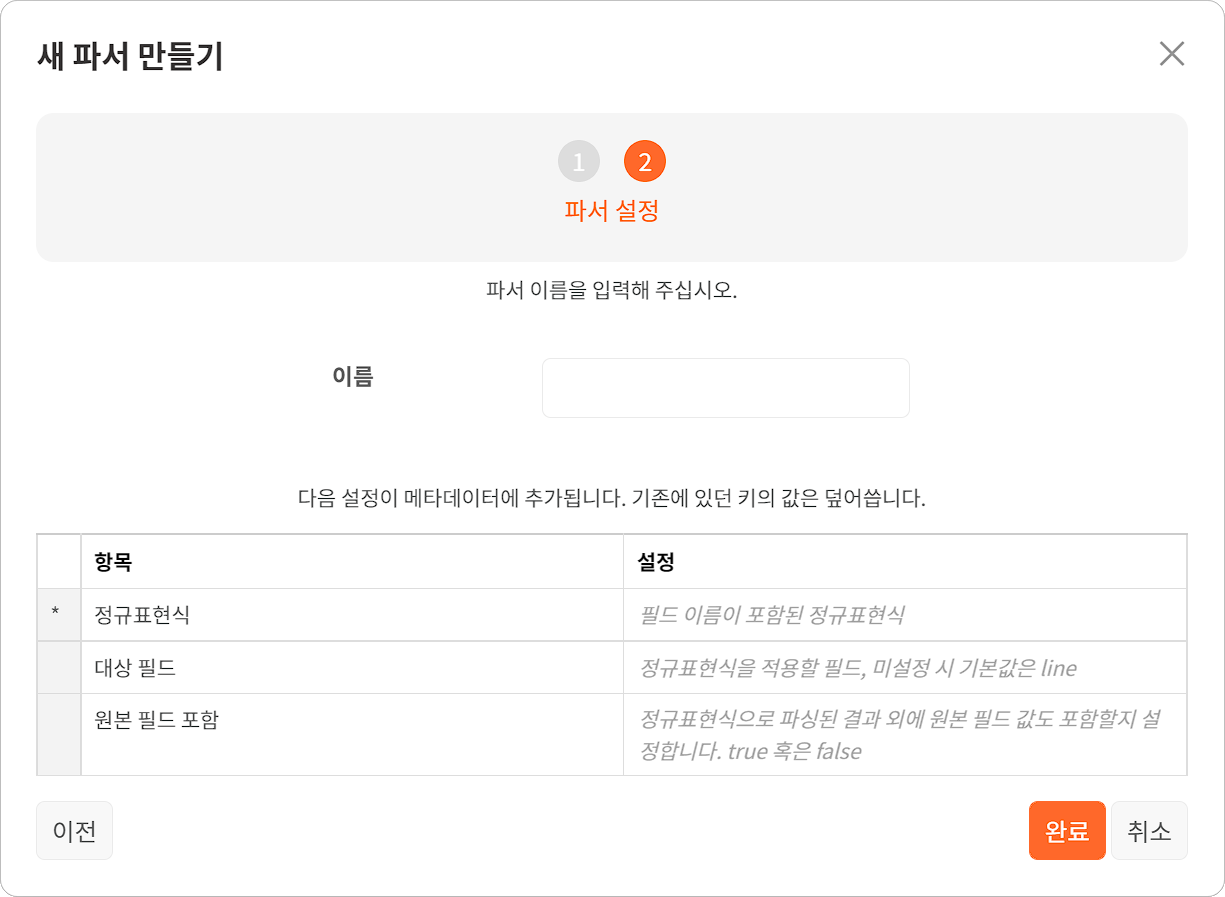
구분자 파서는 구분자로 식별되는 각 토큰을 필드에 순서대로 할당하여 파싱합니다.



* **구분자**: 하나의 16진수 ASCII 코드(예: 0x0d) 또는 4자리 유니코드 이스케이프 시퀀스(예: \u0007)를 입력합니다. 유니코드 이스케이프 시퀀스는 [UnicodePlus](https://unicodeplus.com)에서 검색할 수 있습니다.
* **필드 이름 목록**: 필드 이름 목록을 쉼표(,)로 구분해서 파싱할 순서대로 입력합니다.
* **대상 필드**: 구분자로 파싱할 대상 필드 이름을 입력합니다.
* **원본 값 포함 여부**: 파싱된 결과 외에 원본 필드 값도 출력에 포함할 지 여부를 설정합니다. true 혹은 false를 입력합니다.

정규표현식 파서

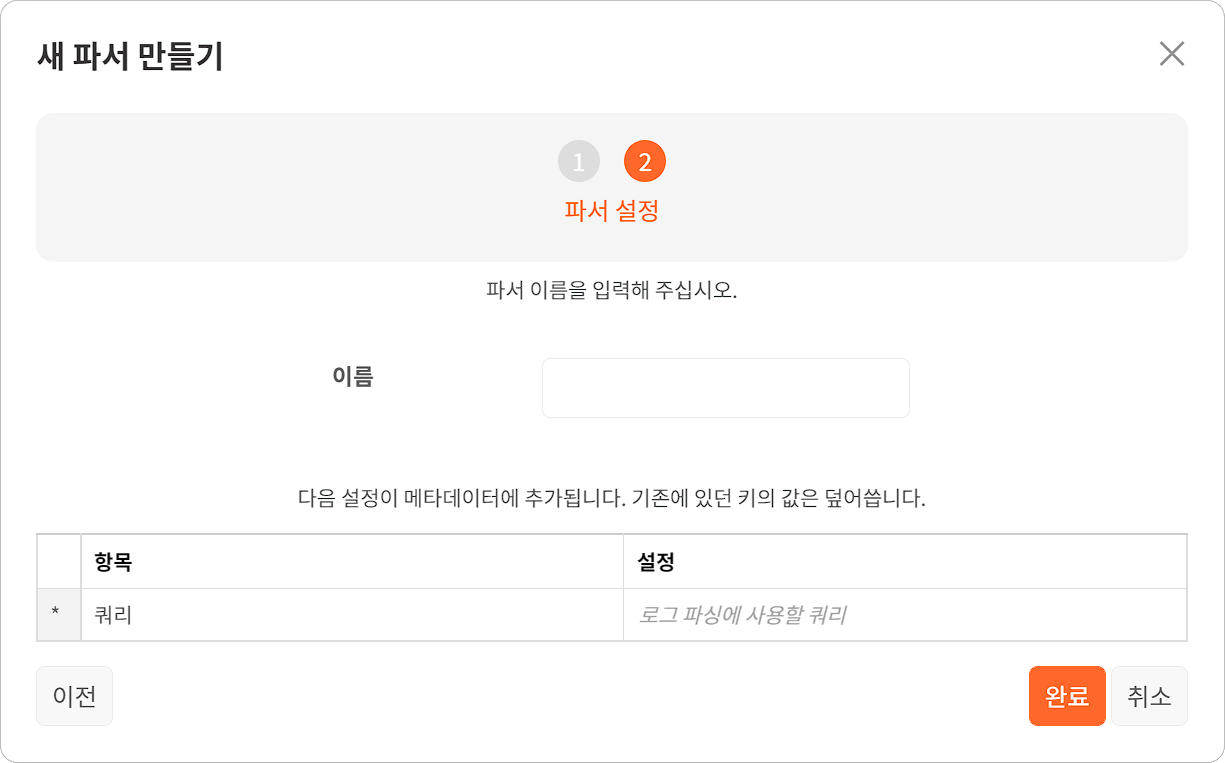
정규표현식을 이용하여 로그를 파싱합니다.



* **정규표현식**: 필드값 추출에 적용할 정규표현식을 입력합니다. 정규표현식과 일치하는 문자열을 필드에 할당할 수 있도록 필드 이름을 정규표현식 안에 그룹 이름 형식으로 포함해야 합니다(예: (?<date>\d{4}-\d{2}-\d{2})).
* **대상 필드**: 정규표현식과 대조할 필드명을 입력합니다.
* **원본 필드 포함**: 원본필드를 표현할지 true, false로 입력합니다.

쿼리 기반 파서

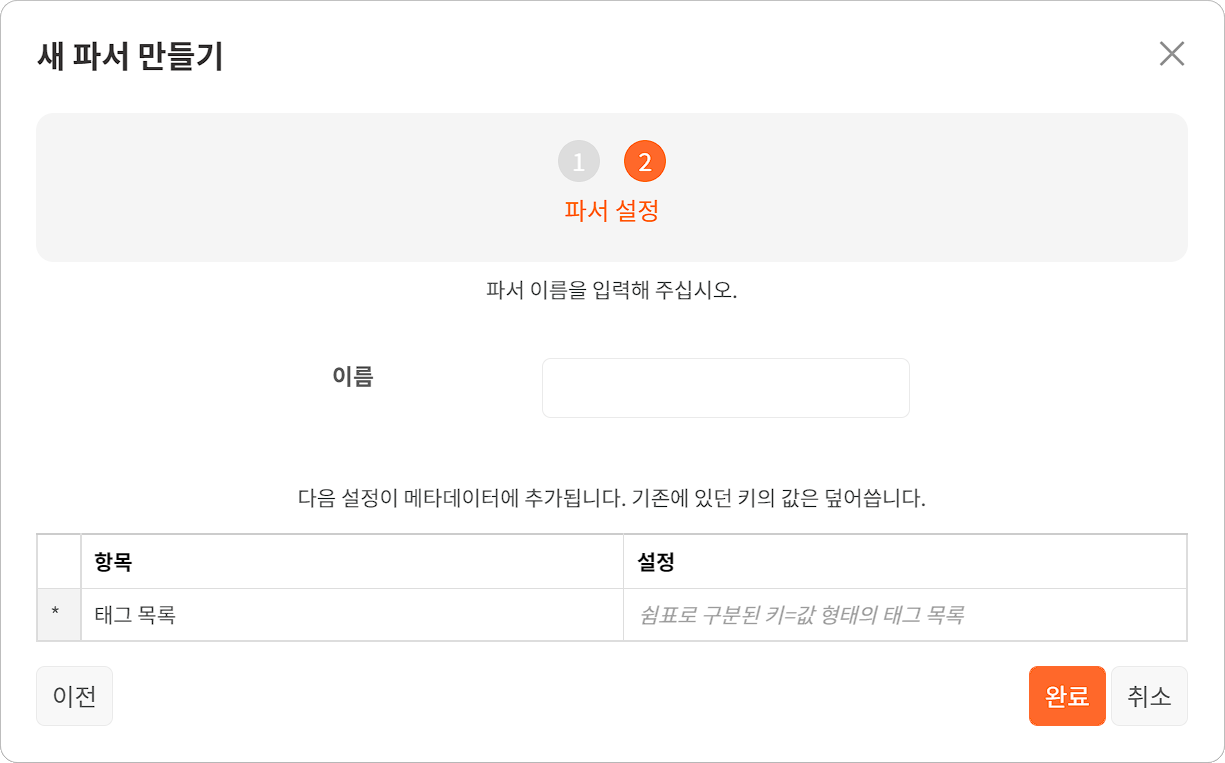
쿼리 기반 파서는 입력 데이터에 쿼리문을 수행함으로써 필드에 값을 할당합니다. 쿼리 문법을 그대로 사용할 수 있으므로 다른 파서에 비해 상대적으로 복잡하고 정교한 파싱을 수행할 수 있습니다.



* **쿼리**: 로그 파싱에 사용할 쿼리문을 입력합니다. 쿼리 문자열, 입력 로그와 쿼리 결과가 일대일로 매핑되는 쿼리 커맨드를 파이프로 연결한 쿼리를 설정할 수 있습니다. 예를 들어 [아파치 웹 서버 앱](https://logpresso.store/ko/apps/apache-httpd)의 user\_agent\_type 파서는 쿼리 기반 파서입니다. 이 파서는 다음과 같은 쿼리를 사용합니다.
* eval agent\_type = case( user\_agent == "\*Googlebot\*", "google", user\_agent == "\*GoogleDocs\*", "google docs", user\_agent == "\*bingbot\*" or user\_agent == "\*BingPreview\*", "bing", user\_agent == "\*facebookexternalhit\*", "facebook", user\_agent == "\*Yandex\*", "yandex", user\_agent == "\*api.slack.com\*", "slack", user\_agent == "\*CensysInspect\*", "censys", user\_agent == "\*Chrome\*", "chrome", user\_agent == "\*Safari\*", "safari", user\_agent == "\*Firefox\*", "firefox", user\_agent == "\*Python\*" or user\_agent == "\*python\*", "python", user\_agent == "\*Go-http-client\*", "golang", user\_agent == "\*MJ12bot\*", "mj12", user\_agent == "\*Expanse, a Palo Alto Networks\*", "xpanse", user\_agent == "\*SemrushBot\*", "semrush", user\_agent == "\*PetalBot\*", "petal", user\_agent == "\*AhrefsBot\*", "ahrefs", "misc" )

태그 파서

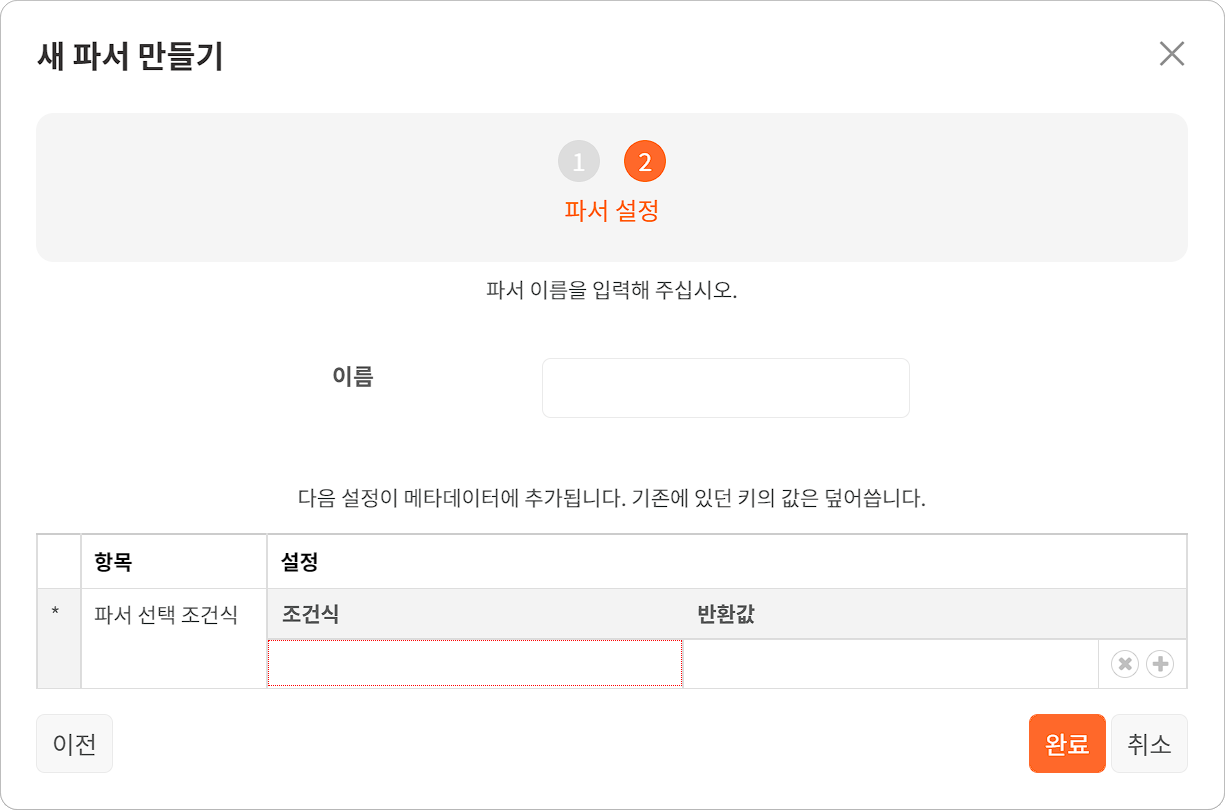
태그 파서는 메타데이터에 키-값 쌍을 추가하여 파싱합니다.



* **태그 목록**: 쉼표(,)로 구분된 키=값 쌍(메타데이터 태그)을 쉼표로 구분하여 입력합니다.

파서 선택기

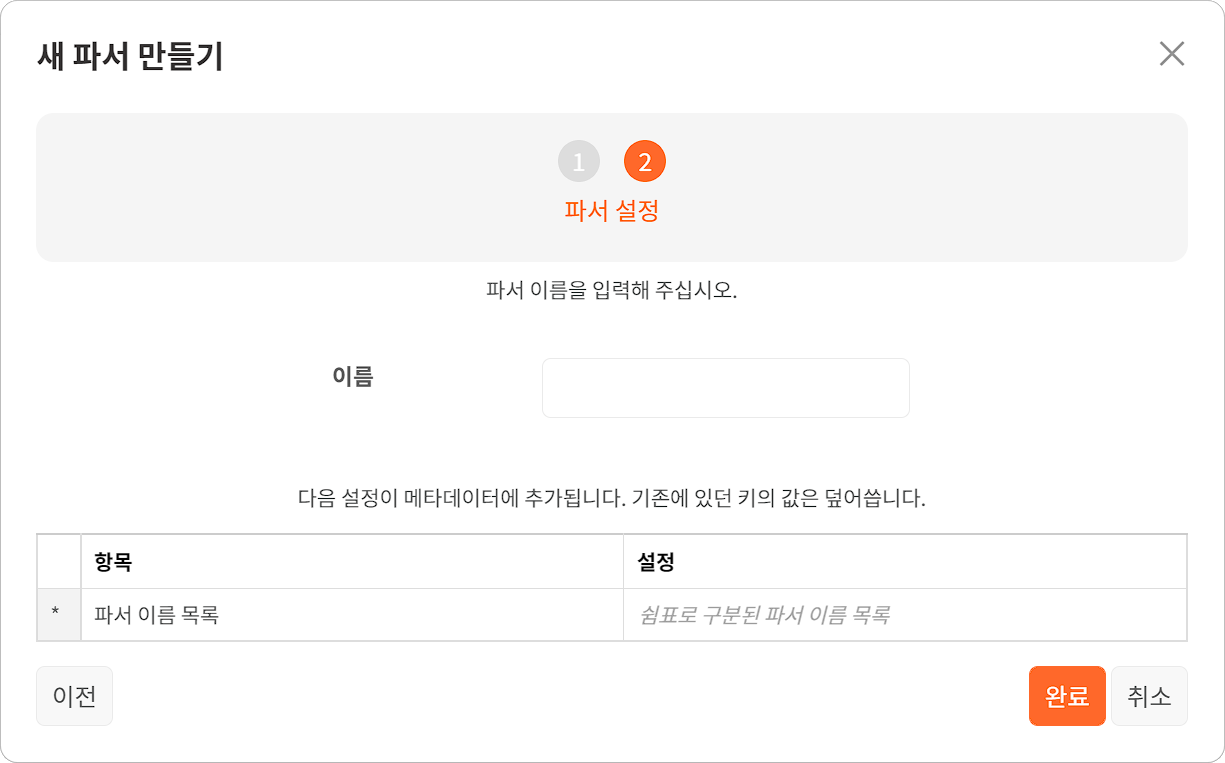
파서 선택기는 표현식 조건과 일치하는 첫번째 파서를 선택하여 파싱을 수행합니다.



* **파서 선택 조건식**: 조건식을 더 추가하려면 "**+**"를 누르십시오. "**⨉**"를 누르면 해당 조건식을 삭제합니다.
* **조건**: 파서를 선택할 조건 쿼리를 입력합니다. 여러 조건을 만족할 경우 가장 첫 번째 조건에 해당하는 파서를 선택합니다.
* **반환값**: 조건을 만족할 경우 사용할 파서의 이름을 입력합니다.

파서 체인

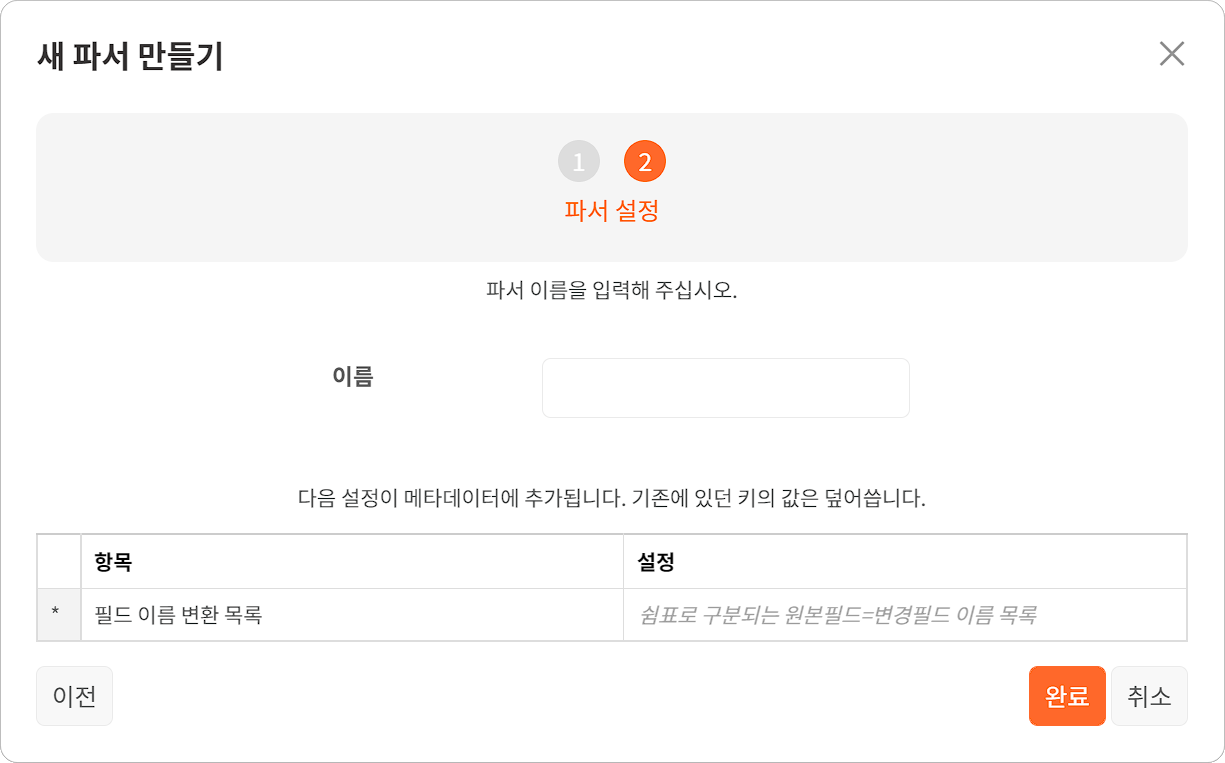
파서 체인은 여러 개 파서를 순서대로 지정하여 순차적으로 적용해 파싱합니다.



* **파서 이름 목록**: 파서의 이름을 적용할 순서대로 쉼표(,)로 구분해서 입력합니다.

필드 이름 변경 파서

필드 이름 변경 파서는 필드의 이름을 변경합니다.



* **필드 이름 변환 목록**: **원본필드=변경필드** 형식으로 쉼표(,)로 구분해서 입력합니다.