Sparrow SAST/SAQT

사용 설명서

www.SparrowFasoo.com

Sparrow

Sparrow Enterprise 소개

Sparrow Enterprise는 (주)스패로우에서 개발한 다양한 제품을 사용할 수 있는 통합 플랫폼입니다. Sparrow Enterprise를 통해 소프트웨어 개발부터 운영에 이르는 전과정에 필요한 보안 솔루션, 테스트 케이스 최적화, 워크플로 관리를 하나의 플랫폼에서 사용하실 수 있습니다.

SDLC에서 발생하는 이슈 통합 관리

Sparrow Enterprise는 소프트웨어 개발과 운영 과정에서 발생하는 다양한 보안 취약점 및 품질 이슈를 검출하고 확인함으로써 사용자가 소프트웨어 개발 수명 주기(SDLC)를 통합 관리할 수 있는 기반을 제공합니다.

워크플로 실행

워크플로 기능을 통해 DevSecOps를 구현하기 위해 필요한 태스크를 설정함으로써 프로세스를 하나로 연결할 수 있습니다. 동시에 현재 실행한 워크플로를 모니터링하고 장기적으로 워크플로의 히스토리 및 워크플로에서 발생한 이슈를 확인하고 관리할 수 있습니다.

검출 규칙 관리

Sparrow Enterprise에서는 분석에 사용할 검출 규칙을 활성화하거나 비활성화하여 규칙을 변경할 수 있습니다. 작업 프로파일을 통해 프로젝트에 따라 필요한 레퍼런스나 검출 규칙으로 필요한 이슈만을 검사하도록 조정할 수 있습니다.

웹 기반 사용자 인터페이스

Sparrow Enterprise는 웹 브라우저를 이용하여 손쉽게 분석을 수행하고 결과를 확인하도록 지원합니다. 프로젝트라는 단위로 분석 작업을 구분하고 대시보드 및 프로젝트 요약 정보 페이지를 제공하여 작업 결과 검출한 이슈를 한 눈에 확인하고 추이를 파악할 수 있습니다.

다수 사용자에 최적화된 시스템

Sparrow Enterprise는 사용자의 권한 및 역할을 커스터마이징하여 개별 사용자에게 필요한 역할을 분배합니다. 시스템뿐만 아니라 프로젝트에서도 세부적인 권한을 지정할 수 있습니다. 동시에 결재선을 통해 주요 동작을 실행하기 전에 관리자의 승인을 거치도록 설계되었습니다.

이제 Sparrow Enterprise에서 사용하실 수 있는 제품을 소개하겠습니다. Sparrow Enterprise에서 제공하는 솔루션은 **소스코드의 보안 취약점과 품질을 점검하는 Sparrow SAST/SAQT**, **웹 애플리케이션의 취약점을 분석하는 Sparrow DAST**, **오픈소스 라이선스와 컴포넌트를 관리하는 Sparrow SCA**, **웹 애플리케이션을 모니터링하며 방어하는 Sparrow RASP**, **테스트 케이스를 관리하는 Sparrow TSO** 등이며 **개발 사이클 전반에 DevSecOps를 구현하는 관리 도구인 워크플로**를 기본 기능으로 사용할 수 있습니다. 필요에 따라 원하는 제품의 라이선스를 구입하시고 해당하는 솔루션의 기능을 단일 웹 페이지에서 자유롭게 사용해보세요.

Sparrow SAST/SAQT 둘러보기

Sparrow SAST/SAQT는 정적분석을 통해 보안이나 품질과 관련하여 소스코드에 존재하는 취약점이나 잠재적인 문제를 정확하고 빠르게 검출하는 소스코드 분석 도구입니다. 웹 기반의 인터페이스뿐만 아니라 클라이언트를 통해 GUI 및 CLI 분석을 수행할 수 있으며 IDE 플러그인을 사용할 수도 있습니다. 이러한 높은 사용성과 접근성으로 인해 다양한 개발 환경에서 활용할 수 있는 제품입니다.

Sparrow SAST/SAQT 주요 기능

Sparrow SAST/SAQT에서 제공하는 주요 기능은 소스코드 분석이며 다음과 같습니다.

소스코드에 포함된 잠재적 취약점 검출

소스코드에 포함된 보안 문제는 소프트웨어의 취약점으로 이어질 수 있는 잠재적인 원인이 됩니다. **Sparrow SAST/SAQT**에서는 국내외 주요 레퍼런스를 기준으로 코드를 배포하기 전에 이러한 보안약점이 존재하는지 먼저 찾아냅니다.

소스코드에 포함된 품질 이슈 검출

보안 문제와 함께 품질 결함도 애플리케이션 배포와 운영 과정에서 중요한 이슈입니다. **Sparrow SAST/SAQT**에서는 국내외 주요 코딩 스탠다드 혹은 컨벤션과 관련된 기준을 제공합니다.

폭 넓은 지원 언어

Sparrow SAST/SAQT에서는 소프트웨어에 가장 널리 사용하는 언어에서부터 최신 언어까지 다양한 개발 언어를 분석합니다. 필요한 경우 개발 환경에 따라 분석 대상을 구분하여 보다 정확한 분석을 수행할 수도 있고 빌드 없이 대략적인 이슈를 확인하는 기능도 사용하실 수 있습니다.

제품 구성

Sparrow Enterprise는 분석 엔진과 DB를 포함하는 **서버**와 각 제품의 분석을 실행하는 **클라이언트** 및 분석 명령을 전달하는 **에이전트**로 구성됩니다.

제품 사양 및 지원 환경

Sparrow Enterprise 서버

Sparrow Enterprise 서버는 다음과 같은 하드웨어 및 지원 환경에서 설치하도록 권장합니다. 프로그램을 설치하시기 전에 확인해주세요.

CPU : Quad Core 2.50 GHz 이상

RAM : 16.0 GB 이상

HDD : 300 GB 이상

OS : Windows 10

Rocky 9.1

데이터베이스 : PostgreSQL (자체 내장)

브라우저 : Chrome 100.0.4896.88

Internet Explorer 11

Sparrow Enterprise 클라이언트

Sparrow Enterprise 클라이언트는 다음과 같은 하드웨어 및 지원 환경에서 설치하도록 권장합니다. 프로그램을 설치하시기 전에 확인해주세요.

CPU : Quad Core 2.50 GHz 이상

RAM : 16.0 GB 이상

HDD : 130 GB 이상

OS : Windows 10

Rocky 9.1

데이터베이스 : PostgreSQL (자체 내장)

플러그인 : Eclipse 2018-09

IntelliJ 2023.1.6

Visual Studio Code 1.88.1

Sparrow 태스크 에이전트

Sparrow 태스크 에이전트는 다음과 같은 지원 환경에서 설치하도록 권장합니다. 프로그램을 설치하시기 전에 확인해주세요.

Java 11

빠른 시작

사용 방법 가이드

✓ 실행하기

1. Sparrow Enterprise 서버를 시작하세요.

2. 웹 브라우저에서 Sparrow Enterprise 서버 URL(**https://{Sparrow Enterprise 서버 IP 주소}:{포트 번호}**)로 이동하세요.

3. 최고 관리자에게 받은 ID와 비밀번호를 입력한 후에 **로그인** 버튼을 클릭하세요.

자세한 내용은 **서버 시작하기** 혹은 **로그인하기**에서 확인하시기 바랍니다.

✓ 프로젝트 만들기

1. 왼쪽 사이드 바에서 **프로젝트 목록** 아이콘을 클릭하세요.

2. **프로젝트 추가하기** 버튼을 클릭하세요.

3. 프로젝트 정보를 입력하세요.

4. **추가** 버튼을 클릭하세요.

자세한 내용은 **새 프로젝트 만들기**에서 확인하시기 바랍니다.

✓ Sparrow SAST/SAQT 소스코드 분석 수행하기

웹 서버에서 직접 분석하는 방법은 다음과 같습니다.

1. 웹 브라우저에서 Sparrow Enterprise 서버 URL(**https://{Sparrow Enterprise 서버 IP 주소}:{포트 번호}**)로 이동하세요.

2. **프로젝트 상세 정보** 페이지에서 **새 작업 시작하기** 버튼을 클릭하세요.

3. **전수 분석** 혹은 **수시 분석** 카드를 클릭하고 **작업 프로파일**을 선택하세요.

4. **분석 대상** 중에서 **압축 파일**을 선택하세요.

5. 압축된 소스코드 파일을 선택하고 **확장자**를 선택하세요.

6. **선택하기** 버튼과 **시작하기** 버튼을 차례대로 클릭하세요.

자세한 내용은 **웹 서버에서 소스코드 분석하기**에서 확인하시기 바랍니다.

클라이언트를 통해 분석하는 방법은 다음과 같습니다.

1. **Sparrow Enterprise 클라이언트 설치 디렉토리**로 이동하세요.

2. Windows 환경에서는 **sparrow-client-manager.exe** 파일을 실행하고 작업을 수행할 프로젝트 및 작업 프로파일을 선택하고 실행하세요.

자세한 내용은 **클라이언트 GUI: 소스코드 분석하기**에서 확인하시기 바랍니다.

3. 다른 환경인 경우 **sparrow-cli** 파일을 명령어 및 옵션과 함께 실행하세요.

자세한 내용은 **클라이언트 CLI: 소스코드 분석하기**에서 확인하시기 바랍니다.

✓ 분석 이슈 보기

1. 왼쪽 사이드 바에서 **프로젝트 목록** 아이콘을 클릭하세요.

2. 확인하려는 **프로젝트**를 클릭하세요.

3. 오른쪽 탭에서 **이슈**를 클릭하세요.

4. 해당 정보를 확인할 수 있습니다.

자세한 내용은 라이선스에 따라 **최근 이슈 확인하기**, **소스코드 이슈**, **컴포넌트 이슈**, **웹 취약점 이슈**, **자가 방어 이슈**에서 확인하시기 바랍니다.

✓ 워크플로 실행하기

이 작업은 **워크플로 관리** 권한을 가진 사용자만 사용할 수 있습니다.

1. 왼쪽 사이드 바에서 **워크플로** 아이콘을 클릭하세요.

2. **워크플로**를 추가하세요.

3. **태스크**와 **액션**을 추가하세요.

4. **워크플로 상세 정보** 페이지에서 **워크플로 실행하기** 버튼을 클릭하세요.

자세한 내용은 **워크플로**에서 확인하시기 바랍니다.

사용자 혹은 관리자를 위한 가이드

본 가이드는 Sparrow Enterprise를 사용하는 기본적인 방법을 설명하고 있습니다. 사용자는 부여된 권한에 따라 필요한 내용을 참고하시기 바랍니다.

✓ 사용자용 매뉴얼

- 새 프로젝트 만들기
- 프로젝트 수정하기
- 분석하기
- 작업 예약하기
- Eclipse 플러그인 사용하기
- IntelliJ 플러그인 사용하기
- Visual Studio Code 플러그인 사용하기
- 자산 확인하기
- 이슈 확인하기
- 이슈 제외하기

✓ 관리자용 매뉴얼

- Sparrow Enterprise 서버 설치하기
- Sparrow Enterprise 클라이언트 설치하기
- Sparrow 태스크 에이전트 설치하기
- 제품 라이선스 적용하기
- 워크플로 만들기
- 시스템 역할 관리하기 및 프로젝트 역할 관리하기
- 결재선 관리하기
- 사용자 관리하기 및 사용자 그룹 관리하기
- 이슈 검출 규칙 관리하기 및 작업 프로파일 관리하기
- 태스크 에이전트 관리하기
- 보고서 템플릿 관리하기
- 시스템 정보 확인하기 및 제품 라이선스 정보 확인하기

이제 Sparrow Enterprise를 설치하는 과정부터 시작해서, 프로젝트를 생성하고, 각 제품에서 분석 및 방어, 최적화를 수행하며, 결과를 확인하는 등 Sparrow Enterprise를 사용하는 과정 및 계정 정보를 확인하고,

Sparrow Enterprise와 관련된 설정을 변경하는 등 관리하는 방법을 순서대로 설명하겠습니다.

설치하기

Sparrow Enterprise 서버 설치하기

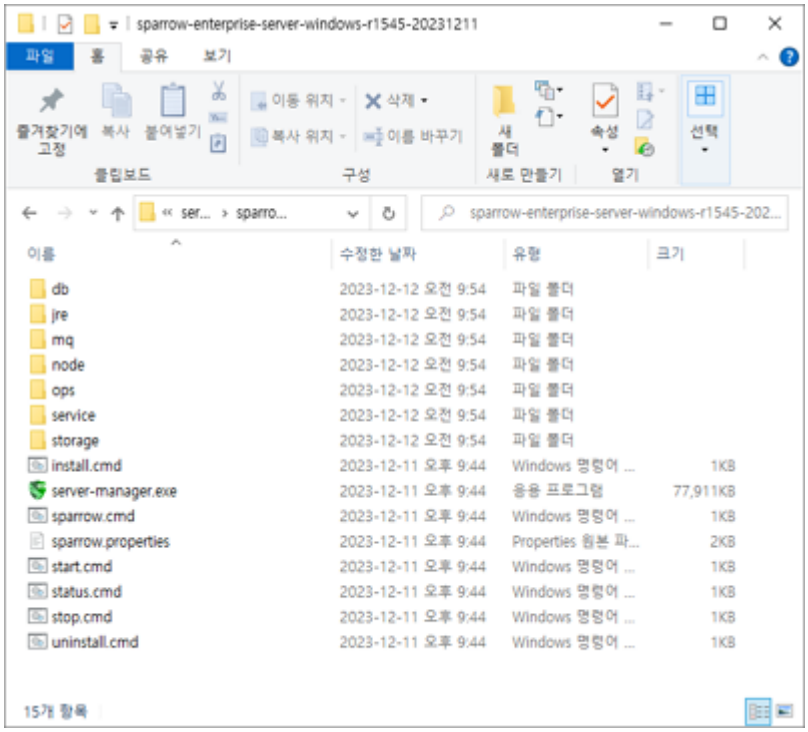
Windows 환경에서 Sparrow Enterprise를 설치하는 경우 **서버 매니저**를 사용할 수 있습니다. Linux 환경에 서버를 설치해야 하거나 Windows에서 GUI를 사용하지 않고 설치하려면 **CMD**로 설치 명령어를 입력하세요.

> **Tip**: **자가 방어**를 수행하려면 Sparrow Enterprise를 Linux 환경에 설치하세요.
>
> **워크플로**를 실행하려면 시스템 환경 변수에 `JAVA_HOME`을 설정했는지 확인하세요.

Sparrow Enterprise 서버 매니저로 설치하기

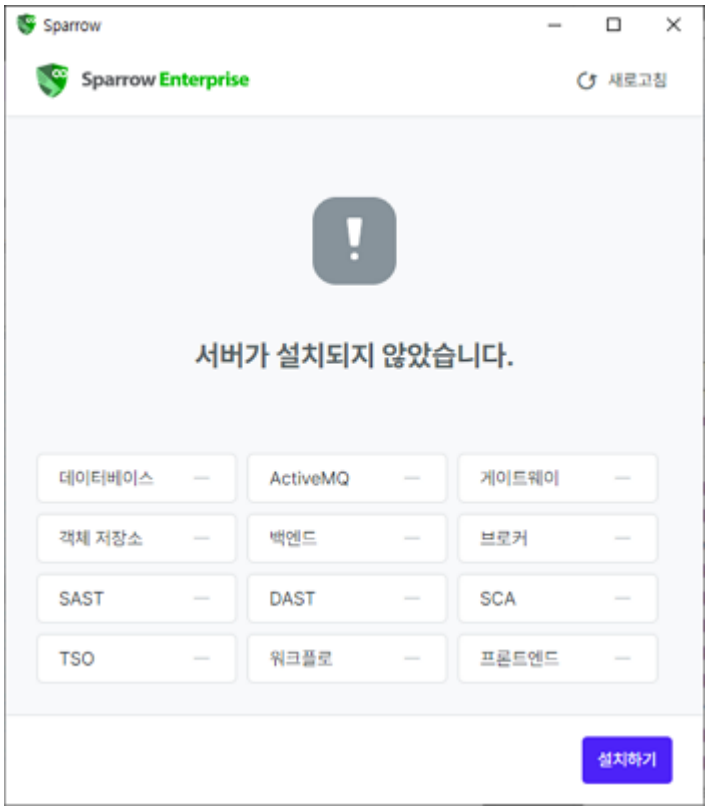
Windows에서는 **서버 매니저**를 사용하여 Sparrow Enterprise를 설치하고 시작할 수 있습니다.

1. 패키지에 포함된 CD를 설치할 컴퓨터에 삽입하세요.
2. CD에 포함된 **sparrow-enterprise-server-{OS+version}.zip** 파일을 원하는 영문 디렉토리에 복사한 후 압축을 해제하세요.



> **Warning**: Sparrow Enterprise의 설치 경로에 한글 또는 공백이 포함되어 있으면 정상적으로 설치되지 않습니다.

3. **{Sparrow Enterprise 서버 설치 디렉토리}** 폴더에 있는 **server-manager.exe** 파일을 실행하세요.



4. **Sparrow Enterprise**가 설치됩니다.

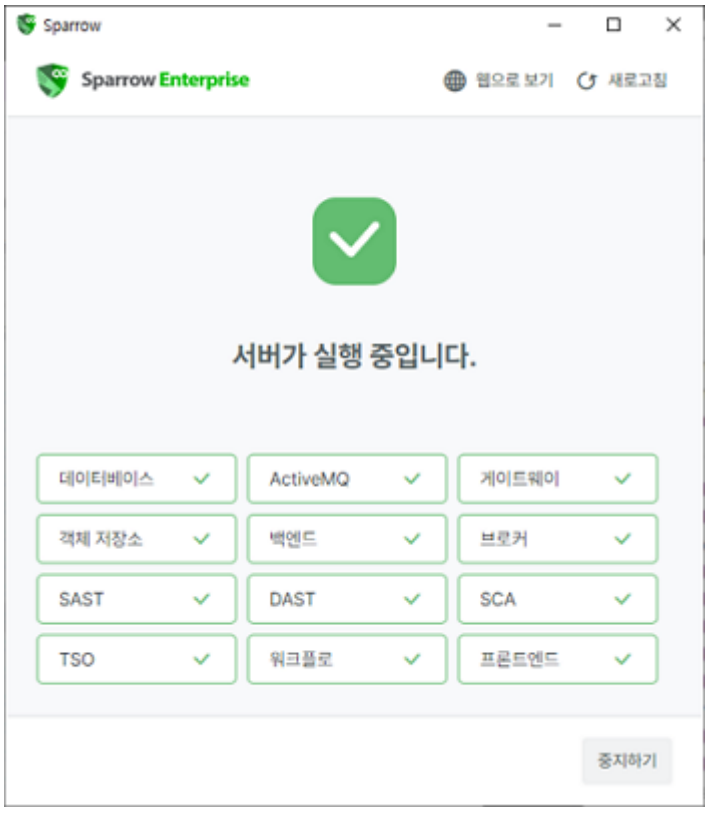
서버 매니저를 사용해서 Sparrow Enterprise 서버를 시작하는 방법은 다음과 같습니다.

5. **서버 매니저**를 실행하세요.

6. **모두 실행하기** 버튼을 클릭하세요.

> **Tip**: **설치되지 않은 모듈**이 있는 경우 **실행하기** 버튼을 클릭할 수 없습니다. 모든 모듈이 설치되었는지 확인하세요.

7. 서버가 시작됩니다.



서버 매니저를 사용해서 Sparrow Enterprise 서버를 중지하는 방법은 다음과 같습니다.

8. **서버 매니저**를 실행하세요.
9. **모두 중지하기** 버튼을 클릭하세요.
10. 서버가 중지됩니다.

CMD 명령어로 Sparrow Enterprise 설치하기

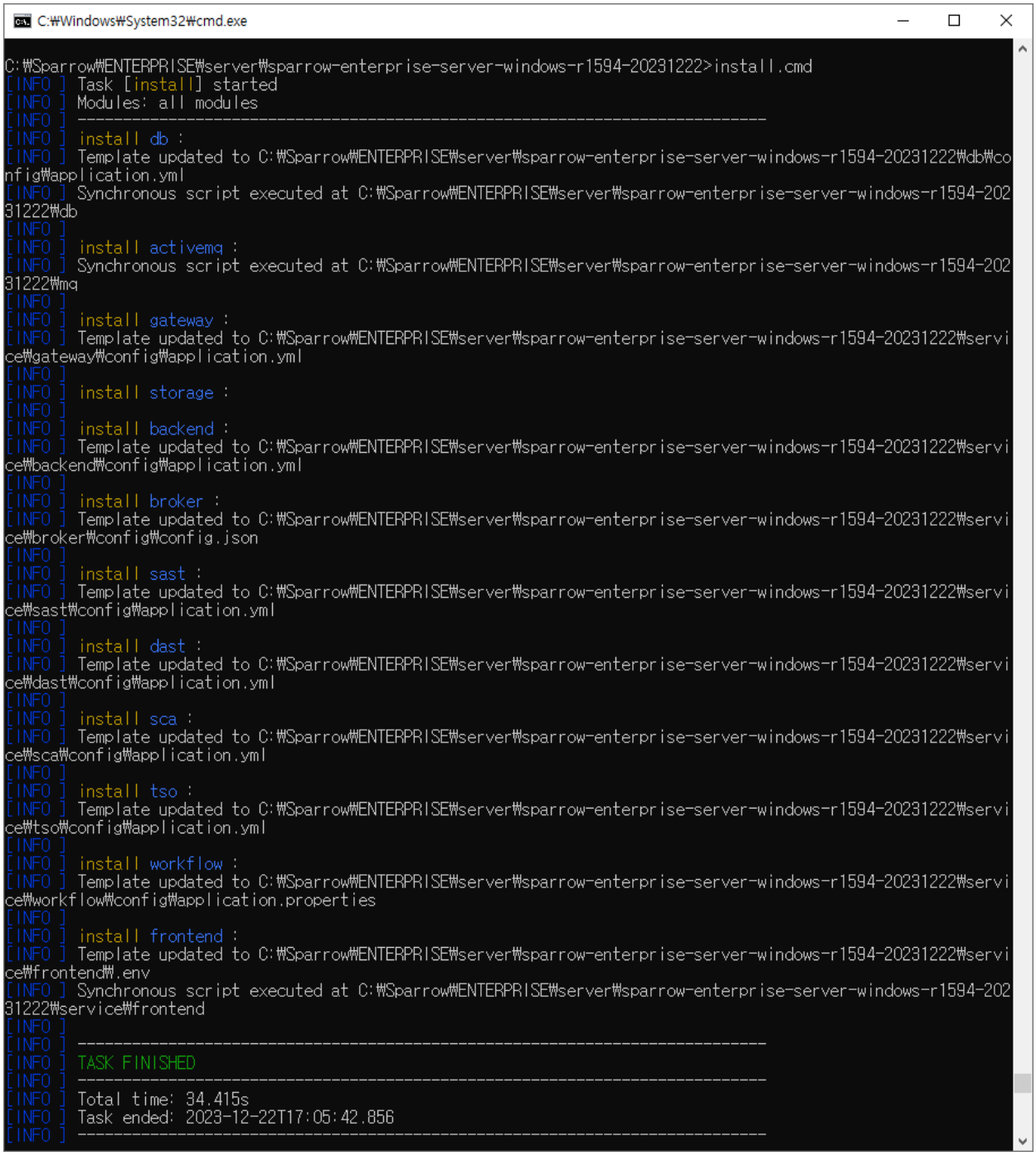
<Windows 환경>

서버 매니저 대신 CMD 명령어로 Sparrow Enterprise 서버를 설치할 수 있습니다.

1. 패키지에 포함된 CD를 설치할 컴퓨터에 삽입하세요.
2. CD에 포함된 **sparrow-enterprise-server-{OS+version}.zip** 파일을 원하는 영문 디렉토리에 복사한 후 압축을 해제하세요.

> **Warning**: Sparrow Enterprise의 설치 경로에 한글 또는 공백이 포함되어 있으면 정상적으로 설치되지 않습니다.

3. **{Sparrow Enterprise 서버 설치 디렉토리}** 폴더에 있는 **install.cmd** 파일을 실행하세요.



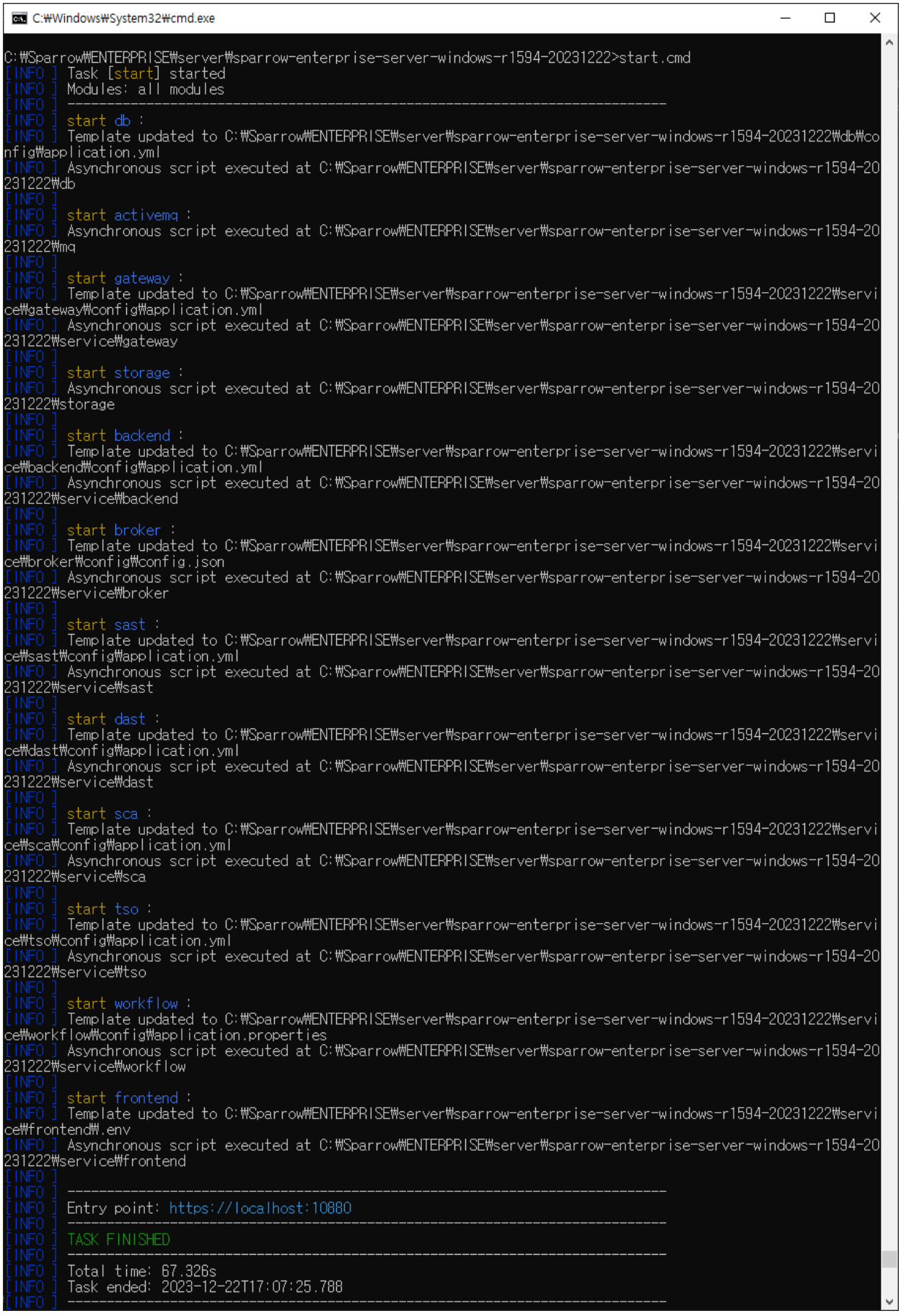
4. **Sparrow Enterprise**가 설치됩니다.

설치된 Sparrow Enterprise 서버를 시작하는 방법은 다음과 같습니다.

5. **{Sparrow Enterprise 서버 설치 디렉토리}** 경로로 이동하세요.

6. **start.cmd** 파일을 실행하세요.

7. 다음과 같은 메시지가 표시되면서 서버가 시작됩니다.

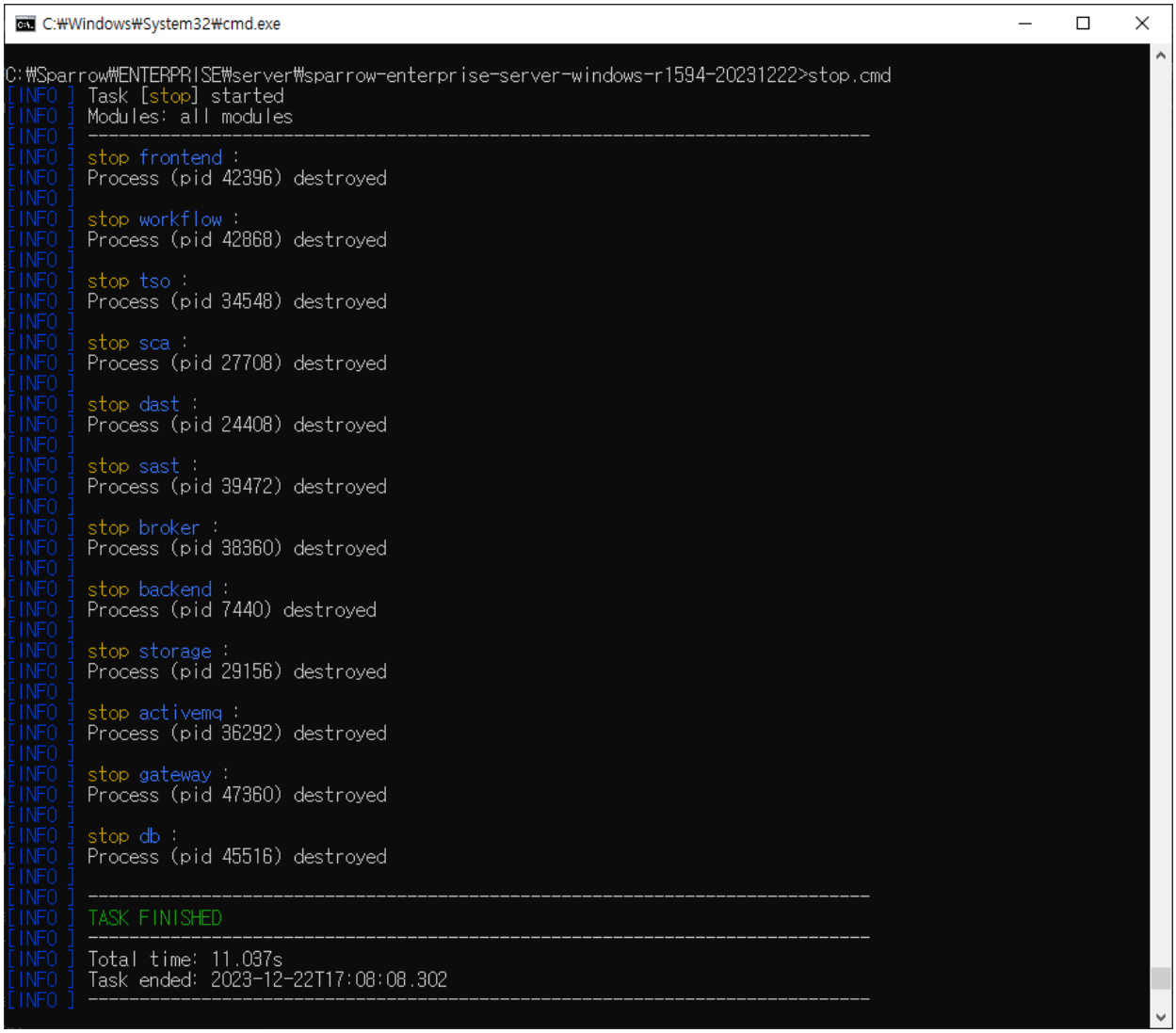


시작된 Sparrow Enterprise 서버를 중지하는 방법은 다음과 같습니다.

8. **{Sparrow Enterprise 서버 설치 디렉토리}** 경로로 이동하세요.

9. **stop.cmd** 파일을 실행하세요.

10. 다음과 같은 메시지가 표시되면서 서버가 중지됩니다.



<Linux 환경>

Sparrow Enterprise 서버는 Rocky 9.1 환경에서 CMD 명령어로 설치할 수 있습니다.

1. 패키지에 포함된 CD를 설치할 컴퓨터에 삽입하세요.

2. CD에 포함된 **sparrow-server-{OS+version}-{YYYYMMDD}.tar.gz** 파일을 원하는 영문 디렉토리에 복사한 후 압축을 해제하세요.

> **Warning**: Sparrow Enterprise의 설치 경로에 한글 또는 공백이 포함되어 있으면 정상적으로 설치되지 않습니다.

3. **{Sparrow Enterprise 서버 설치 디렉토리}** 폴더에 있는 **install** 파일을 실행하세요.

4. **Sparrow Enterprise**가 설치됩니다.

설치된 Sparrow Enterprise 서버를 시작하는 방법은 다음과 같습니다.

5. **{Sparrow Enterprise 서버 설치 디렉토리}** 경로로 이동하세요.
6. **./start** 명령어를 실행하세요.
7. 서버가 시작됩니다.

시작된 Sparrow Enterprise 서버를 중지하는 방법은 다음과 같습니다.

8. **{Sparrow Enterprise 서버 설치 디렉토리}** 경로로 이동하세요.
9. **./stop** 명령어를 실행하세요.
10. 서버가 중지됩니다.

Sparrow Enterprise 프로퍼티 설정하기

Sparrow Enterprise 서버를 설치할 때 필요한 설정 정보는 **{Sparrow Enterprise 서버 설치 디렉토리}**에 있는 **sparrow.properties** 파일에 기록됩니다. 다음을 참고하여 해당 파일에 저장된 내용을 수정하고 저장함으로써 프로그램 설정을 변경할 수 있습니다.

✓ 서비스 설정

service.host

Sparrow Enterprise 서버의 호스트 주소입니다.(기본값: `localhost`)

service.public.host

Sparrow Enterprise 서버를 외부에 공개할 목적으로 사용하는 호스트 주소입니다. 예를 들어, 이 호스트 주소를 사용하여 분석이 완료되고 해당 결과에 접근하는 주소를 안내할 수 있습니다.(기본값: `localhost`)

service.frontend.port

Sparrow Enterprise 서버의 프론트엔드 포트 번호입니다.(기본값: `10880`)

service.gateway.port

Sparrow Enterprise 서버의 게이트웨이 포트 번호입니다.(기본값: `10500`)

service.backend.port

Sparrow Enterprise 서버의 백엔드 포트 번호입니다.(기본값: `10610`)

service.brocker.port

Sparrow Enterprise 서버의 브로커 포트 번호입니다.(기본값: `10700`)

service.brocker.grpc.port

Sparrow Enterprise 서버의 브로커에서 사용하는 gRPC(google Remote Procedure Call) 포트 번호입니다.(기본값: `10800`)

service.sast.port

Sparrow SAST 서버의 포트 번호입니다.(기본값: `10900`)

service.dast.port

Sparrow DAST 서버의 포트 번호입니다.(기본값: `10910`)

service.rasp.port

Sparrow RASP 서버의 포트 번호입니다.(기본값: `10920`)

service.sca.port

Sparrow SCA 서버의 포트 번호입니다.(기본값: `10930`)

service.tso.port

Sparrow TSO 서버의 포트 번호입니다.(기본값: `10950`)

service.workflow.port

워크플로 서버의 포트 번호입니다.(기본값: `10960`)

service.entrypoint

Sparrow Enterprise 서버에 접속하기 위해 사용하는 포트를 지정합니다.(기본값: `frontend`)

✓ 솔루션 구동 설정

service.db.enabled

Sparrow Enterprise 데이터베이스를 구동하는 옵션이며 `true`, `false`로 구분합니다.(기본값: `true`)

service.storage.enabled

Sparrow Enterprise에서 사용하는 객체 저장소를 구동하는 옵션이며 `true`, `false`로 구분합니다.(기본값: `true`)

service.activemq.enabled

워크플로의 미들웨어로 사용되는 ActiveMQ 서버를 구동하는 옵션이며 `true`, `false`로 구분합니다.(기본값: `true`)

service.frontend.enabled

Sparrow Enterprise 서버의 프론트엔드를 구동하는 옵션이며 `true`, `false`로 구분합니다.(기본값: `true`)

service.gateway.enabled

Sparrow Enterprise 서버의 게이트웨이를 구동하는 옵션이며 `true`, `false`로 구분합니다.(기본값: `true`)

service.backend.enabled

Sparrow Enterprise 서버의 백엔드를 구동하는 옵션이며 `true`, `false`로 구분합니다.(기본값: `true`)

service.broker.enabled

Sparrow Enterprise 서버의 브로커를 구동하는 옵션이며 `true`, `false`로 구분합니다.(기본값: `true`)

service.sast.enabled

Sparrow SAST 서버를 구동하는 옵션이며 `true`, `false`로 구분합니다.(기본값: `true`)

service.dast.enabled

Sparrow DAST 서버를 구동하는 옵션이며 `true`, `false`로 구분합니다.(기본값: `true`)

service.rasp.enabled

Sparrow RASP 서버를 구동하는 옵션이며 `true`, `false`로 구분합니다.(기본값: `true`)

service.sca.enabled

Sparrow SCA 서버를 구동하는 옵션이며 `true`, `false`로 구분합니다.(기본값: `true`)

service.tso.enabled

Sparrow TSO 서버를 구동하는 옵션이며 `true`, `false`로 구분합니다.(기본값: `true`)

service.workflow.enabled

워크플로 서버를 구동하는 옵션이며 `true`, `false`로 구분합니다.(기본값: `true`)

service.frontend.https

Sparrow Enterprise 서버의 프론트엔드 프로토콜을 `HTTPS`로 설정하는 옵션이며 `true`, `false`로 구분합니다.(기본값: `true`)

✓ 데이터베이스 설정

db.home

Sparrow Enterprise 데이터베이스의 홈 디렉토리 경로입니다.(기본값: `./db`)

db.host

Sparrow Enterprise 데이터베이스의 호스트입니다.(기본값: `localhost`)

db.port

Sparrow Enterprise 데이터베이스의 포트 번호입니다.(기본값: `10620`)

db.name

Sparrow Enterprise 데이터베이스의 이름입니다.(기본값: `sparrow`)

db.username

Sparrow Enterprise 데이터베이스의 사용자 이름입니다.(기본값: `postgres`)

db.password

Sparrow Enterprise 데이터베이스의 사용자 비밀번호입니다. 설치 후 기본 비밀번호를 변경하는 것을 권장합니다.(기본값: `iXzVzYiXl2U3W9X82wbA4w==`)

> **Tip**: AES-256 알고리즘으로 암호화된 경우 비밀번호가 다르게 표시됩니다. Sparrow Enterprise에서는 AES-256을 사용하여 프로퍼티 파일의 비밀번호를 암호화합니다.

✓ 스토리지 설정

storage.home

Sparrow Enterprise에서 사용하는 객체 저장소의 홈 디렉토리 경로입니다.(기본값: `./storage`)

storage.port

Sparrow Enterprise에서 사용하는 객체 저장소의 포트 번호입니다.(기본값: `10621`)

storage.console.port

Sparrow Enterprise에서 사용하는 객체 저장소의 콘솔 포트 번호입니다.(기본값: `8888`)

storage.username

Sparrow Enterprise에서 사용하는 객체 저장소의 사용자 이름입니다.(기본값: `sparrow`)

storage.password

Sparrow Enterprise에서 사용하는 객체 저장소의 사용자 비밀번호입니다.(기본값: `gLUZGcZAoyhjXtvwBFEd9g==`)

✓ ActiveMQ 설정

activemq.port

워크플로의 미들웨어로 사용되는 ActiveMQ 서버의 포트 번호입니다.(기본값: `61616`)

activemq.console.port

워크플로의 미들웨어로 사용되는 ActiveMQ 서버의 콘솔 포트 번호입니다.(기본값: `8161`)

activemq.username

워크플로의 미들웨어로 사용되는 ActiveMQ 서버의 사용자 이름입니다.(기본값: `sparrow`)

activemq.password

워크플로의 미들웨어로 사용되는 ActiveMQ 서버의 사용자 비밀번호입니다.(기본값: `qRqXD92vMcDFs5BuroCvZtXwKFqCuFF8`)

✓ 기타 설정

jre.home

Java 런타임 환경의 홈 디렉토리 경로입니다.(기본값: `./jre`)

node.home

Node.js 런타임 환경의 홈 디렉토리 경로입니다.(기본값: `./node`)

✓ 보안 설정

security.auth.trials.max

사용자 계정에서 비밀번호를 잘못 입력하여 실패한 로그인 시도를 허용하는 횟수입니다. 한 번 로그인하면 해당 로그인 이전에 시도한 잘못된 로그인 기록은 삭제됩니다.(기본값: `5`)

security.auth.password.pattern

사용자 계정에서 비밀번호가 만족해야 할 조건입니다. 기본적으로 **영문자, 숫자, 특수문자의 조합으로 이루어진 최소 9자에서 최대 16자까지의 문자열**로 설정되어 있습니다.(기본값: `^(?\=.*\\d)(?\=.*[a-zA-Z])(?\=.*[^\\da-zA-Z]).{9,16}$`)

security.session.age

사용자 세션이 만료되는 시간이며 사용자가 Sparrow Enterprise 서버에 로그인한 시점부터 측정합니다.(단위: ms, 기본값: `86,400,000`)

security.ip.allowed

Sparrow Enterprise에 접속 가능한 사용자의 IP를 가리키며 하나 이상의 IP를 입력하고 띄어쓰기 없이 쉼표(,)로 구분할 수 있습니다.

이 옵션에 접속을 허용할 사용자의 IP를 입력하는 경우 해당 IP에서 접속을 요청하지 않는 사용자는 시스템에 연결할 수 없습니다. 이 옵션에 값을 입력하지 않으면 사용자의 접속을 제한하지 않습니다.

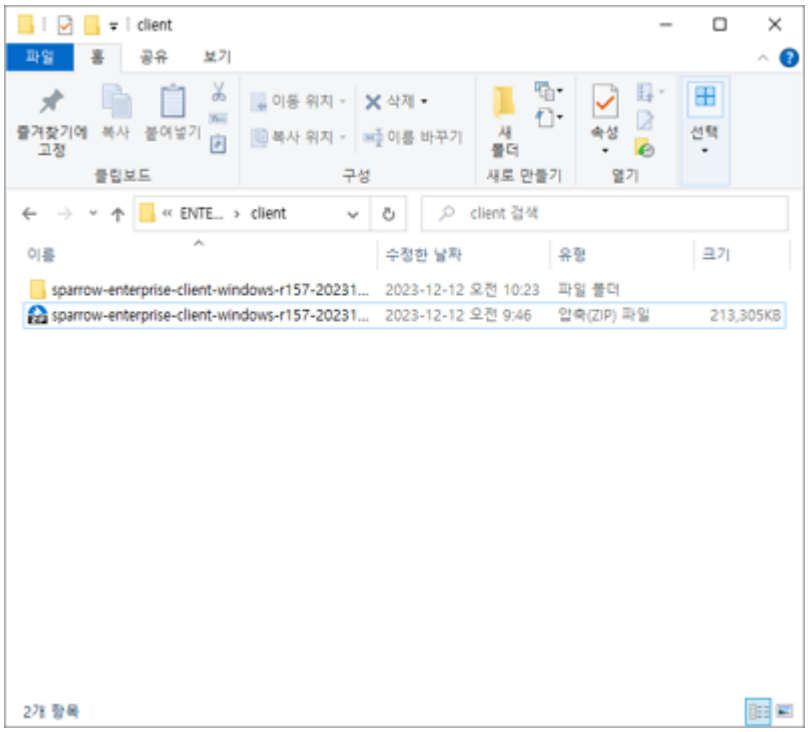
Sparrow Enterprise 클라이언트 설치하기

Sparrow Enterprise 클라이언트에서는 소스코드 분석과 컴포넌트 분석을 수행할 수 있습니다. 특히 컴포넌트 분석은 **Sparrow Enterprise 서버**로 연결된 웹 브라우저에서 직접 명령할 수 없습니다. 따라서 서버를 설치한 후 Sparrow Enterprise 클라이언트도 설치해야 합니다. 아래를 참고하여 **Sparrow Enterprise 클라이언트**를 설치하세요.

> **Tip**: **Sparrow Enterprise 클라이언트**는 Windows 환경의 경우 **GUI**와 **CLI**, Linux 계열의 경우 **CLI**를 사용하는 분석을 지원합니다.

<Windows 환경>

1. 패키지에 포함된 Sparrow Enterprise CD를 설치할 컴퓨터에 삽입하세요.
2. **Sparrow Enterprise 클라이언트** 경로로 이동하여, **sparrow-client-{OS+version}-{YYYYMMDD}.zip** 파일을 원하는 영문 디렉토리 경로에 복사한 뒤 압축을 해제하세요.



3. 이제 클라이언트 설치가 완료되었습니다.

<Linux 환경>

1. 패키지에 포함된 Sparrow Enterprise CD를 설치할 컴퓨터에 삽입하세요.
2. **Sparrow Enterprise 클라이언트** 경로로 이동하여, **sparrow-client-{OS+version}-{YYYYMMDD}.tar.gz** 파일을 원하는 영문 디렉토리 경로에 복사한 뒤 압축을 해제하세요.

> **Warning**: root 계정이 아닌 일반 계정으로 Sparrow Enterprise 클라이언트를 설치해야 합니다. 또한, Sparrow Enterprise 클라이언트의 설치 경로에 한글 또는 공백이 포함되어 있으면 정상적으로 설치되지 않습니다.

3. 이제 클라이언트 설치가 완료되었습니다.

Sparrow Enterprise 클라이언트를 사용해서 분석을 시작하려면 소스코드 분석 및 컴포넌트 분석을 참고하세요.

Sparrow Enterprise 클라이언트 환경 설정하기

클라이언트 GUI의 오른쪽 위에 있는 설정 아이콘을 클릭하면 클라이언트에서 분석에 사용되는 설정을 저장할 수 있습니다. 여기에서 저장한 내용은 클라이언트 GUI를 사용하여 수행하는 모든 분석에 적용됩니다.

✓ 데이터 관리

분석 임시 파일 경로

분석을 수행할 때 전처리 파일과 같은 임시 파일을 저장하는 위치입니다. **찾아보기** 버튼을 클릭하여 경로를 선택할 수 있습니다.

분석 후 임시 파일 삭제

분석 임시 파일 경로에 저장된 임시 파일을 분석이 완료된 후 제거하도록 설정하는 옵션이며 예, 아니요로 구분합니다.

이 옵션을 예로 설정하면 분석이 완료된 후 분석의 임시 파일을 자동으로 삭제합니다. 이 옵션을 아니요로 설정하면 분석이 완료된 후에도 임시 파일을 삭제하지 않고 그대로 둡니다.(기본값: 아니요)

✓ IDE 설정

소스코드 분석을 수행할 때 C/C++ 관련 IDE와 연동한 경우 **찾아보기** 버튼을 클릭하여 Visual Studio, Code Warrior, Code Composer Studio, Wind River와 같은 개발 도구의 경로를 설정합니다.

이 옵션에 입력한 값은 소스코드 분석을 수행하기 위해 입력하는 옵션 중 하나인 **IDE 경로**의 기본값으로 입력됩니다. 자세한 내용은 클라이언트 GUI: 소스코드 분석하기를 참고하세요.

Sparrow 태스크 에이전트 설치하기

태스크 에이전트는 워크플로에서 태스크에 명령을 전달하는 모듈을 가리킵니다.

1. **task-agent.jar** 파일을 태스크를 실행할 머신의 로컬에 배치하세요.
2. 아래 내용을 참고하여 실행하세요.

```
java -Dsparrow.agent={AGENT_NAME} -Dsparrow.url={GATEWAY_HOST}:{GATEWAY_PORT} -
Dsparrow.username={USER_NAME} -Dsparrow.password={USER_PASSWORD} -
Dsparrow.opt.server.port={AGENT_PORT} -jar task-agent.jar
```

> **Tip**: Java 명령어에서 입력할 때는 옵션 앞에 `-D`를 붙여야 합니다.

sparrow.agent

{AGENT_NAME}은 태스크 에이전트의 이름이며 64자까지 표시됩니다. 워크플로에서 태스크에 지정 태스크 에이전트를 선택하거나 워크플로 실행에서 태스크 목록을 표시하는 경우 해당 태스크가 사용한 태스크 에이전트의 이름이 표시됩니다. 자세한 내용은 태스크 추가하기 혹은 워크플로 실행 확인하기를 참고하세요.(예시: `local_agent`)

sparrow.url

`{GATEWAY_HOST}`는 `HTTP` 프로토콜을 포함한 게이트웨이의 호스트 주소이고 `{GATEWAY_PORT}`는 게이트웨이의 포트 번호입니다. 게이트웨이는 Sparrow Enterprise 서버를 설치할 때 함께 설치됩니다. Sparrow Enterprise 서버의 설정 파일인 **sparrow.properties**에서 정보를 확인하세요. 자세한 내용은 Sparrow Enterprise 프로퍼티 설정하기를 참고하세요.(예시: `https://192.168.100.98:10500`)

sparrow.username

`{USER_NAME}`은 태스크 에이전트를 사용하는 사용자의 이름입니다. 이 옵션을 올바르게 입력하지 않은 경우 구동할 수 없습니다.

sparrow.password

`{USER_PASSWORD}`는 태스크 에이전트를 사용하는 사용자의 비밀번호입니다. 올바르게 입력하지 않은 경우 구동에 실패합니다.

sparrow.opt.server.port

`{AGENT_PORT}`는 태스크 에이전트의 포트 번호입니다. 태스크 에이전트에서 사용할 포트를 지정하세요. (예시: `10110`)

시작하기

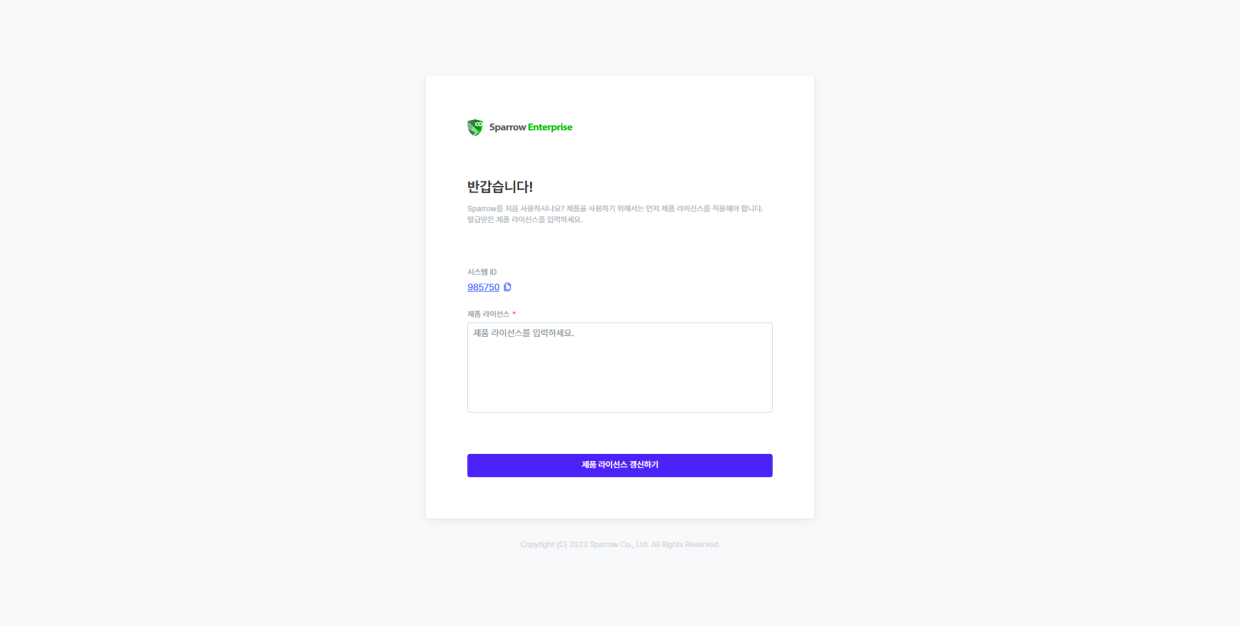
제품 라이선스 적용하기

Sparrow Enterprise를 사용하기 위해서는 Sparrow Enterprise **제품 라이선스**가 필요합니다. Sparrow Enterprise 제품 라이선스를 적용하는 방법은 다음과 같습니다.

1. 웹 브라우저를 여세요.
2. **Sparrow Enterprise 서버 URL(https://{Sparrow Enterprise 서버 IP 주소}:{포트 번호})**를 입력하세요.
3. **최고 관리자**로 로그인하세요.

> **Tip**: 기본 설정된 최고 관리자 계정의 ID는 **admin**이며, 비밀번호는 **a1234567!** 입니다.

4. 최초로 로그인하면 비밀번호를 새로 설정한 후 **제품 라이선스**를 입력하는 화면이 표시됩니다. 제품 라이선스를 만들기 위해 **시스템 ID**를 복사하여 스패로우 엔지니어에게 전달하세요.



5. 담당자에게서 발급 받은 제품 라이선스 키를 **제품 라이선스**에 입력하고 **제품 라이선스 갱신하기** 버튼을 클릭하세요.

이미 적용된 제품 라이선스가 무엇인지 확인하려면 제품 라이선스 정보 확인을 참고하세요.

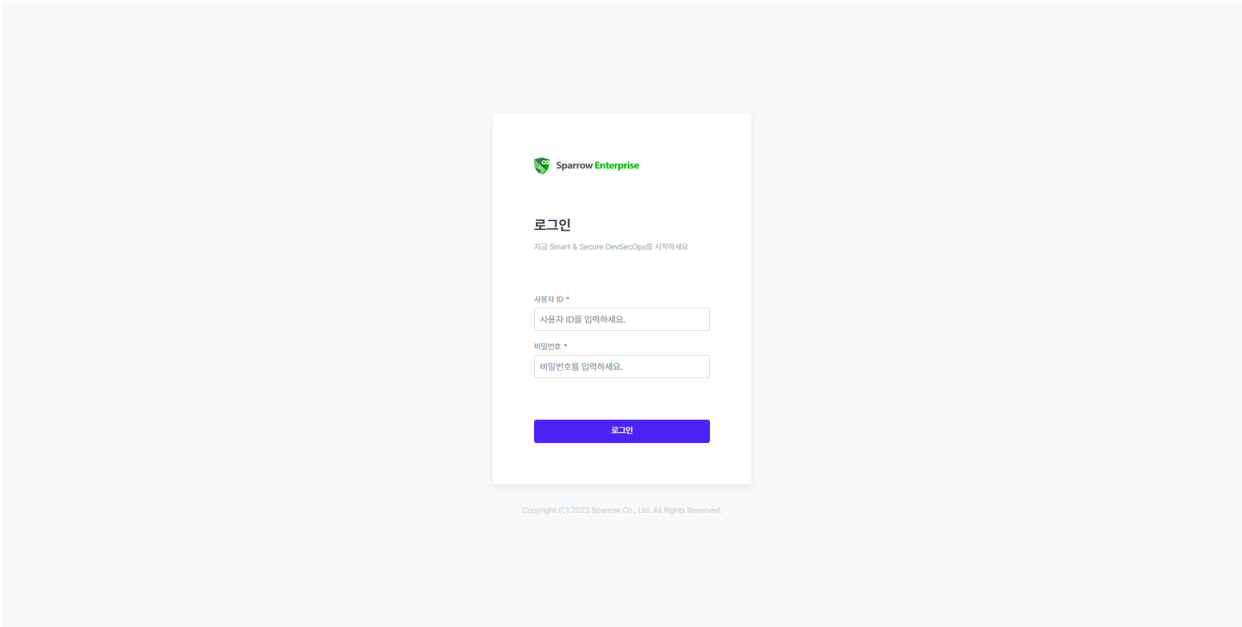
로그인하기

Sparrow Enterprise를 사용하기 위해서는 다른 클라이언트보다 먼저 **Sparrow Enterprise 서버**에 로그인해야 합니다. 시스템의 **인증 및 사용자 관리** 권한을 가진 관리자가 설정한 ID와 비밀번호를 입력하여 로그인합니다. ID와 비밀번호를 알 수 없는 경우 관리자에게 문의하시기 바랍니다.

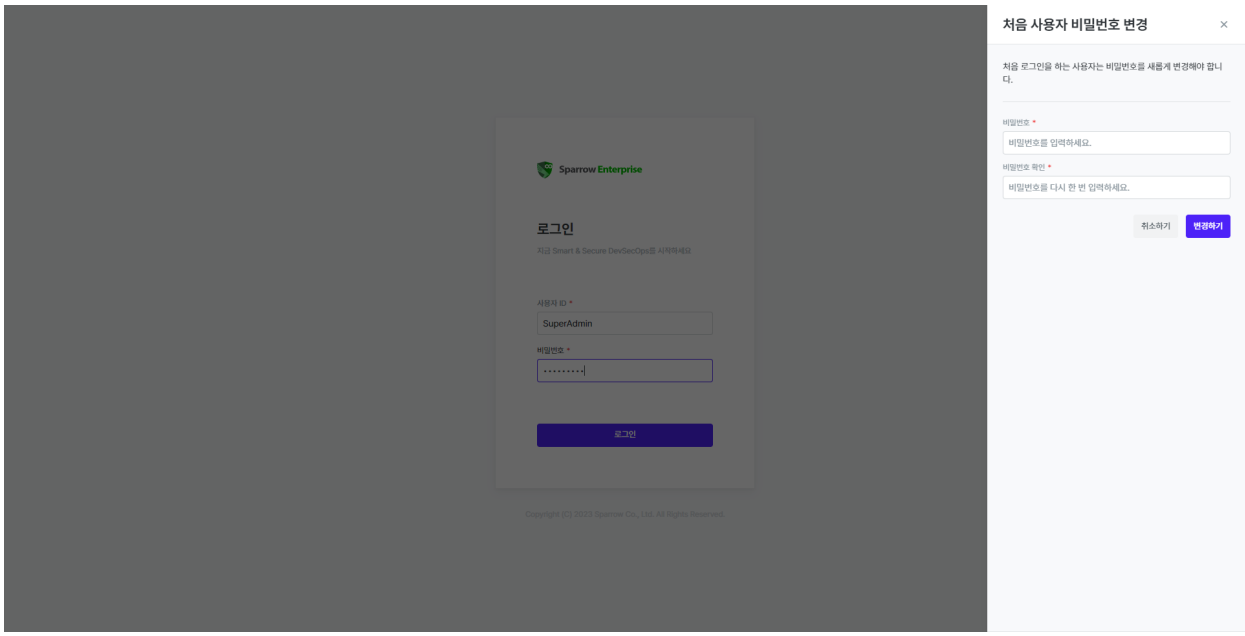
1. 웹 브라우저를 여세요.

> **Tip**: Sparrow Enterprise는 Google Chrome 웹 브라우저에 최적화되어 있습니다.

2. Sparrow Enterprise 서버 URL(**https://{Sparrow Enterprise 서버 IP 주소}:{포트 번호}**)을 입력하세요.
3. 관리자에게서 전달 받은 사용자 계정 ID와 비밀번호를 입력하고 **로그인** 버튼을 클릭하세요.



4. **처음 사용자 비밀번호 변경** 슬라이드에서 비밀번호를 변경하고 **확인** 버튼을 클릭하세요.



> **Tip**: 모든 사용자는 최초로 로그인할 때 비밀번호를 새로 설정해야 합니다.

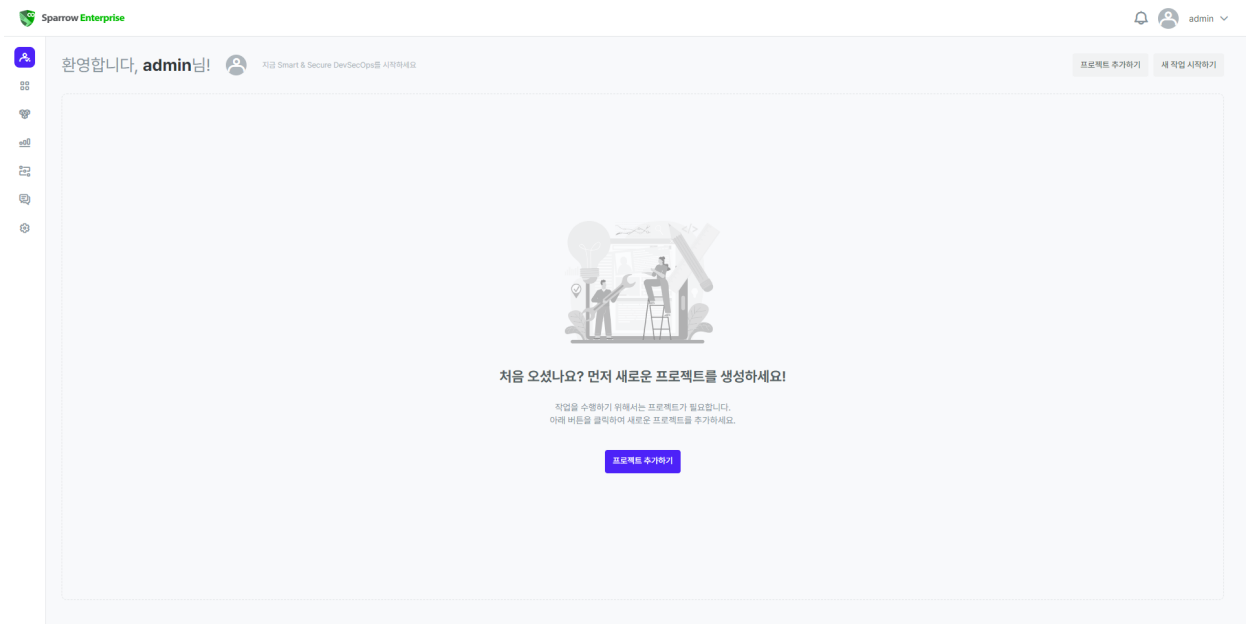
6. 이제 Sparrow Enterprise에 로그인됩니다.

새 프로젝트 만들기

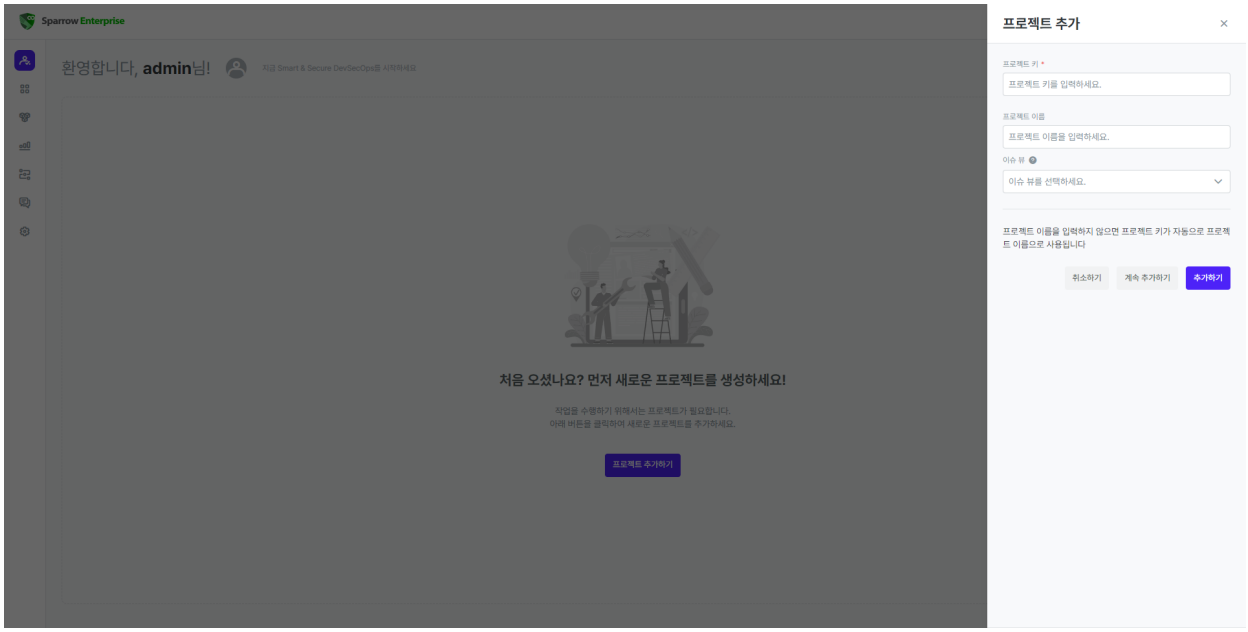
Sparrow Enterprise에서는 분석을 묶어서 프로젝트 단위로 저장합니다. 다수의 분석을 수행하는 경우 사용자가 분석을 프로젝트 단위로 쉽게 구분할 수 있습니다. 프로젝트에는 분석할 소스코드를 비롯하여 분석과 관련된 정보를 모아두었습니다. 따라서 분석을 수행하기 위해서는 이미 생성된 프로젝트를 활용하거나 먼저 프로젝트를 만들어야 합니다.

시스템의 **프로젝트 관리** 권한이 있는 관리자만 프로젝트를 새로 생성할 수 있습니다. 또한 생성된 프로젝트의 설정은 나중에 프로젝트 설정에서 다시 수정할 수 있습니다.

1. **마이페이지** 혹은 **전체 프로젝트 목록**의 오른쪽에 있는 **프로젝트 추가하기** 버튼을 클릭하세요.



2. **프로젝트 추가** 슬라이드에서 아래를 참고하여 **프로젝트 키**, **프로젝트 이름**을 입력하세요.(*는 필수 입력 항목)



3. **추가하기** 버튼을 클릭하면 추가한 프로젝트로 이동합니다.

> **Tip**: 이제 필요한 작업에 맞춰 소스코드 분석, 웹 취약점 분석, 컴포넌트 분석, 자가 방어, 테스트 케이스, 워크플로를 실행하세요.

프로젝트 키*

프로젝트를 구분하는 키이며 영문, 숫자, 하이픈(-), 밑줄(_), 마침표(.)로 최대 50자까지 입력할 수 있습니다.

> **Tip**: 프로젝트 이름을 입력하지 않으면 프로젝트 키가 자동으로 프로젝트 이름으로 사용됩니다.

프로젝트 이름

프로젝트의 이름이며 한글, 영문, 숫자, 하이픈(-), 밑줄(_), 마침표(.), 공백으로 최대 50자까지 입력할 수 있습니다. 프로젝트 키에 문자를 입력하면 동일한 문자가 자동으로 프로젝트 이름에도 입력됩니다. 다른 프로젝트 이름을 사용하려면 원하는 이름을 입력하세요.

새 작업 시작하기

이제 본격적으로 작업을 시작해봅시다. 먼저, 프로젝트에서 작업을 수행하려면 1) 프로젝트의 **프로젝트 구성원**으로써 프로젝트 권한 중 2) **작업 수행** 권한을 포함한 프로젝트 역할을 가져야 합니다.

작업 프로파일

작업에서 대상을 분석하고, 앱을 보호하고, 테스크 케이스를 확인하는 기준을 **작업 프로파일**이라는 정보에 모아두었습니다. **작업 프로파일**은 시스템의 **작업 및 규칙 관리** 권한을 가진 관리자가 특정 작업에 사용하도록 미리 설정해둡니다. 사용자는 이렇게 미리 설정한 작업 프로파일을 가져와서 그대로 작업에 적용하기만 하면 됩니다. 프로젝트 구성원으로써 주어진 역할에 따라 작업 프로파일을 사용하세요.

> **Tip**: 작업 프로파일을 설정하는 방법은 작업 프로파일 관리하기를 참고하세요.

분석

분석은 **전수 분석**과 **수시 분석**으로 구분합니다. 두 분석은 분석 결과를 업데이트하는 방식이 다릅니다. **전수 분석**은 프로젝트에서 이전에 수행한 분석의 결과를 고려하지 않고 해당 분석의 결과만 표시합니다. 따라서 프로젝트를 처음 시작할 때나 최종적으로 마무리할 때 사용하는 것이 좋습니다. 반면, **수시 분석**은 프로젝트에서 이미 수행한 전수 분석의 결과를 그대로 두고 변경된 결과만 업데이트합니다. 따라서 프로젝트를 진행하는 도중 변경되거나 추가된 내용을 재확인할 때 사용하는 것이 좋습니다.

> **Tip**: 프로젝트에서 **전수 분석을 먼저 수행해야 수시 분석을 수행할 수 있습니다**.

소스코드 분석

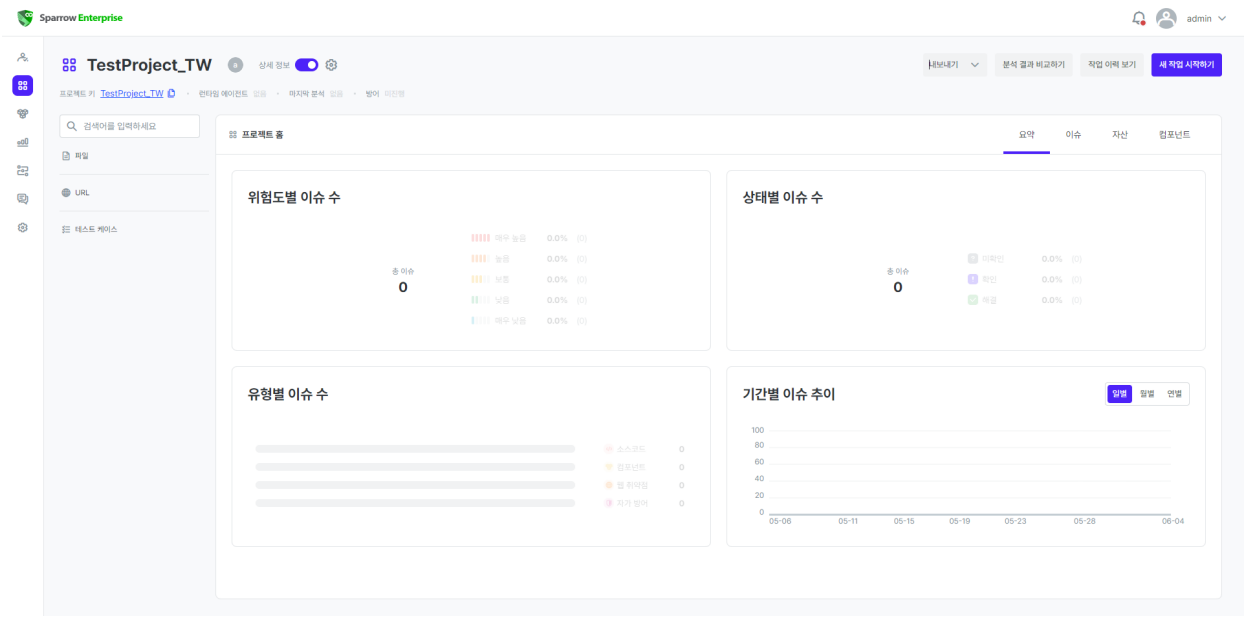
Sparrow SAST/SAQT에서는 다양한 방법의 소스코드 분석을 지원하고 있습니다. 먼저, 브라우저에서 웹 서버로 이동하여 간단히 분석을 수행할 수 있습니다. 하지만, 업로드할 수 있는 파일의 형식과 크기에 제한이 있고 개발 환경을 고려하여 분석할 수 없다는 단점이 있습니다. 클라이언트 GUI나 CLI 명령어를 사용하면 개발 환경에 따른 정확한 결과를 확인하실 수 있습니다. 클라이언트를 사용하려면 Sparrow Enterprise 클라이언트를 설치하세요. 플러그인을 설치하면 IDE에서 직접 분석을 수행할 수 있습니다. Sparrow Enterprise는 현재 Eclipse, IntelliJ 및 Visual Studio Code 플러그인을 지원합니다.

> **Tip**: 형상 관리 시스템에 Sparrow Enterprise 연동을 설정하면 파일을 푸시할 때 해당 파일의 해시값을 확인하여 커밋을 거절하거나 혹은 승인하도록 제어할 수 있습니다. 자세한 내용은 스패로우 엔지니어에게 문의하세요.

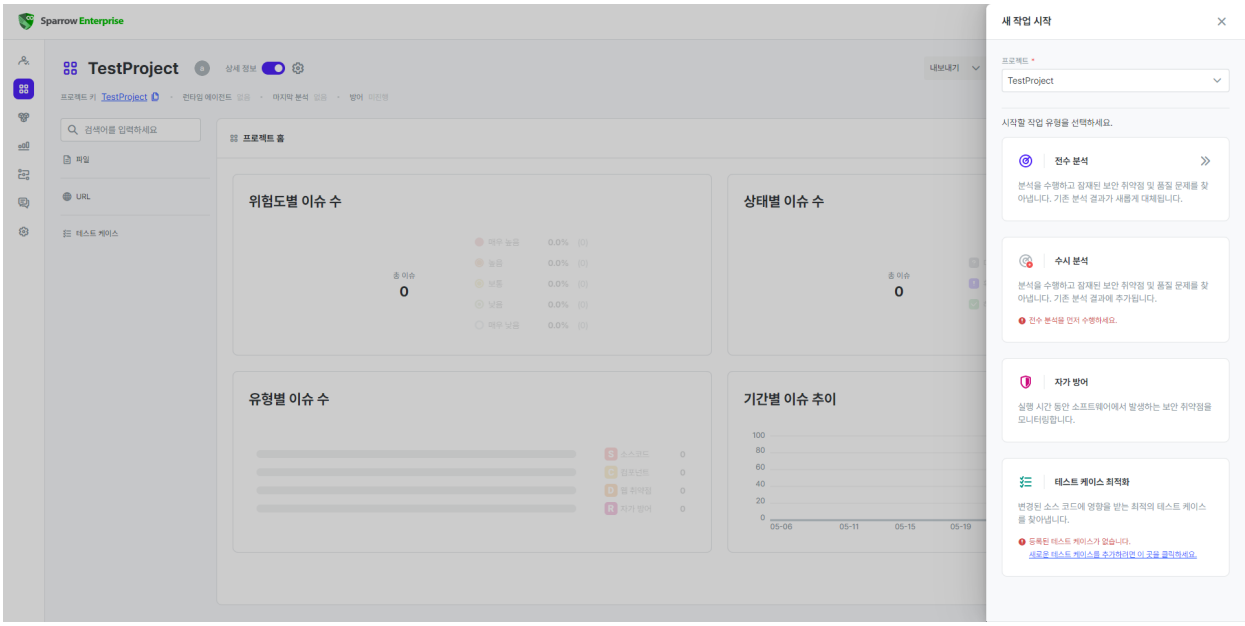
웹 서버에서 소스코드 분석

웹 서버에서 소스코드를 분석하는 방법은 다음과 같습니다.

1. **웹 서버**에 로그인하고 분석하려는 프로젝트를 클릭하세요.

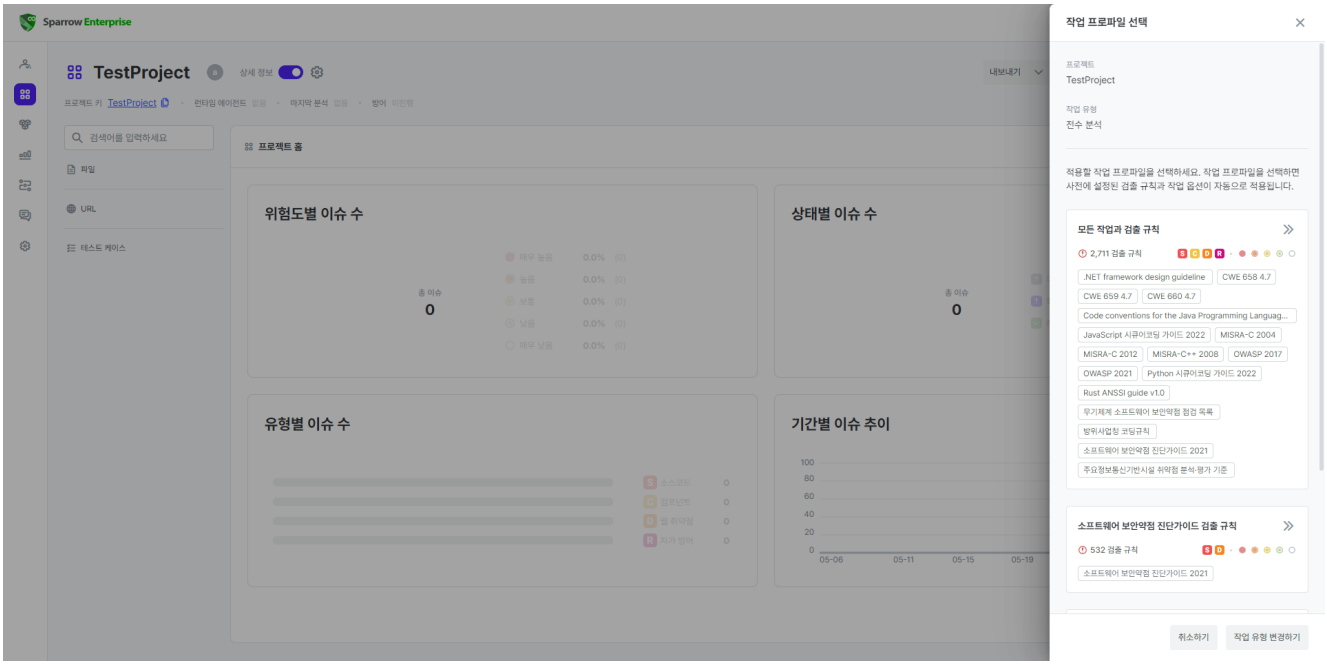


2. **새 작업 시작하기** 버튼을 클릭하세요.



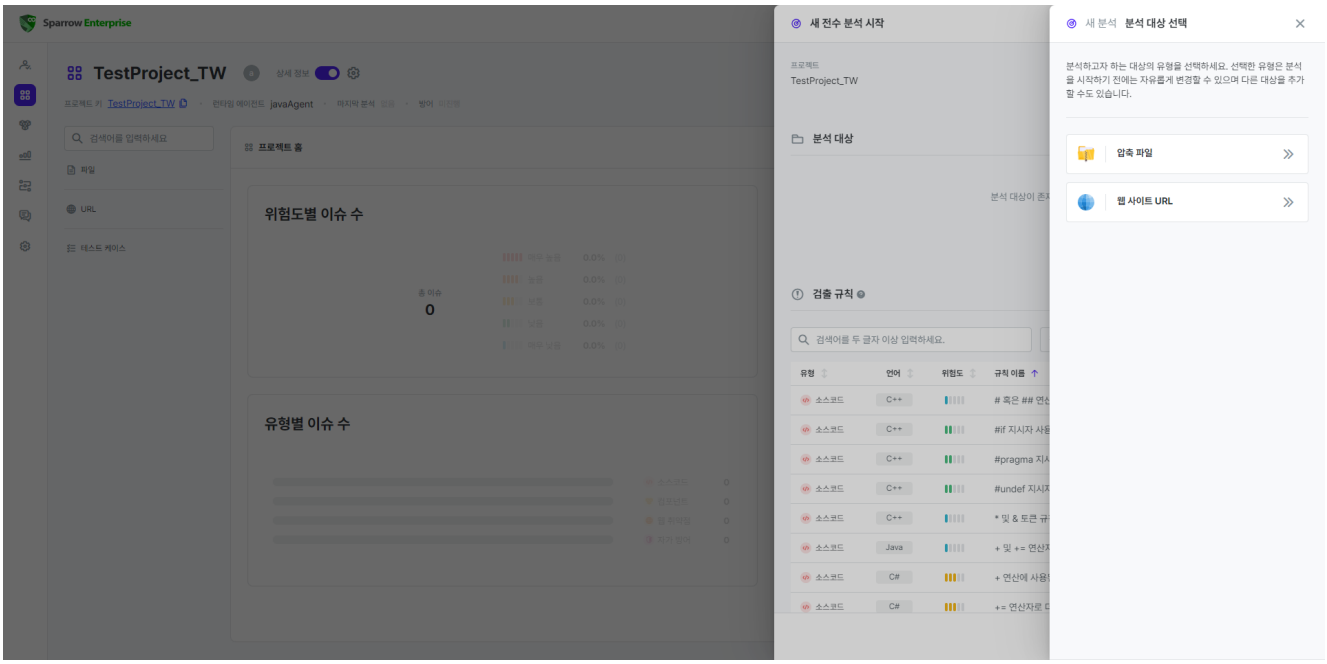
3. **전수 분석** 또는 **수시 분석** 카드를 클릭하세요.

> **Tip**: **전수 분석**과 **수시 분석**에 대한 설명은 분석을 참고하세요.

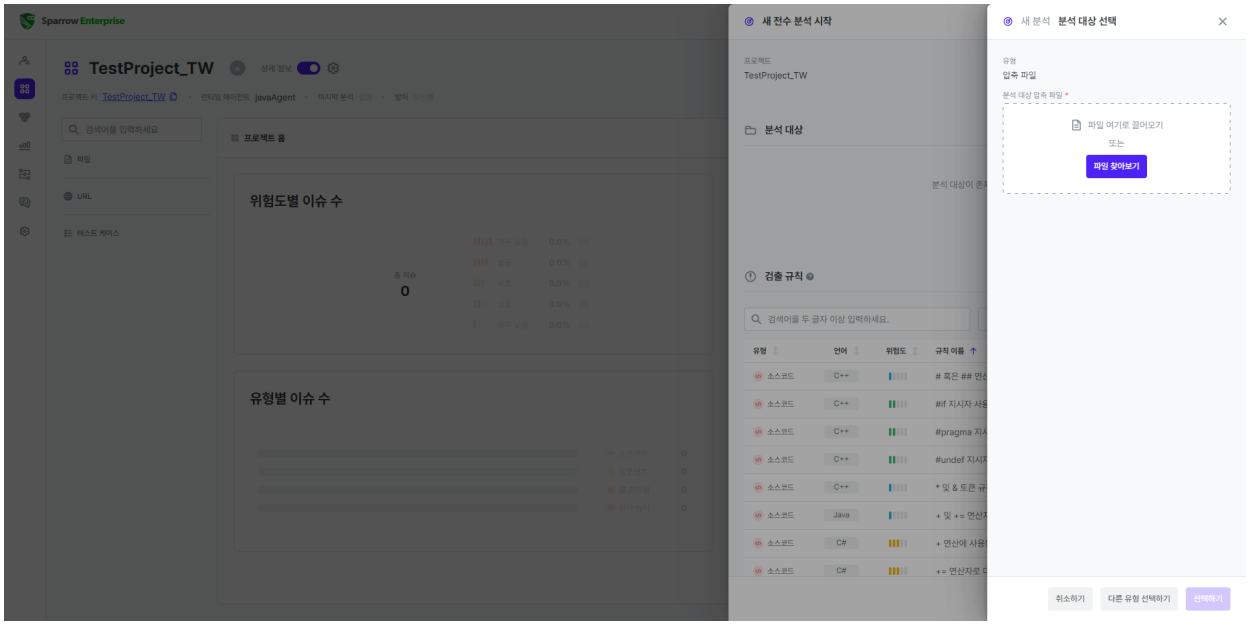


4. **작업 프로파일**을 선택하세요.

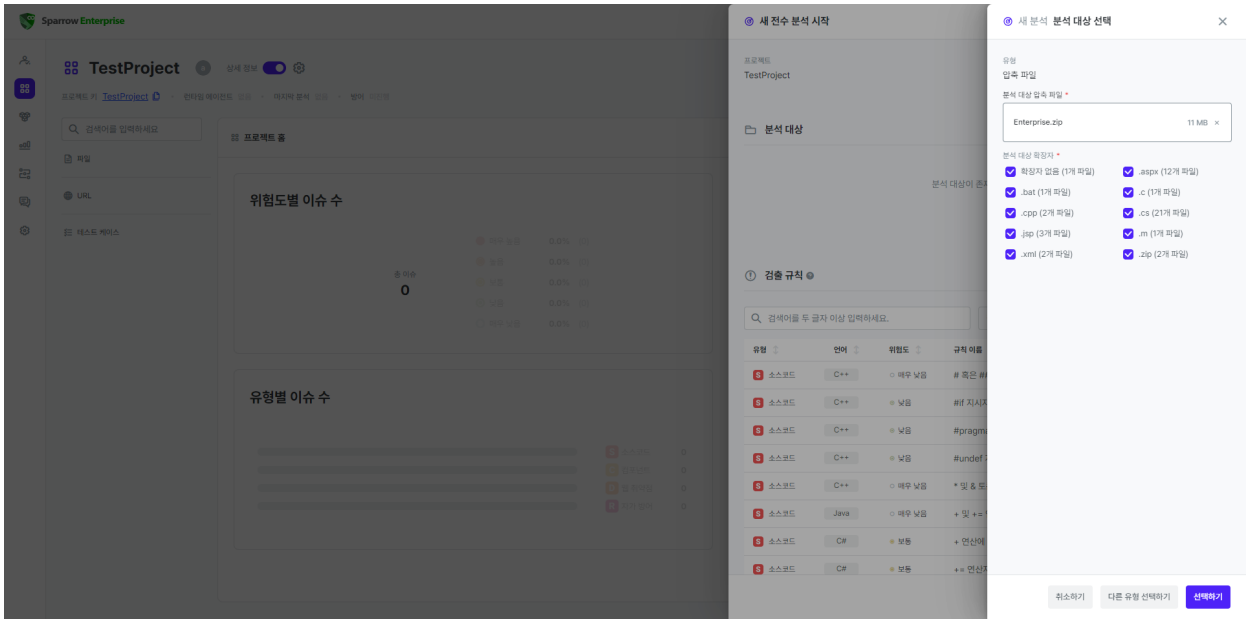
> **Tip**: **작업 프로파일**은 이슈 검출 규칙과 작업 옵션 등 작업에 필요한 정보를 모아둔 데이터입니다. 자세한 내용은 작업 프로파일을 참고하세요.



5. **분석 대상** 중에서 **압축 파일**을 선택하세요.

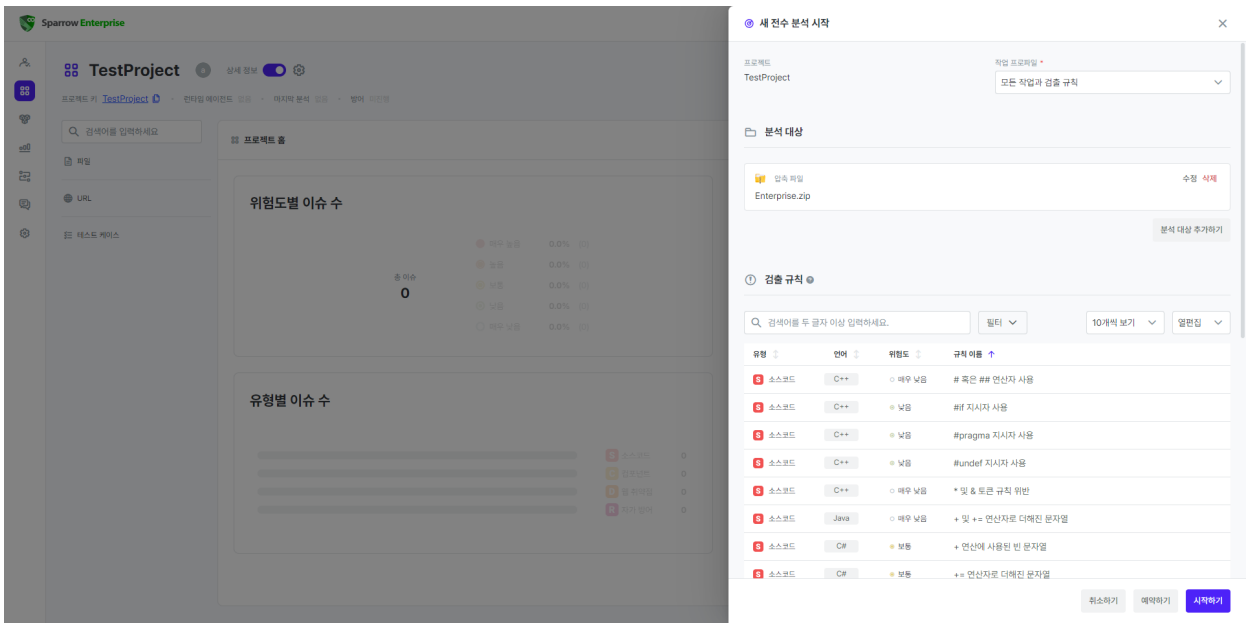


6. **분석 대상 압축 파일**에서 분석할 파일을 끌어오거나 **파일 찾아보기**를 클릭하여 파일을 선택하세요.



7. 분석할 언어의 파일 확장자를 선택하세요.

8. **선택하기** 버튼을 클릭하세요.



9. **시작하기** 버튼을 클릭하세요.

> **Tip**: 웹 서버에서는 zip 형식의 파일만 분석할 수 있습니다. 나머지 형식의 파일을 분석하려면 클라이언트 GUI: 소스코드 분석하기 혹은 클라이언트 CLI: 소스코드 분석하기를 참고하세요.

클라이언트 GUI로 소스코드 분석

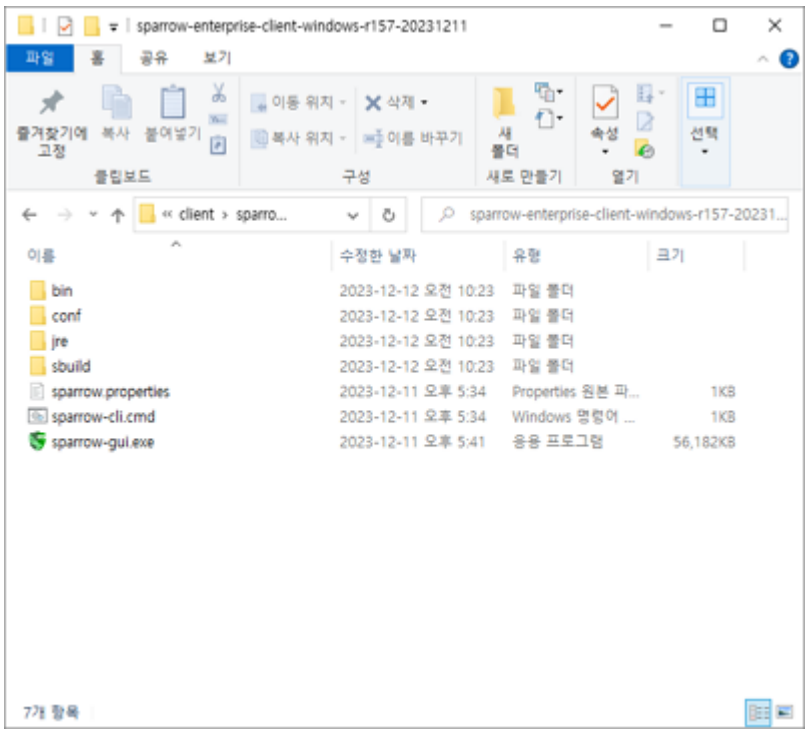
클라이언트 GUI: 로그인하기

클라이언트 GUI를 실행하기 위해서는 **Sparrow Enterprise 클라이언트**를 설치해야 합니다. 또한 사용자가 **Sparrow Enterprise 서버**에 먼저 로그인하지 않았다면 클라이언트에서도 로그인할 수 없습니다.

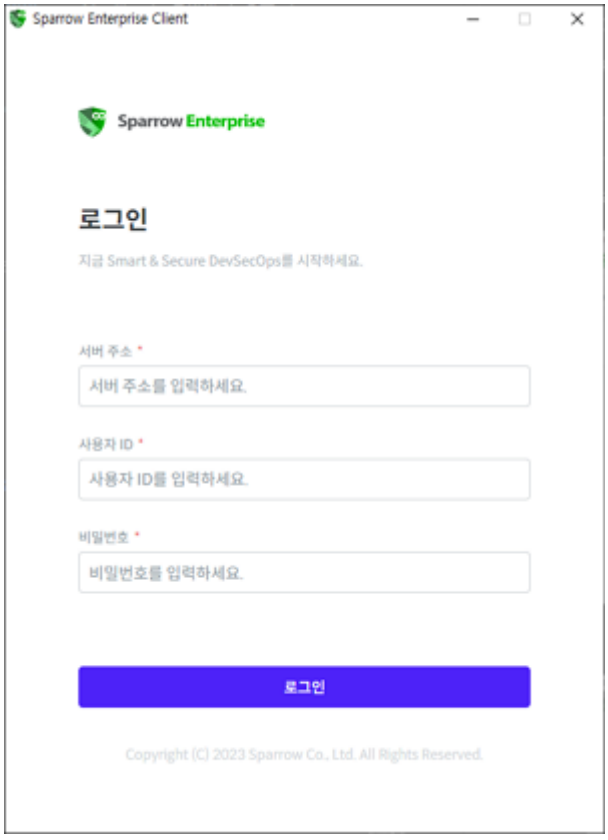
> **Warning**: Sparrow Enterprise를 처음 사용하는 사용자는 **Sparrow Enterprise 서버**에 먼저 로그인하여 비밀번호를 변경한 후, 변경한 비밀번호로 클라이언트에 로그인하세요.

Sparrow Enterprise 클라이언트 GUI에 로그인하는 방법은 다음과 같습니다.

1. **{Sparrow Enterprise 클라이언트 설치 디렉토리}**로 이동하세요.



2. **sparrow-gui.exe** 파일을 실행하세요.



3. Sparrow Enterprise의 **서버 주소**, **사용자 ID**, **비밀번호**를 입력하세요.

> **Tip**: 서버 주소에는 **https://{Sparrow Enterprise 서버 IP 주소}:{포트 번호}**를 입력해야 합니다.
> **Sparrow Enterprise 서버**를 기본값으로 설치하신 경우 포트 번호는 **10880**입니다.

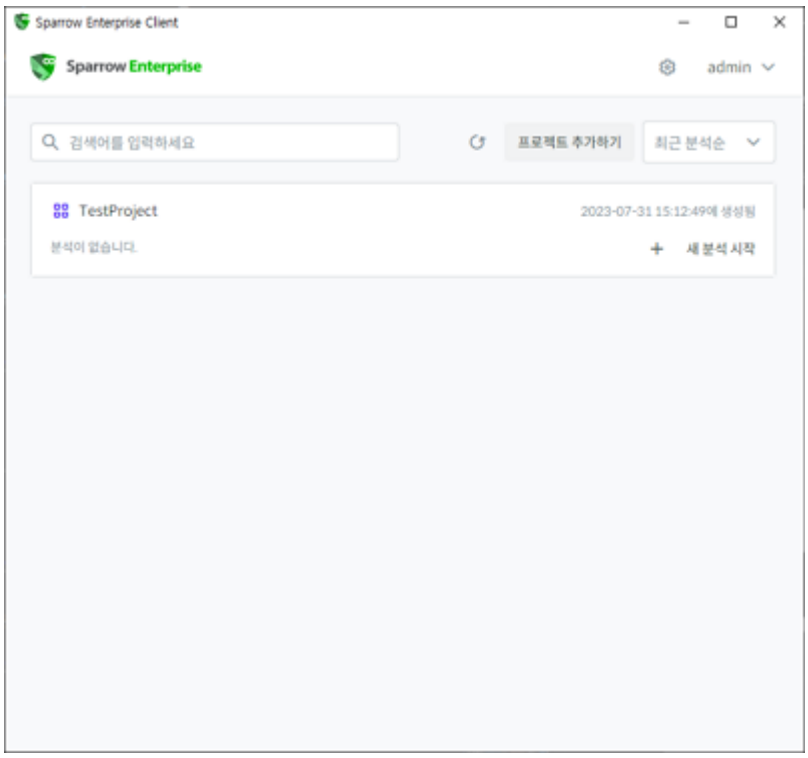
3. **로그인** 버튼을 클릭하세요.

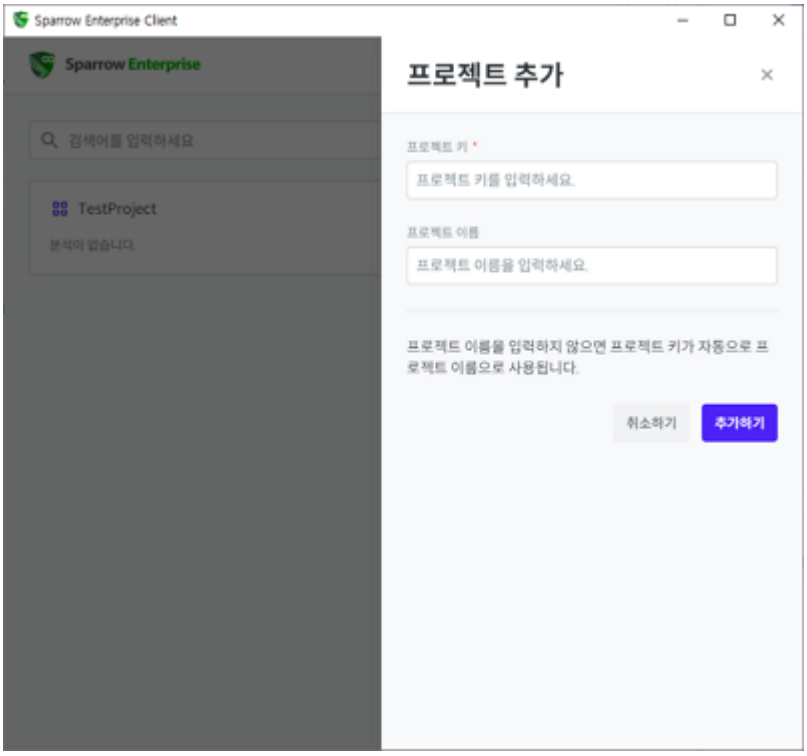
그러면 **Sparrow Enterprise 클라이언트 GUI**에 로그인하게 됩니다.

클라이언트 GUI: 소스코드 분석하기

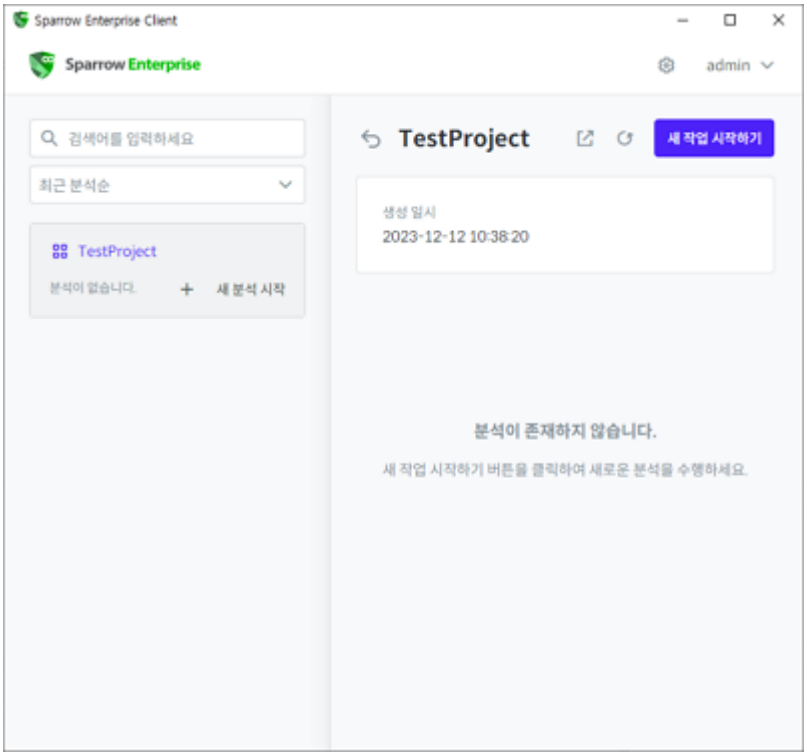
클라이언트 GUI를 통해 소스코드를 분석하는 방법은 다음과 같습니다.

1. **클라이언트 GUI**의 프로젝트 목록에서 분석할 프로젝트를 선택하거나 새로운 프로젝트를 추가하세요.

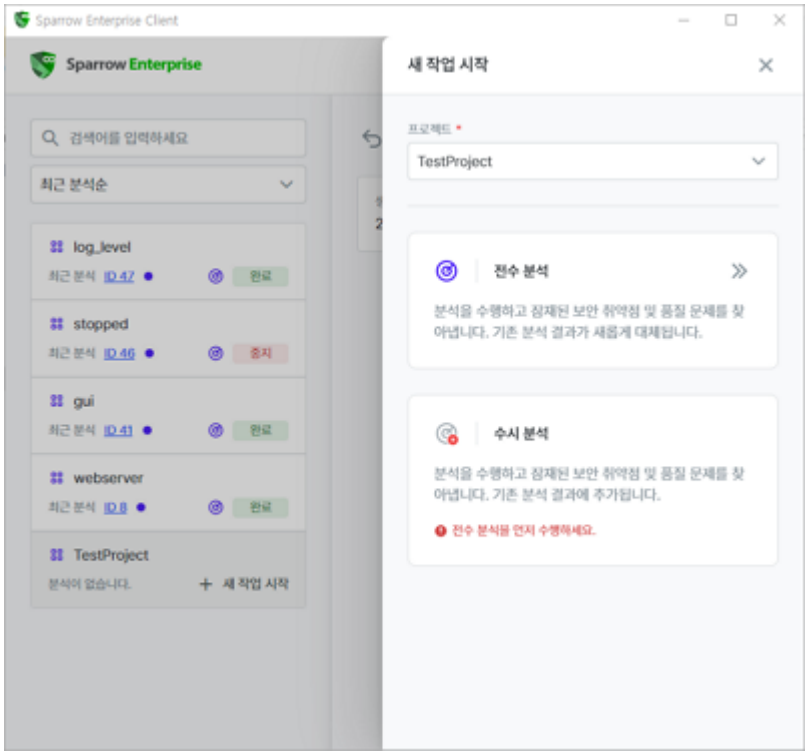




2. 프로젝트로 이동하세요.

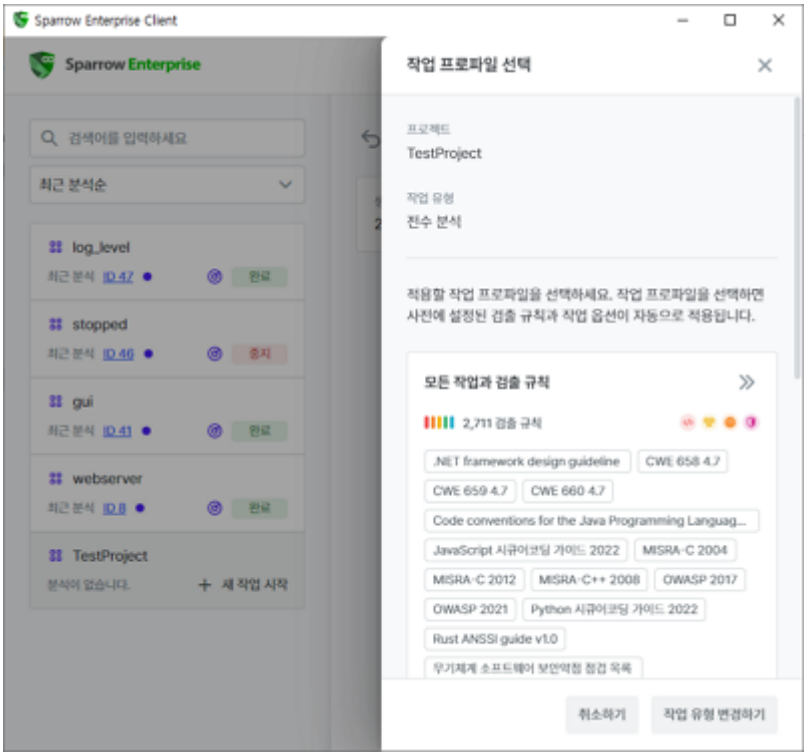


3. **새 작업 시작하기** 버튼을 클릭하세요.



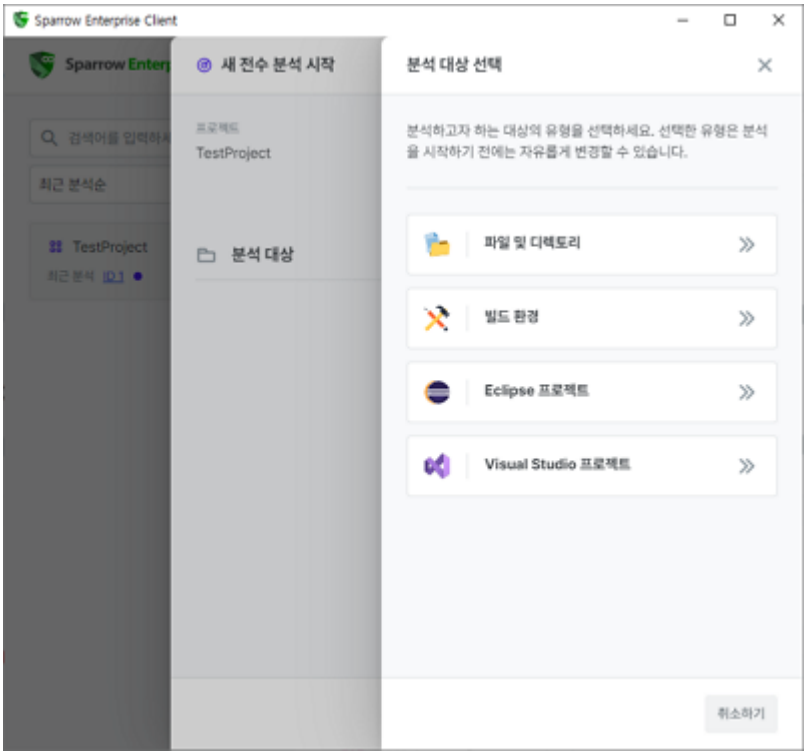
4. **전수 분석** 또는 **수시 분석** 카드를 클릭하세요.

> **Tip**: **전수 분석**과 **수시 분석**에 대한 설명은 분석을 참고하세요.



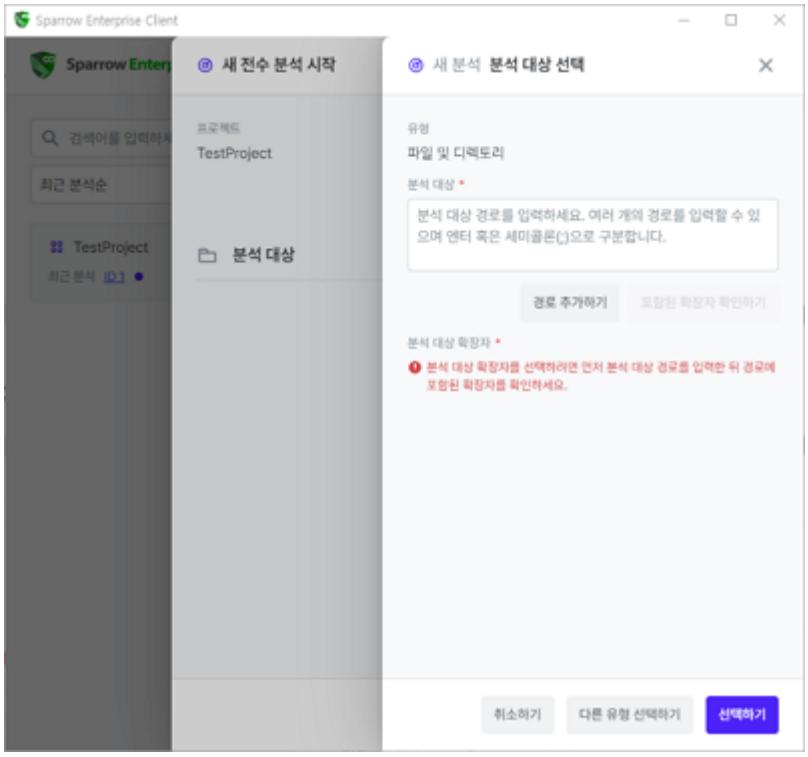
5. **작업 프로파일**을 선택하세요.

> **Tip**: **작업 프로파일**은 이슈 검출 규칙과 작업 옵션 등 작업에 필요한 정보를 모아둔 데이터입니다. 자세한 내용은 작업 프로파일을 참고하세요.

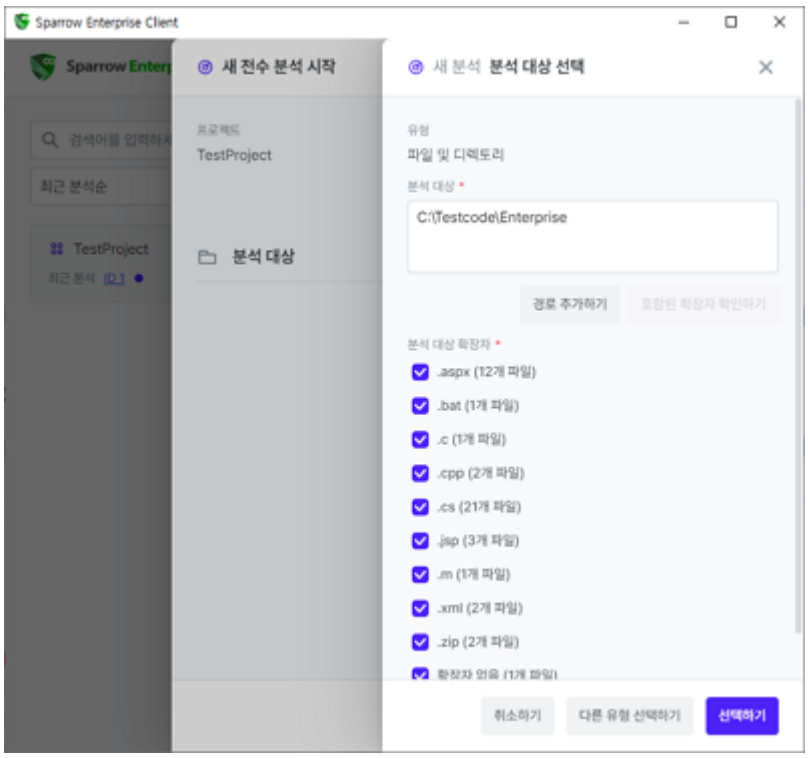


6. 분석하려는 대상에 따라 **파일 및 디렉토리**, **빌드 환경**, **Eclipse 프로젝트**, **Visual Studio 프로젝트** 중 하나를 클릭하세요.

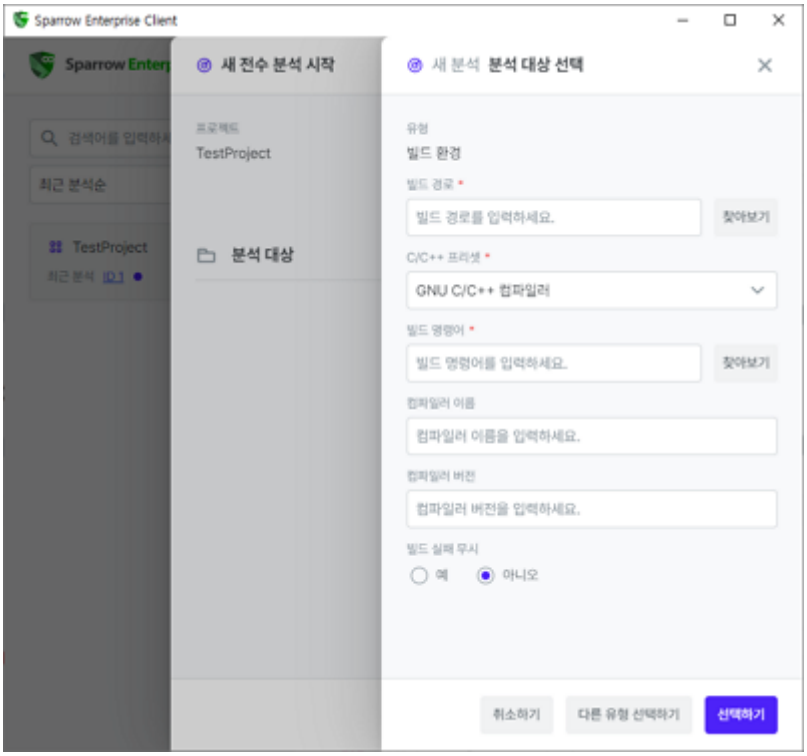
7. **파일 및 디렉토리**를 선택한 경우 **분석 대상**에 분석할 파일의 경로를 직접 입력하거나 **경로 추가하기** 버튼을 클릭하여 폴더를 선택하세요.



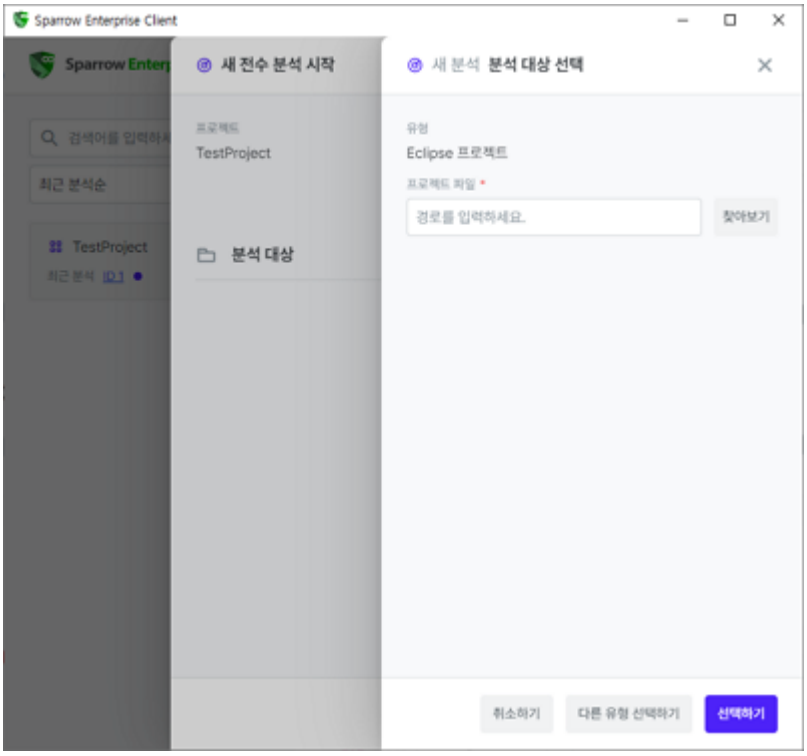
8. **포함된 확장자 확인하기** 버튼을 클릭하면 위에서 선택한 파일에 포함된 파일 형식이 **분석 대상 확장자**에 표시됩니다. 그 중에 분석할 파일의 확장자를 선택하고 **선택하기** 버튼을 클릭하세요.



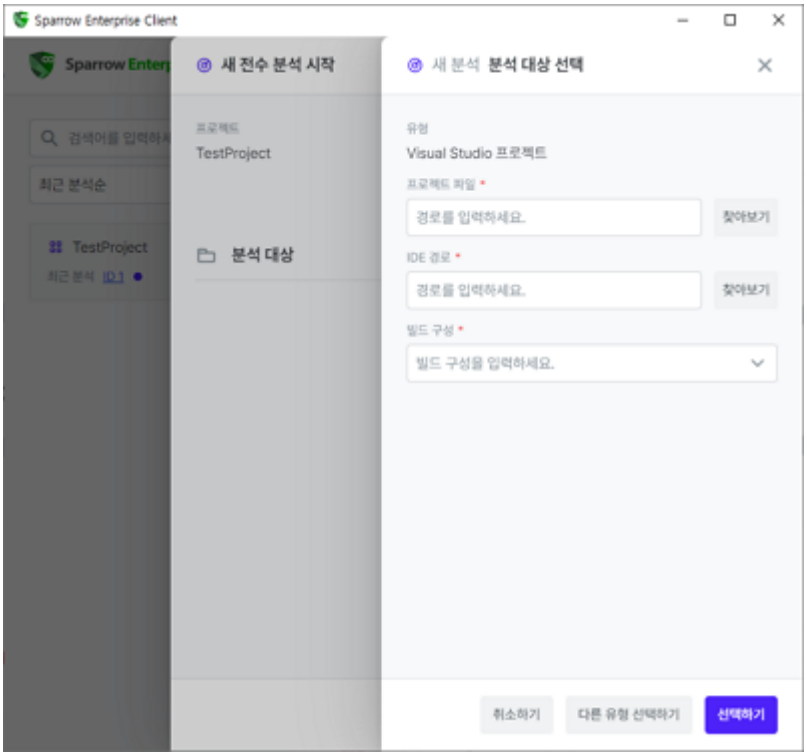
9. 분석하려는 대상이 **빌드 환경**인 경우 **빌드 경로**, **C/C++ 프리셋**, **빌드 명령어**, **컴파일러 이름**, **컴파일러 버전**, **빌드 실패 무시** 등 추가적으로 입력해야 하는 옵션이 표시됩니다. 이 옵션은 컴파일러 혹은 IDE 도구를 미리 설치한 경우에 정상적으로 분석에 사용할 수 있습니다. 자세한 내용은 아래 내용을 참고하세요. 옵션을 입력하고 **선택하기** 버튼을 클릭하세요. (*는 필수 입력 항목)



10. 분석 대상으로 **Eclipse 프로젝트**를 선택한 경우 **프로젝트 파일**을 선택하고 **선택하기** 버튼을 클릭하세요.

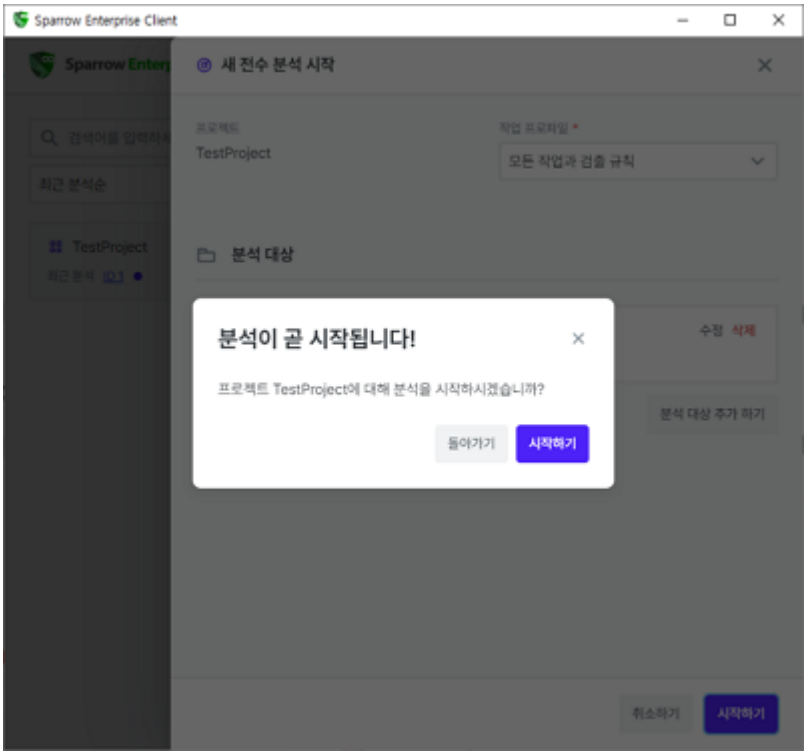


11. **Visual Studio 프로젝트**를 분석하려는 경우 **프로젝트 파일**, **IDE 경로**, **빌드 구성**을 선택하세요. 이 옵션은 Visual Studio를 미리 설치한 경우에 정상적으로 분석에 사용할 수 있습니다. 자세한 내용은 아래 내용을 참고하세요. 옵션을 입력하고 **선택하기** 버튼을 클릭하세요. (*는 필수 입력 항목)



12. **시작하기** 버튼을 클릭하세요.

13. **프로젝트에 대해 분석을 시작하시겠습니까?**라는 메시지에 **시작하기** 버튼을 클릭하면 작업이 시작됩니다.



✓ 파일 및 디렉토리

분석 대상*

취약점 및 품질 문제를 포함하는 이슈를 분석할 대상인 소스코드의 파일 혹은 디렉토리 경로입니다. 분석을 시작하기 전에 하나 이상의 경로를 입력하고 엔터로 구분할 수 있습니다.

분석 대상 확장자*

분석 대상에 포함된 분석 대상 파일의 확장자이며 하나 이상의 확장자를 선택할 수 있습니다. 이렇게 확장자를 선택함으로써 **분석 대상**에 존재하는 파일의 소스코드에서 해당하는 언어만 분석하도록 지정하게 됩니다.

✓ 빌드 환경

빌드 경로

C/C++ 언어를 분석하는 경우 사용할 빌드를 수행할 경로입니다. 빌드 경로를 직접 입력하거나, **찾아보기** 버튼을 클릭하여 폴더를 선택할 수 있습니다.

C/C++ 프리셋

C/C++ 언어를 분석하는 경우 사용할 프리셋입니다. C/C++ 언어의 컴파일러 혹은 IDE 도구가 프리셋으로 지정되어 있습니다.

현재 버전에서는 GNU C/C++ 컴파일러만 선택할 수 있습니다.

빌드 명령어

C/C++ 언어를 분석하는 경우 사용할 빌드 명령어입니다. 빌드 명령어를 직접 입력하거나 **찾아보기** 버튼을 클릭하여 파일을 선택할 수 있습니다. 선택한 파일은 기본적으로 **exe, bat, com, cmd**와 같은 실행 파일

로 지정됩니다.

컴파일러 이름

빌드 환경에서 사용한 컴파일러의 이름입니다. 특정한 컴파일러를 사용해서 C/C++ 언어의 소스코드를 빌드한 경우 입력하면 됩니다. 이 옵션에 값을 입력하지 않으면 사용자가 입력한 C/C++ 프리셋 옵션에 해당하는 컴파일러 이름을 사용하게 됩니다.

컴파일러 버전

빌드 환경에서 사용한 컴파일러의 버전입니다. 특정한 컴파일러를 사용해서 C/C++ 언어의 소스코드를 빌드한 경우 입력하면 됩니다. 이 옵션에 값을 입력하지 않으면 사용자가 입력한 C/C++ 프리셋 옵션에 해당하는 컴파일러 버전을 사용하게 됩니다

빌드 실패 무시

C/C++ 언어를 분석하는 경우 빌드 단계에서 실패가 발생하더라도 분석을 계속 진행하도록 강제하는 분석 방법을 의미하며 예, 아니요로 구분합니다.

이 옵션을 예로 설정하면 **빌드가 실패하더라도 무시하고 분석을 계속 진행**합니다. 따라서 빌드 실패로 인해 분석이 실패하지 않게 됩니다. 이 옵션을 아니요로 설정하면 **빌드가 실패하는 경우 자동으로 분석도 실패**하게 됩니다. 따라서 분석을 수행하지 못할 가능성이 있지만 빌드가 정상적으로 이루어졌는지를 확인할 수 있습니다.(기본값: 아니요)

✓ Eclipse 프로젝트

프로젝트 파일*

소스코드를 분석할 Eclipse 프로젝트 파일인 **.project** 파일의 디렉토리 경로입니다. 하나의 경로만 입력할 수 있습니다.

✓ Visual Studio 프로젝트

프로젝트 파일*

소스코드를 분석할 Visual Studio 프로젝트 파일인 **.project** 파일의 디렉토리 경로입니다. 하나의 경로만 입력할 수 있습니다.

IDE 경로*

프로젝트 파일 옵션에 입력한 Visual Studio 프로젝트 파일을 작성한 Visual Studio의 설치 경로입니다. Visual Studio 버전을 다수 설치하고 사용하는 경우 정확한 버전의 Visual Studio를 선택하도록 주의하세요.

이 옵션은 클라이언트 GUI 설정의 **IDE 경로**에서 저장한 값을 자동으로 가져옵니다. 자세한 내용은 Sparrow Enterprise 클라이언트 환경 설정하기를 참고하세요.

빌드 구성*

Visual Studio 프로젝트 파일을 빌드할 때 구성을 의미합니다. **프로젝트 파일** 혹은 **IDE 경로**를 선택하는 경우 자동으로 입력됩니다.

클라이언트 CLI로 소스코드 분석

클라이언트 CLI로 분석을 수행하는 경우 웹 서버를 사용하는 것보다 제한 없이 분석을 수행할 수 있습니다. 또한 클라이언트 GUI와 달리 GUI 기반이 아닌 OS를 사용하는 장치에서 사용하기에 적합합니다. CLI는 클라이언트 분석 방법 중에 하나이며 Sparrow Enterprise 클라이언트를 설치할 때 함께 설치됩니다. 클라이언트를 설치하는 방법은 Sparrow Enterprise 클라이언트 설치하기를 참고하세요.

> **Tip**: **-h 또는 --help** 옵션과 함께 Sparrow Enterprise 클라이언트 CLI 파일을 실행하면 명령어에 대한 도움말을 확인할 수 있습니다.

클라이언트 CLI: 새 프로젝트 추가하기

Sparrow Enterprise 클라이언트 CLI에서 새로운 프로젝트를 추가하려면 다음을 수행하세요.

1. 명령 프롬프트를 실행하세요.
2. {Sparrow Enterprise 클라이언트 설치 디렉토리}로 이동하세요.
3. Linux 환경에서는 **sparrow-cli** 파일과 `create project` 명령어 및 **옵션**을 입력하세요.

```
./sparrow-cli create project -f /home/user/workspace/project.json -s
https://localhost:10880 -u admin -p /home/user/workspace/password.txt
```

4. Windows 환경에서는 **sparrow-cli.cmd** 파일과 `create project` 명령어 및 **옵션**을 입력하세요.

```
sparrow-cli.cmd create project -f C:\workspace\project.json -s
https://localhost:10880 -u admin -p C:\workspace\password.txt
```

5. 아래 내용을 참고하여 **옵션**을 입력하고 실행하세요.(*는 필수 입력 항목)

-f 또는 --file*

추가할 프로젝트의 설정을 입력한 JSON 파일의 경로입니다. 해당 파일에는 **프로젝트 키(key)**, **프로젝트 이름(name)**을 다음과 같은 형식으로 입력해야 합니다.(예시: `-f {JSON 파일 경로}.json`)

```
{
    "key": "myapp",
    "name": "my-application"
}
```

JSON 파일에서 **프로젝트 키(key)**는 필수 입력 항목입니다. **프로젝트 이름(name)**을 입력하지 않으면 프로젝트 키가 자동으로 프로젝트 이름으로 사용됩니다.

-s 또는 --server*

연결하려는 Sparrow Enterprise 서버의 IP 주소 및 포트 번호입니다.(예시: `-s {Sparrow Enterprise 서버 IP 주소}:{포트 번호}`)

-u 또는 -–user*

프로젝트를 추가하려는 사용자 계정의 ID입니다.(예시: `-u {사용자 ID}`)

-p 또는 -–password

분석을 수행하려는 사용자 계정의 비밀번호를 저장한 txt 파일의 위치입니다. 이 옵션에 값을 입력하지 않은 경우 사용자 계정의 비밀번호를 입력하라는 메시지가 추가로 표시되며 해당 메시지에 비밀번호를 입력하면 됩니다.(예시: `-p {txt 파일 경로}`)

클라이언트 CLI: 소스코드 분석하기

Sparrow Enterprise 클라이언트 CLI에서 분석 작업을 수행하는 방법은 다음과 같습니다.

1. 명령 프롬프트를 실행하세요.
2. {Sparrow Enterprise 클라이언트 설치 디렉토리}로 이동하세요.
3. Linux 환경에서는 **sparrow-cli** 파일과 `create analysis` 명령어 및 **옵션**을 입력하세요.

```
./sparrow-cli create analysis -k myapp -f /home/user/workspace/sast.json -s
https://localhost:10880 -u admin -p /home/user/workspace/password.txt
```

4. Windows 환경에서는 **sparrow-cli.cmd** 파일과 `create analysis` 명령어 및 **옵션**을 입력하세요.

```
sparrow-cli.cmd create analysis -k myapp -f C:\workspace\sast.json -s
https://localhost:10880 -u admin -p C:\workspace\password.txt
```

5. 아래 내용을 참고하여 **옵션**을 입력하고 실행하세요.(*는 필수 입력 항목)

-k 또는 --key*

분석 작업을 수행할 프로젝트의 프로젝트 키입니다.(예시: `-k {프로젝트 키}`)

-f 또는 --file*

수행할 분석의 설정을 입력한 JSON 파일의 경로입니다. 해당 파일에는 다음과 같은 정보가 포함되어야 합니다.(예시: `-f {JSON 파일 경로}`)

아래의 형식에서 **작업 유형(`type`)**은 작업의 유형을 **전수 분석(`full`)**, **수시 분석(`adhoc`)** 중 하나로 입력할 수 있습니다. **작업 프로파일(`profile`)**은 설정한 작업 프로파일 중 하나를 입력할 수 있습니다. **분

석 대상(targets)**의 **유형(type)**은 파일 및 디렉토리(file), 빌드 환경(build), Eclipse 프로젝트(eclipse), Visual Studio 프로젝트(vs) 중 하나를 입력할 수 있습니다. 또한, **분석 대상 경로(path)**는 분석 대상의 절대 경로입니다.

```
{
    "type": "full",
    "profile": "내 작업 프로파일",
    "targets": [{
        "type": "file",
        "path": [
            "C:\\workspace\\src\\all"
        ],
        "extensions": [
            "java", "jsp", "cpp"
        ]
    }]
}
```

분석 대상의 **유형(type)**이 파일 및 디렉토리(file)인 경우 **분석 대상 경로(path)**에 해당하는 파일이나 폴더를 입력하면 됩니다. **분석 대상 파일 확장자 목록(extentions)**은 분석 대상에 포함된 파일의 확장자를 입력하면 됩니다. *을 입력하는 경우 모든 확장자에 대해서 분석을 수행합니다.

```
{
    "type": "full",
    "profile": "내 작업 프로파일",
    "targets": [{
        "type": "build"
        "preset": "gnu",
        "buildCommand": "D:\\testcode\\c\\simple\\make.bat",
        "buildPath": "D:\\testcode\\git_testcode\\util\\testcode\\c\\simple",
        "ignoreBuildError": false
    }]
}
```

유형(type)이 빌드 환경(build)인 경우 **C/C++ 프리셋(preset)**, **빌드 명령어(buildCommand)**, **빌드 경로(buildPath)**, **빌드 실패 무시(ignorebuildError)**를 입력해야 합니다.

```
{
    "type": "full",
    "profile": "내 작업 프로파일",
    "targets" : [{
        "type" : "vs",
        "path": [
            "C:\\testcode\\c\\simple\\build\\simple.vcxproj"
            ],
```

```
        "buildConfiguration" : "Debug|x64",
        "idePath" : "C:\\Program Files (x86)\\Microsoft Visual
Studio\\2022\\Community\\Common7\\IDE\\devenv.com"
    }]
}
```

유형(type)이 Visual Studio 프로젝트(vs)인 경우 **분석 대상 경로(path), 빌드 구성(buildConfiguration)** 및 **IDE 경로(idePath)**를 입력해야 합니다. 단, **IDE 경로(idePath)**는 devenv.com 파일의 경로를 의미합니다.

```
{
    "type": "full",
    "profile": "내 작업 프로파일",
    "targets": [{
        "type": "eclipse",
        "path": [
            "C:\\workspace\\src\\all\\testProject.project"
            ]
    }]
}
```

유형(type)이 Eclipse 프로젝트(eclipse)인 경우 **분석 대상 경로(path)**를 입력해야 합니다.

-s 또는 --server*

연결하려는 Sparrow Enterprise 서버의 IP 주소 및 포트 번호입니다.(예시: -s {Sparrow Enterprise 서버 IP 주소}:{포트 번호})

-u 또는 -–user*

분석을 수행하려는 사용자 계정의 ID입니다.(예시: -u {사용자 ID})

-p 또는 -–password

분석을 수행하려는 사용자 계정의 비밀번호를 저장한 txt 파일의 위치입니다. 이 옵션에 값을 입력하지 않은 경우 사용자 계정의 비밀번호를 입력하라는 메시지가 추가로 표시되며 해당 메시지에 비밀번호를 입력하면 됩니다.(예시: -p {txt 파일 경로})

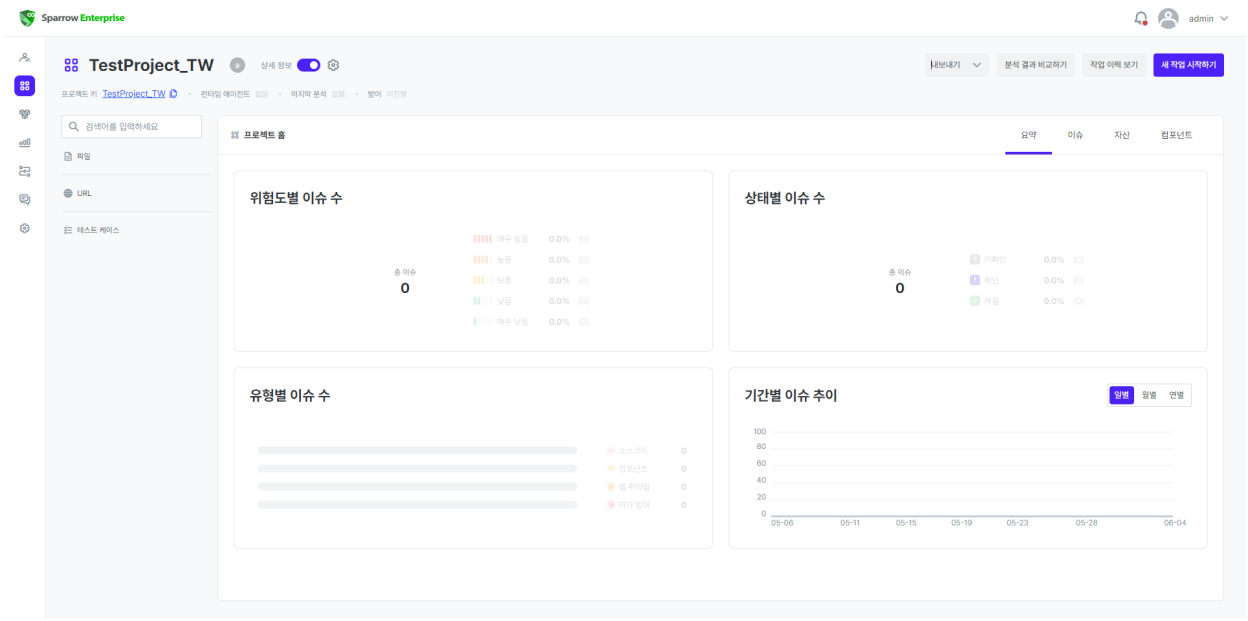
소스코드 분석에서 검출한 이슈를 확인하려면 소스코드 이슈를 참고하세요.

작업 예약

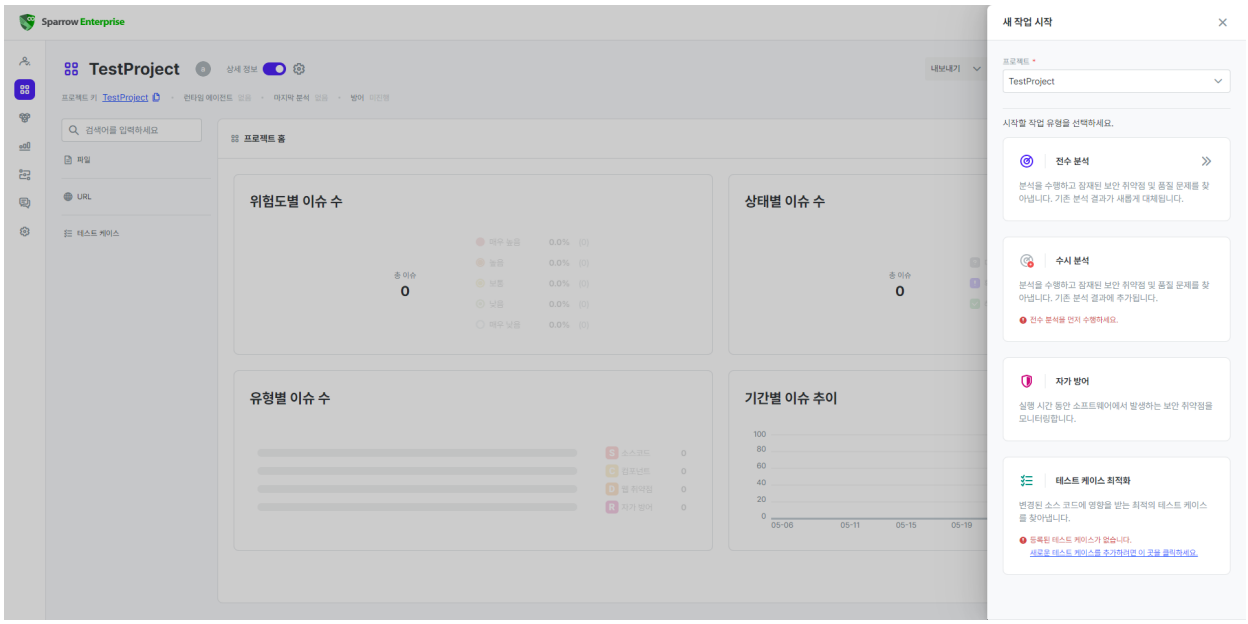
특정 대상을 일정한 시간마다 분석하거나 서버의 부하가 높은 시간을 피해서 분석을 수행하려는 경우 **작업 예약** 기능을 사용할 수 있습니다.

> **Tip**: 현재 **웹 서버에서만 소스코드 분석과 웹 취약점 분석을 대상**으로 작업 예약을 사용할 수 있습니다.

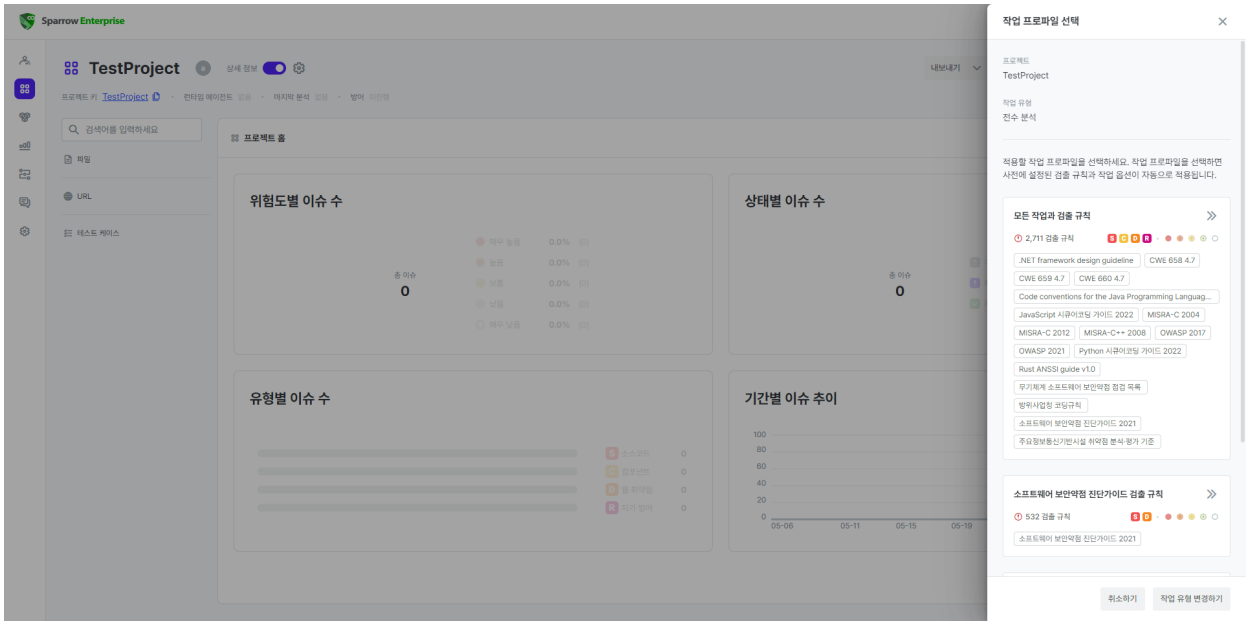
1. 웹 브라우저에서 분석하려는 프로젝트로 이동하세요.



2. **새 작업 시작하기** 버튼을 클릭하세요.



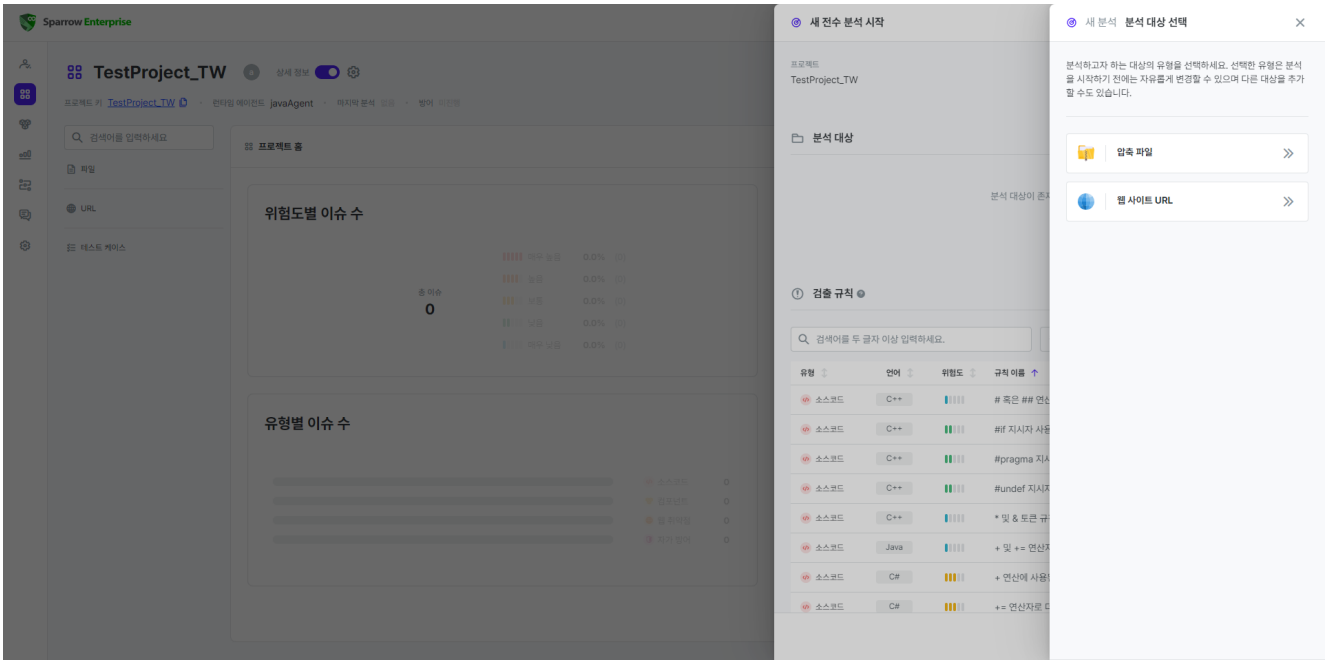
3. **전수 분석** 또는 **수시 분석** 카드를 클릭하세요.



> **Tip**: **전수 분석**과 **수시 분석**에 대한 설명은 분석을 참고하세요.

4. **작업 프로파일**을 선택하세요.

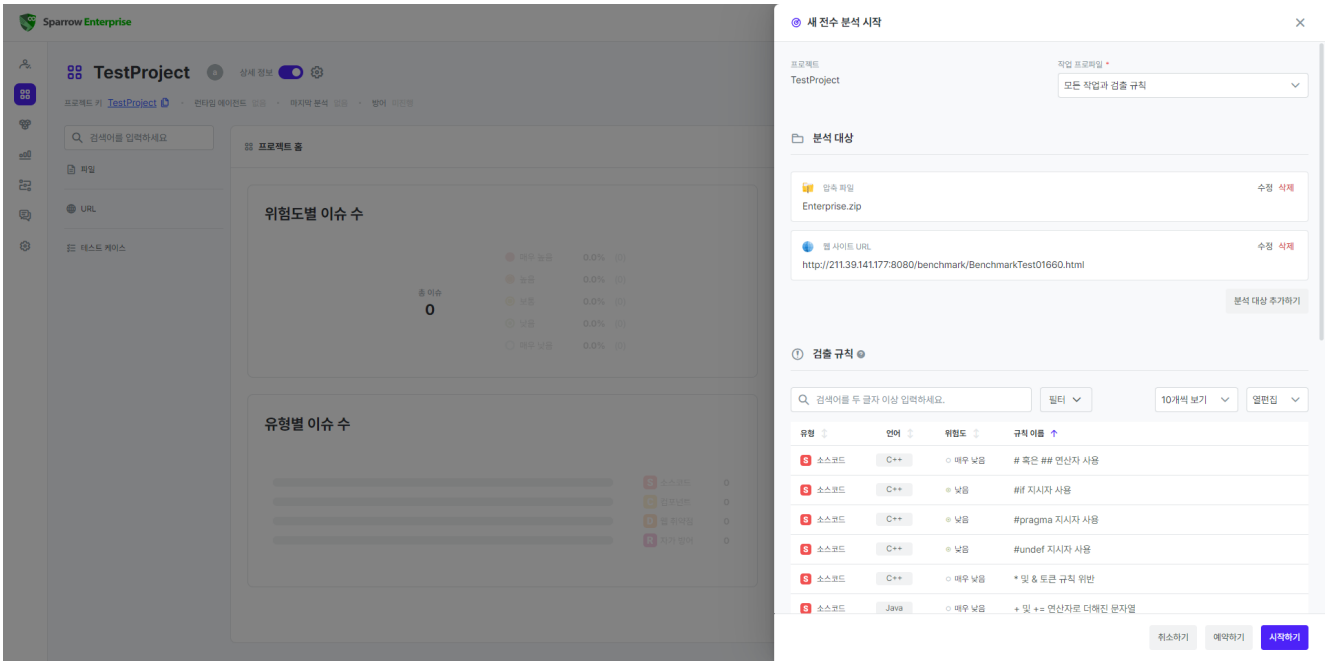
> **Tip**: **작업 프로파일**은 이슈 검출 규칙과 작업 옵션 등 작업에 필요한 정보를 모아둔 데이터입니다. 자세한 내용은 작업 프로파일을 참고하세요.



5. **압축 파일** 또는 **웹 사이트 URL**을 선택하세요.

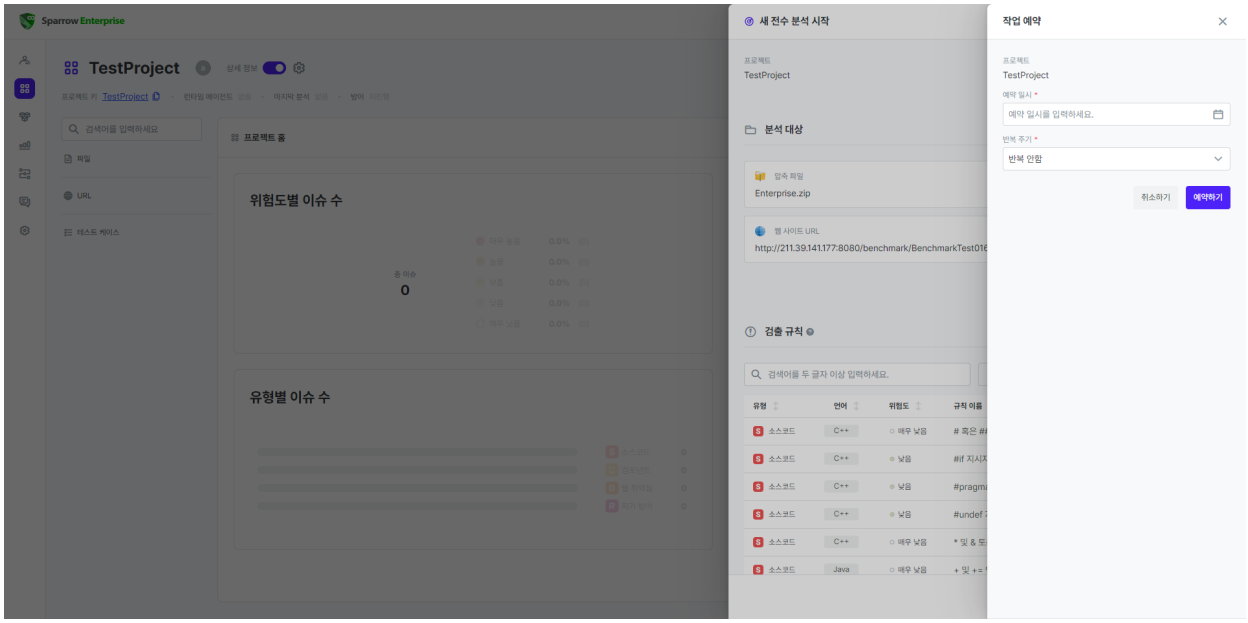
6. 분석하려는 분석 대상을 선택하거나 입력하고 **선택하기** 버튼을 클릭하세요.

> **Tip**: 분석 대상에 대한 자세한 내용은 앞에서 설명한 분석을 참고하세요.



7. **예약하기** 버튼을 클릭하세요.

8. 아래를 참고하여 **예약 일시**와 **반복 주기**를 선택하세요.



9. **예약하기** 버튼을 클릭하세요.

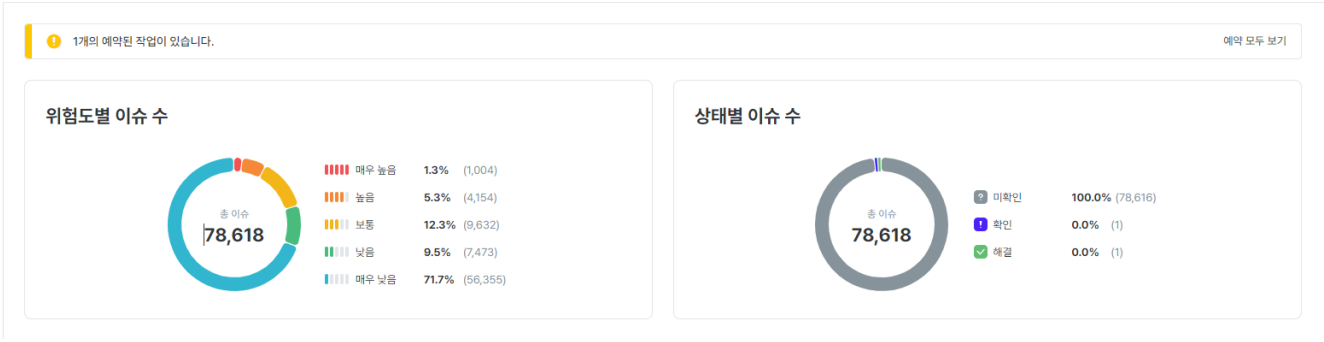
예약 일시*

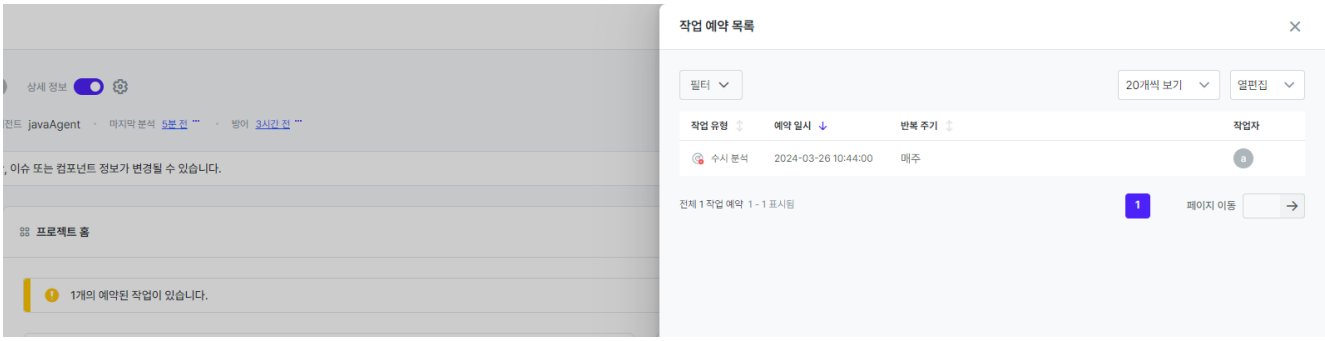
예약한 작업을 처음으로 시작할 일시입니다. 달력에서 예약할 날짜를 선택하면 자동으로 현재 시간이 입력됩니다. 필요한 경우 시간을 수정한 후에 **확인** 버튼을 클릭하세요.

반복 주기*

예약한 작업을 반복하는 기간입니다. 반복 안함, 매일, 매주, 매월, 매년 중 하나를 선택하세요.(기본값: 반복 안함)

분석 예약이 성공하면 프로젝트 상세 정보 페이지에 '**예약된 작업이 있습니다.**'라는 알림 메시지가 표시됩니다. 해당 알림의 오른쪽에 있는 **예약 모두 보기**를 클릭하여 예약된 작업이 무엇인지 확인할 수 있습니다.





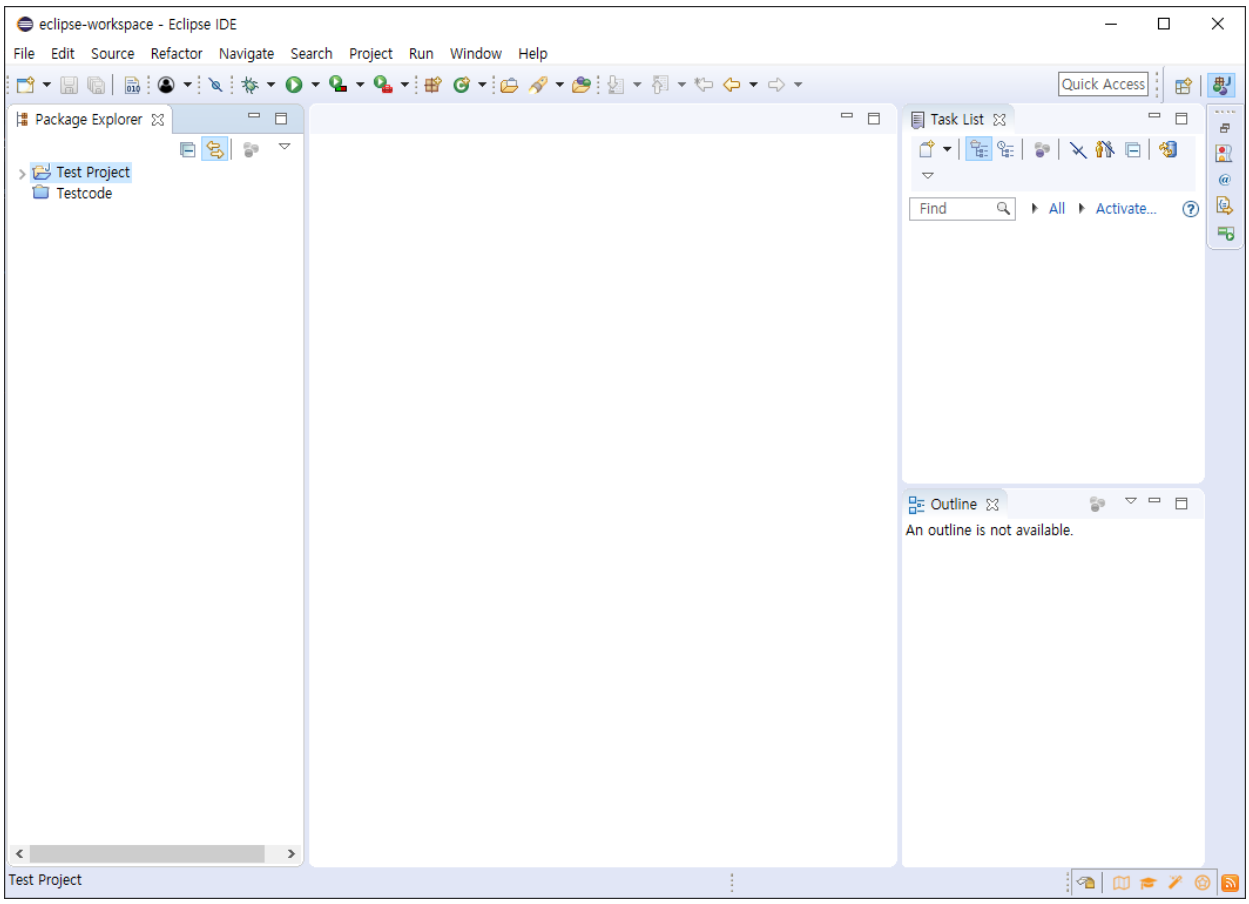
Eclipse 플러그인

개발 환경에서 Eclipse를 활용하고 있는 경우 웹 서버나 클라이언트 GUI, 클라이언트 CLI를 사용하지 않고 **Sparrow Enterprise Eclipse 플러그인**을 통해 직접 분석을 수행할 수 있습니다. **Eclipse 플러그인**은 Sparrow Enterprise 클라이언트를 설치할 때 함께 설치되지 않고 별도로 설치해야 합니다. 다음을 참고하여 Eclipse 플러그인을 설치하세요.

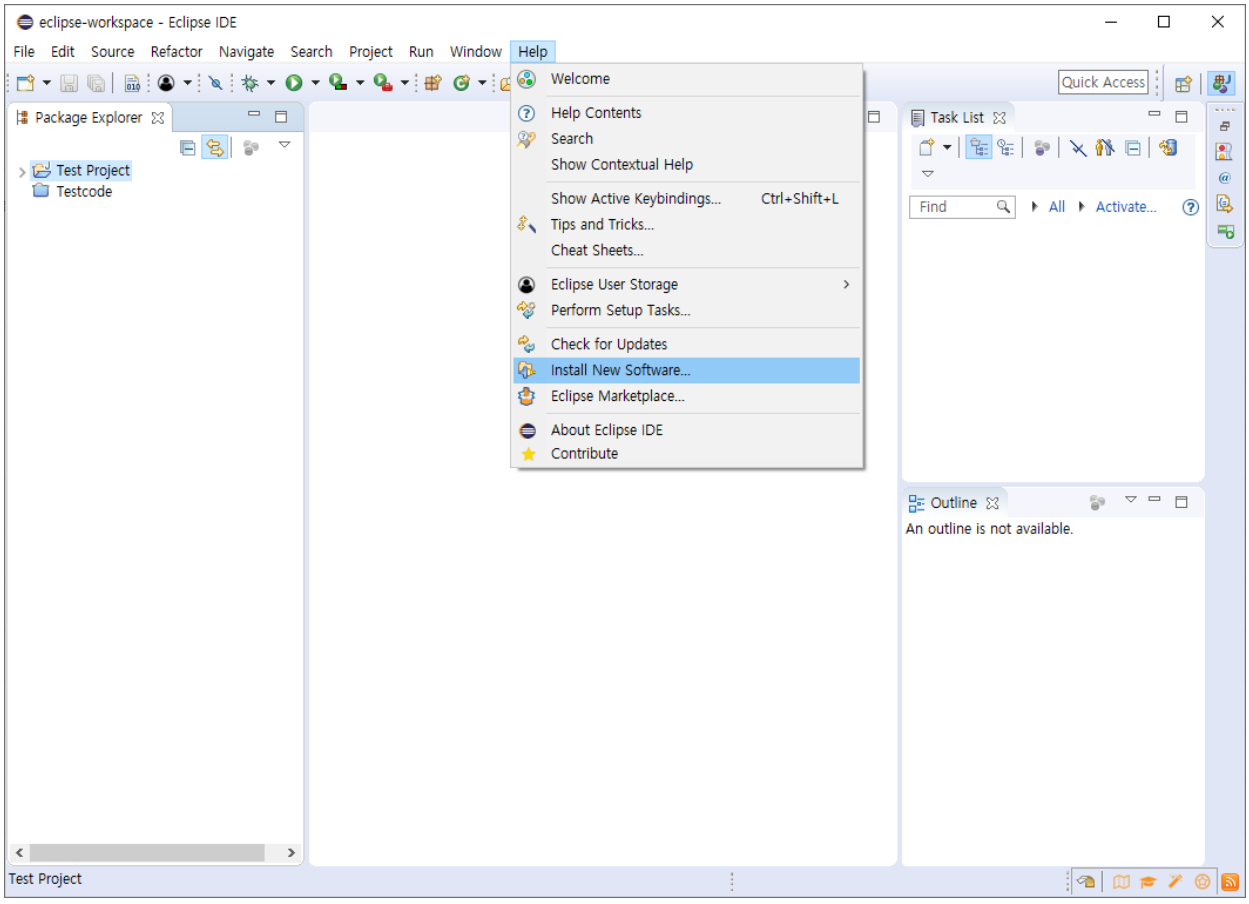
Eclipse 플러그인: 설치하기

Sparrow Enterprise Eclipse 플러그인을 실행하기 위해서는 **Sparrow Enterprise 클라이언트**와 **Sparrow Enterprise Eclipse 플러그인**을 설치해야 합니다. 먼저 Sparrow Enterprise 클라이언트 설치하기를 참고하여 **Sparrow Enterprise 클라이언트**를 설치한 뒤 다음을 단계를 수행하세요.

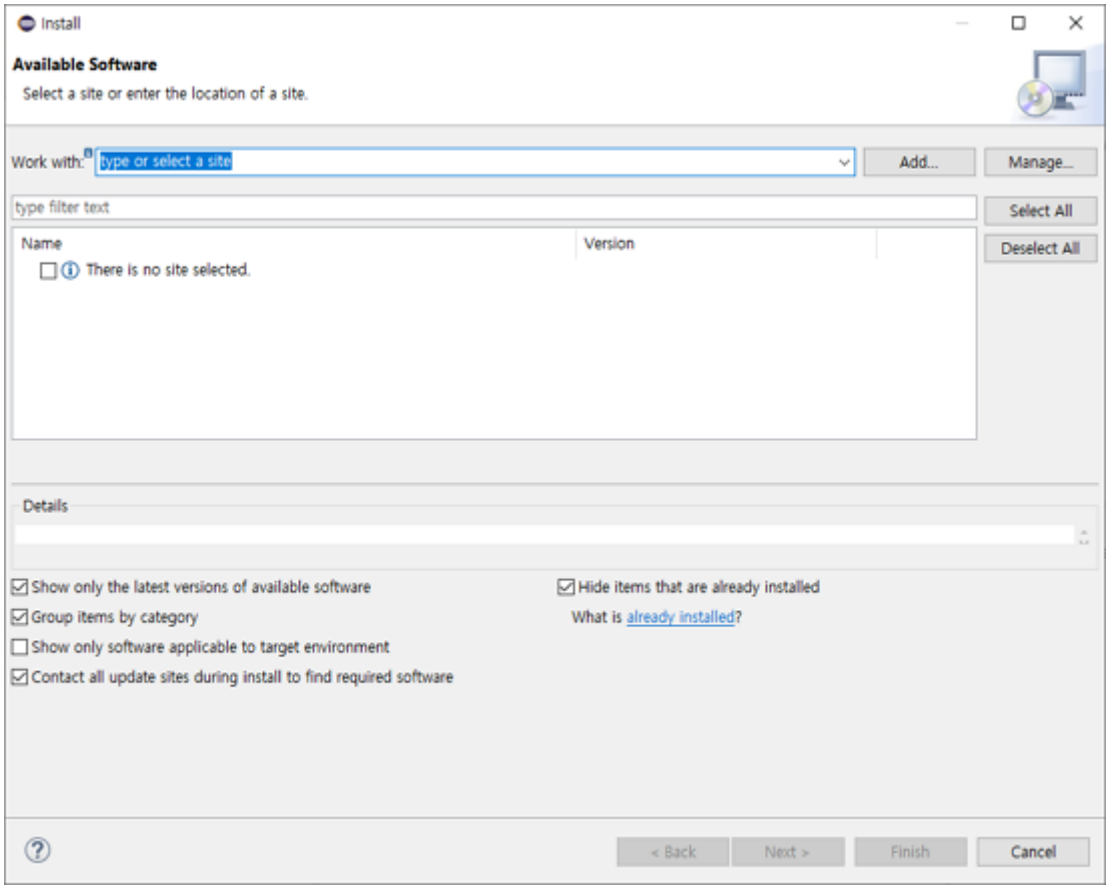
1. **Eclipse**를 실행하세요.



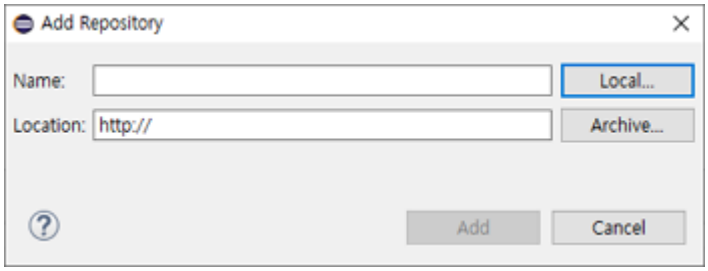
2. Eclipse에 있는 **Help** 메뉴에서 **Install New Software...**를 클릭하세요.



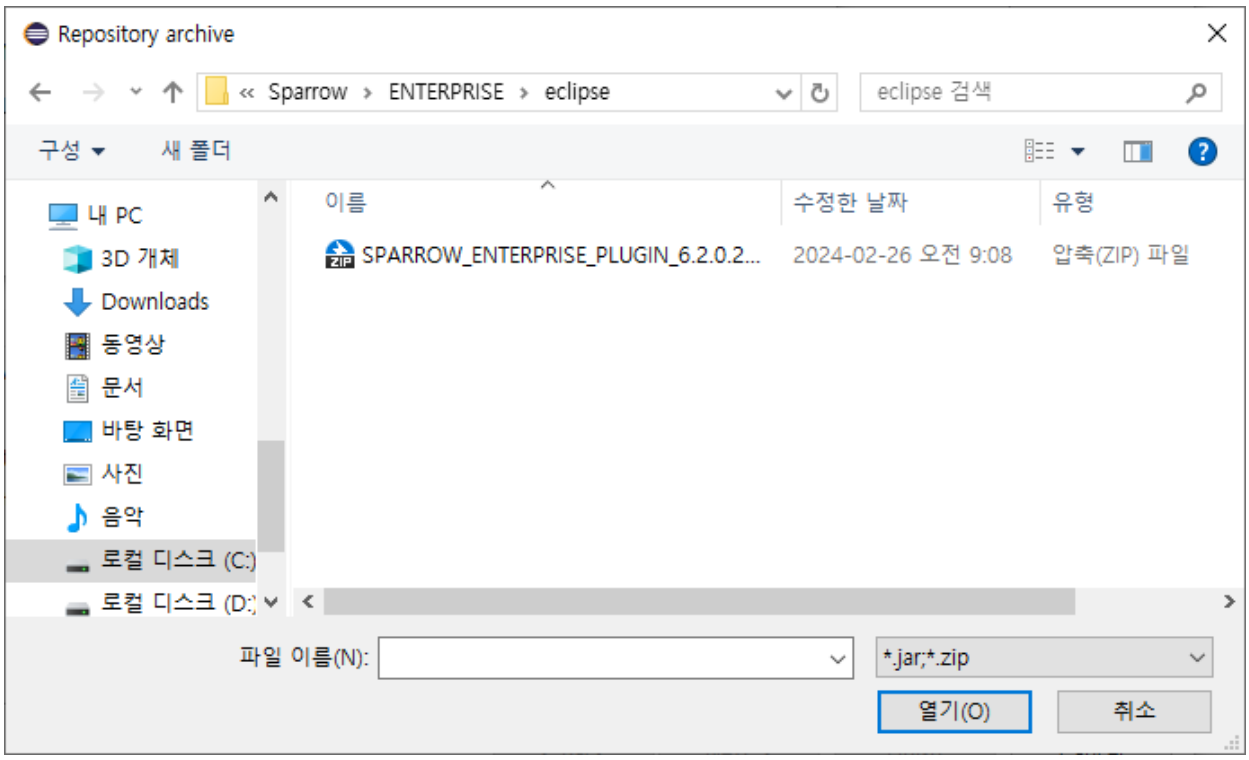
3. **Install** 창이 표시되면 오른쪽 위에 있는 **Add...** 버튼을 클릭하세요.



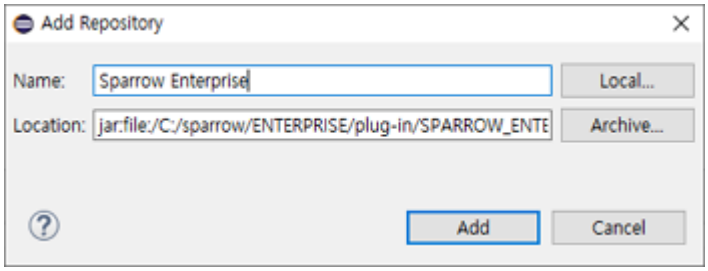
4. **Add Repository** 창이 표시되면 **Name**에 **Sparrow Enterprise**를 입력하고 **Archive...** 버튼을 클릭하세요.



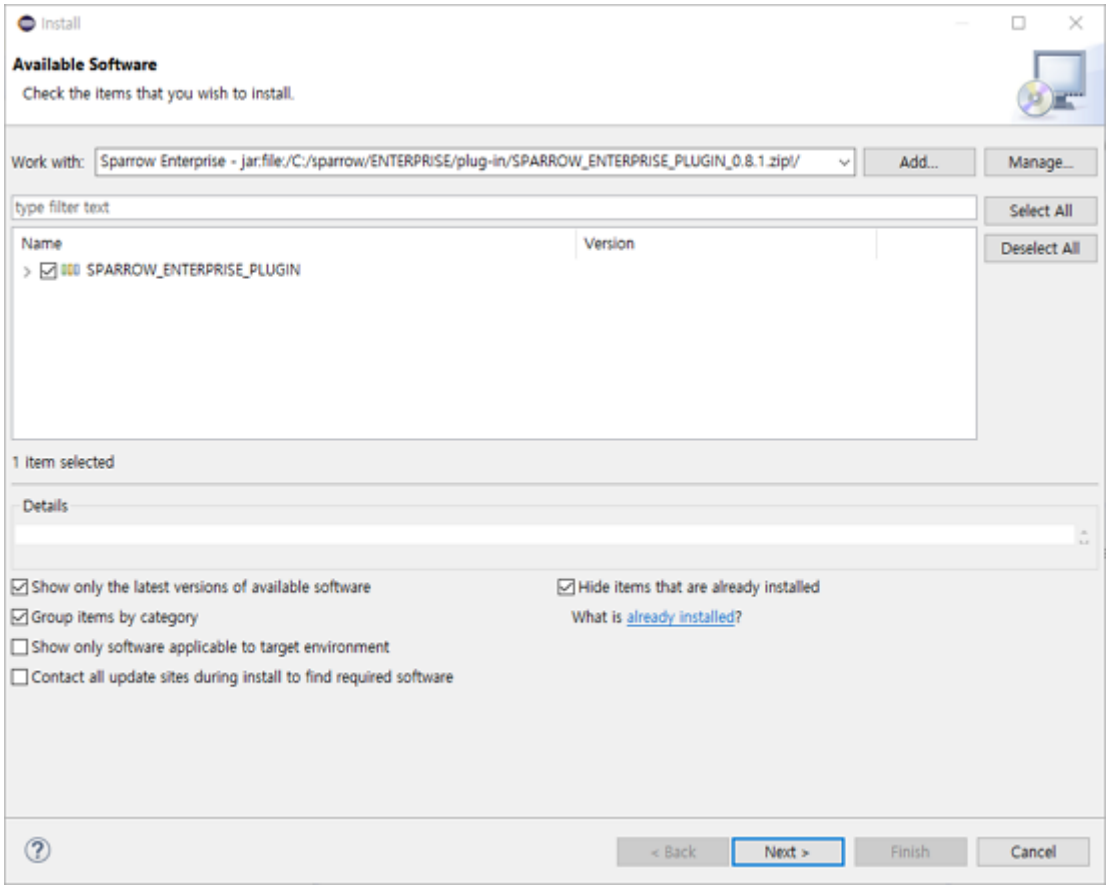
5. 다운로드한 Eclipse 플러그인 설치 파일을 선택하고 **열기** 버튼을 클릭하세요.



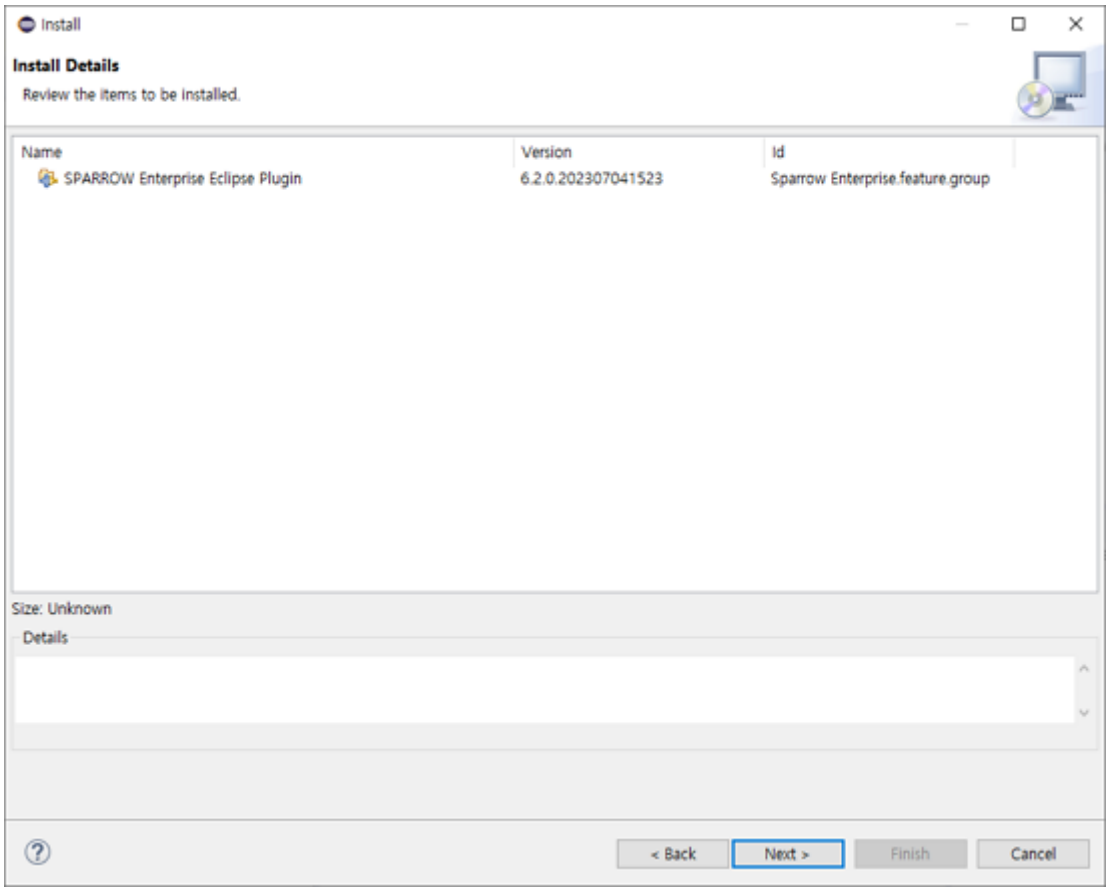
6. **Add Repository** 창에서 **Add** 버튼을 클릭하세요.



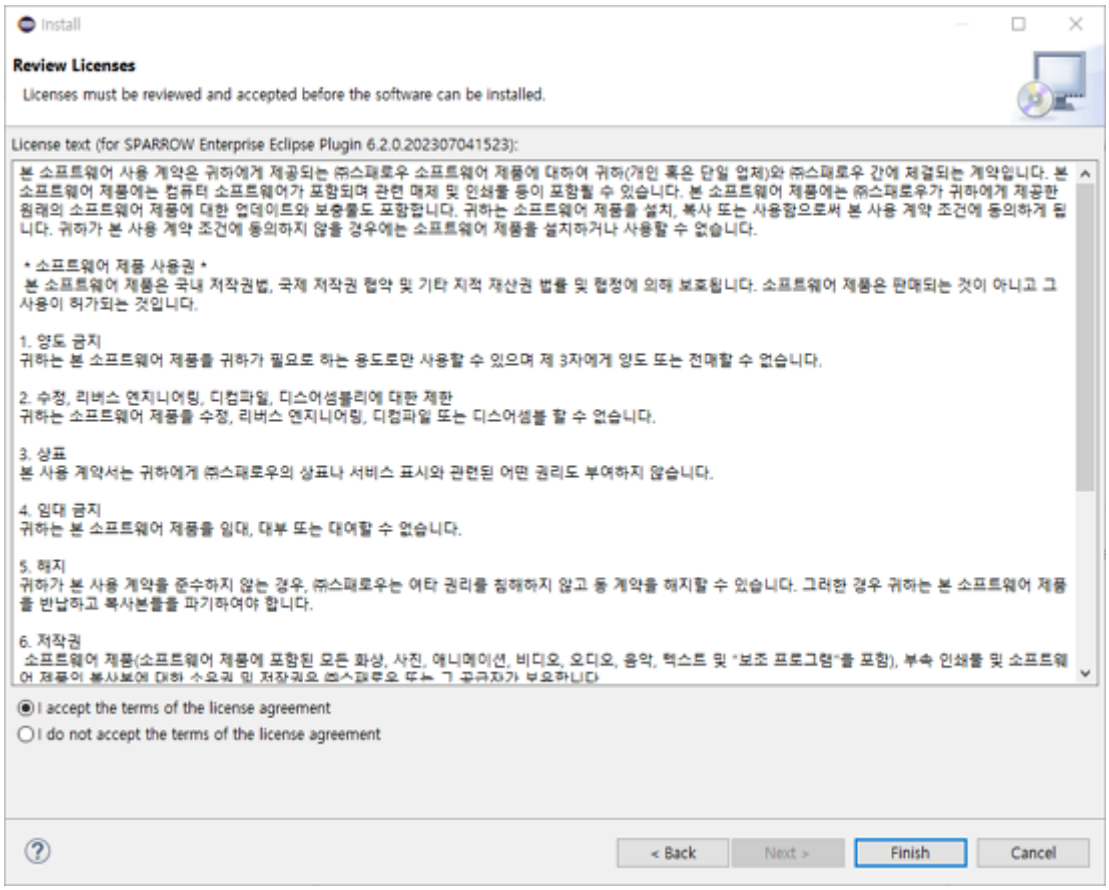
7. **SPARROW_ENTERPRISE_PLUGIN** 체크 박스를 선택하고 **Contact all update sites during install to find required software** 체크 박스의 선택을 해제한 다음 **Next >** 버튼을 클릭하세요.



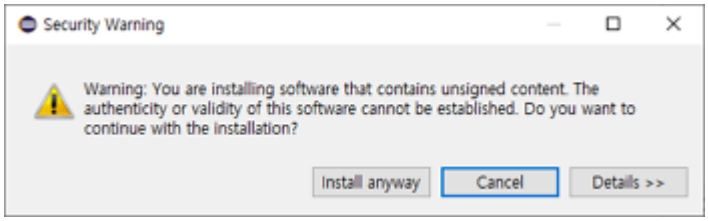
8. **Next >** 버튼을 클릭하세요.



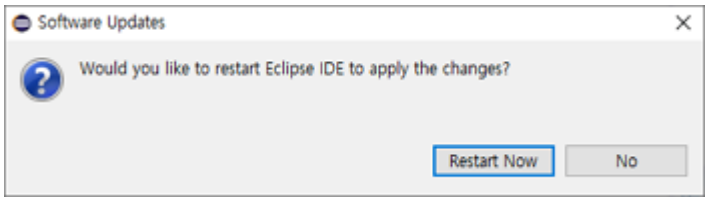
9. **Review Licenses** 창에서 **I accept the terms of the license agreement**를 선택하고 **Finish** 버튼을 클릭하세요.



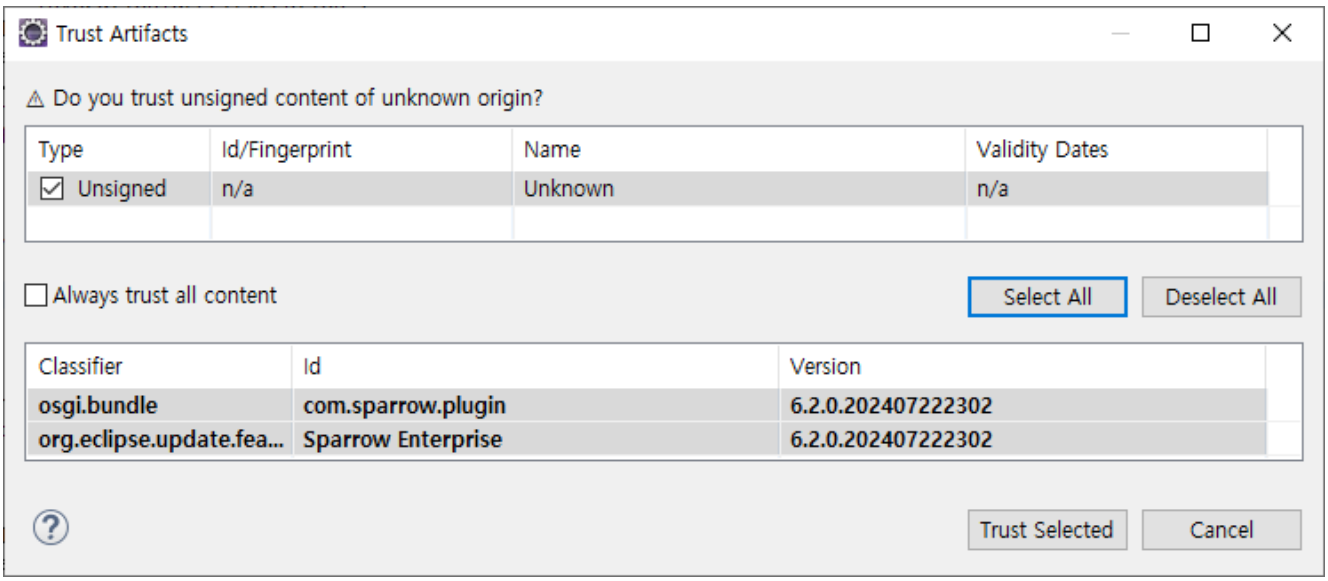
10. **Security Warning** 창이 표시되면 **Install anyway** 버튼을 클릭하세요.



11. **Software Updates** 창이 표시되면 **Restart Now** 버튼을 클릭하여 Eclipse를 다시 시작하세요.



> **Tip**: 다음과 같이 **Trust Artifacts** 창이 표시되면 **Select All** 버튼과 **Trust Selected** 버튼을 차례로 클릭하세요.

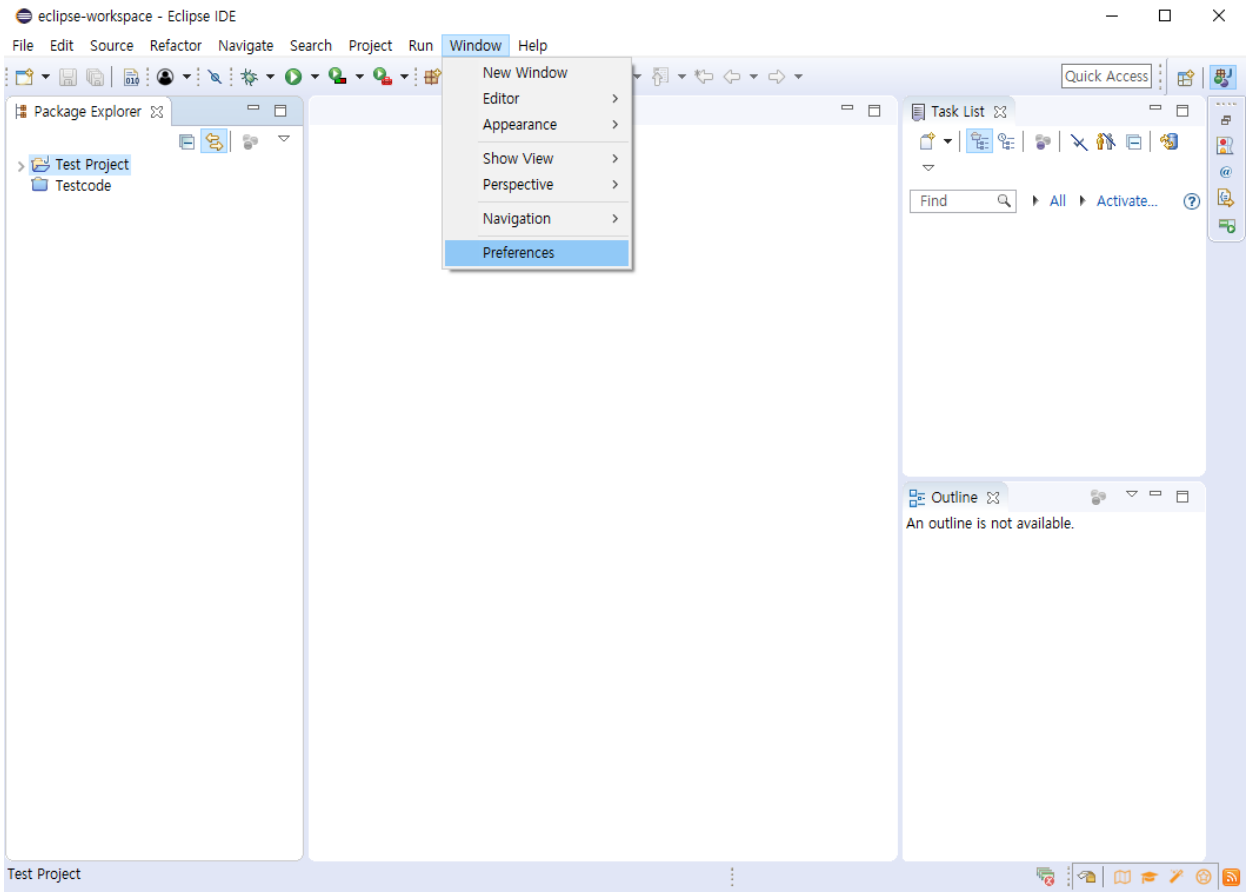


12. Eclipse 플러그인 설치가 완료되었습니다.

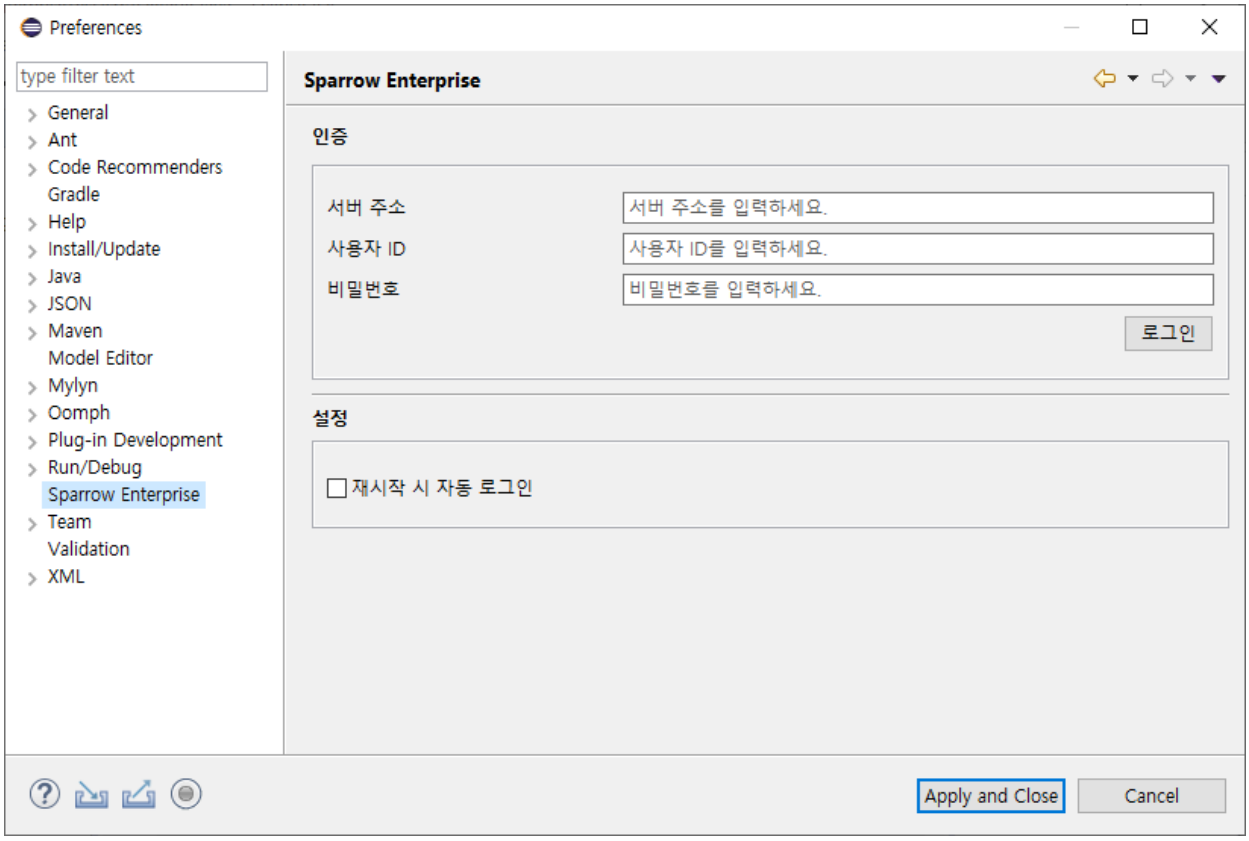
Eclipse 플러그인: 로그인하기

Sparrow Enterprise 웹에 한 번도 로그인하지 않은 사용자 계정은 올바른 사용자 ID와 비밀번호를 입력하더라도 Eclipse 플러그인과 같은 클라이언트에 로그인할 수 없습니다. 따라서 Sparrow Enterprise 웹에 먼저 로그인하여 비밀번호를 변경한 후, 변경한 비밀번호로 플러그인에 로그인해야 합니다.

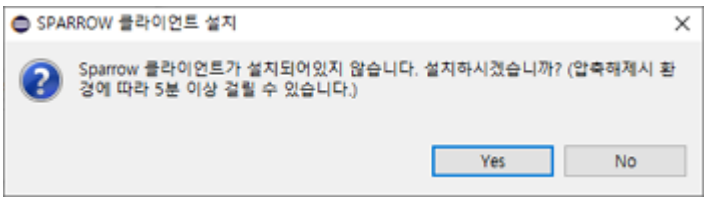
1. **Eclipse**를 실행하세요.
2. **Window** 메뉴에서 **Preferences**를 클릭하세요.



3. **Preferences** 창이 표시되면 **Sparrow Enterprise**를 선택하세요.

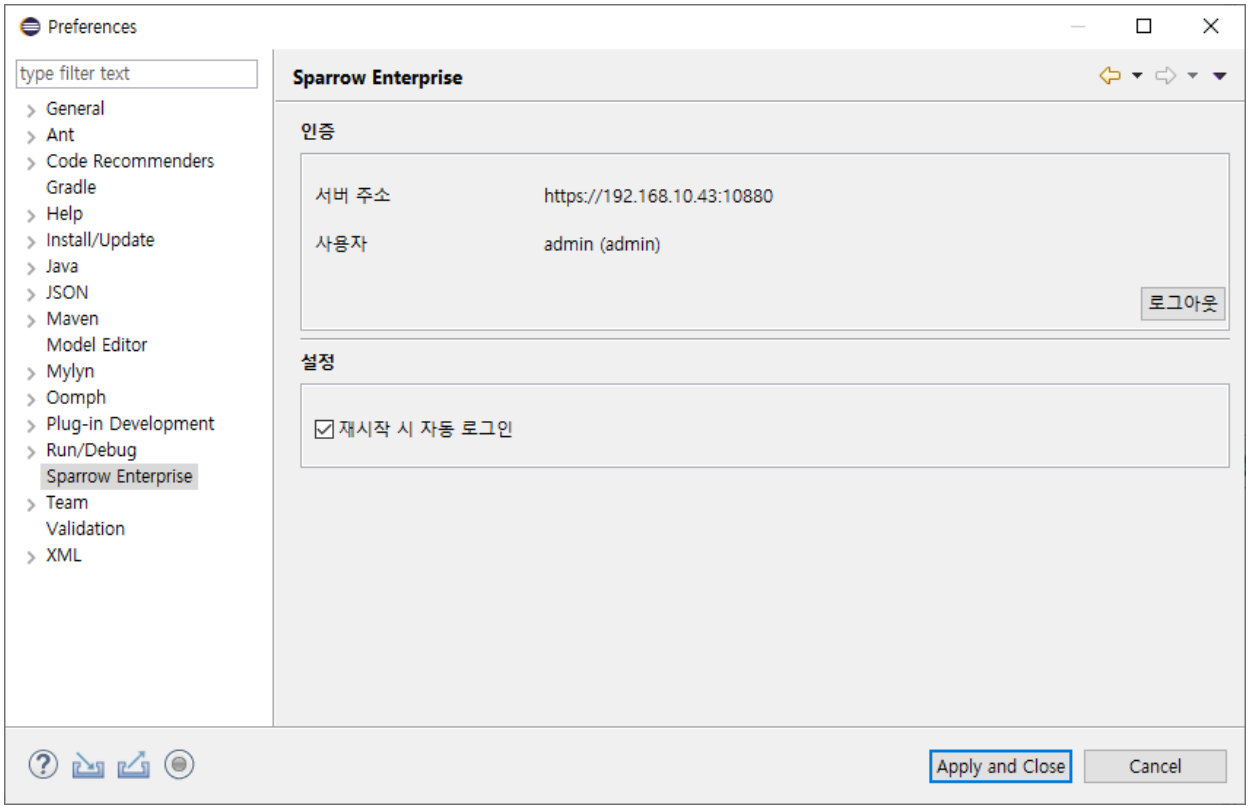


> **Tip**: Sparrow Enterprise 클라이언트를 설치하지 않은 경우 다음 메시지에서 **Yes**를 클릭하여 클라이언트를 설치하세요.



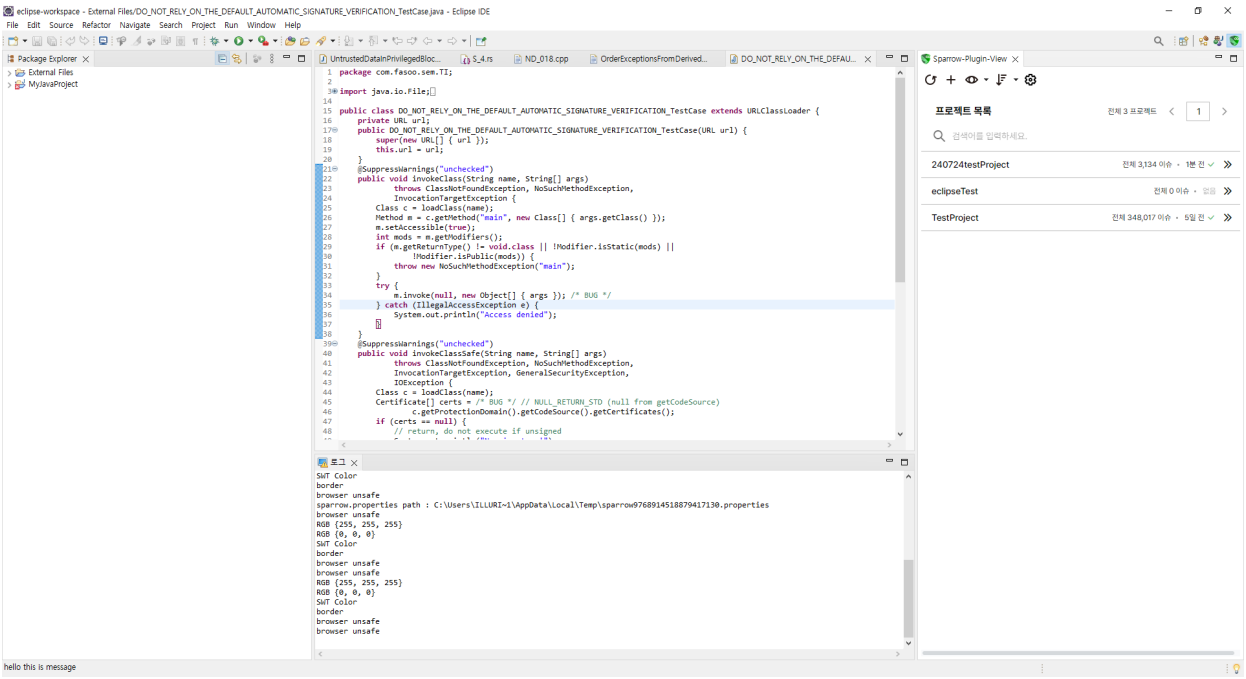
4. **서버 주소**, **사용자 ID**, **비밀번호**를 입력하고 **로그인** 버튼을 클릭하세요.

5. 로그인에 성공하면 **Apply and Close** 버튼을 클릭하세요.



> **Tip**: **재시작 시 자동 로그인** 체크 박스를 선택하면 Eclipse를 실행할 때 자동으로 로그인하게 됩니다.

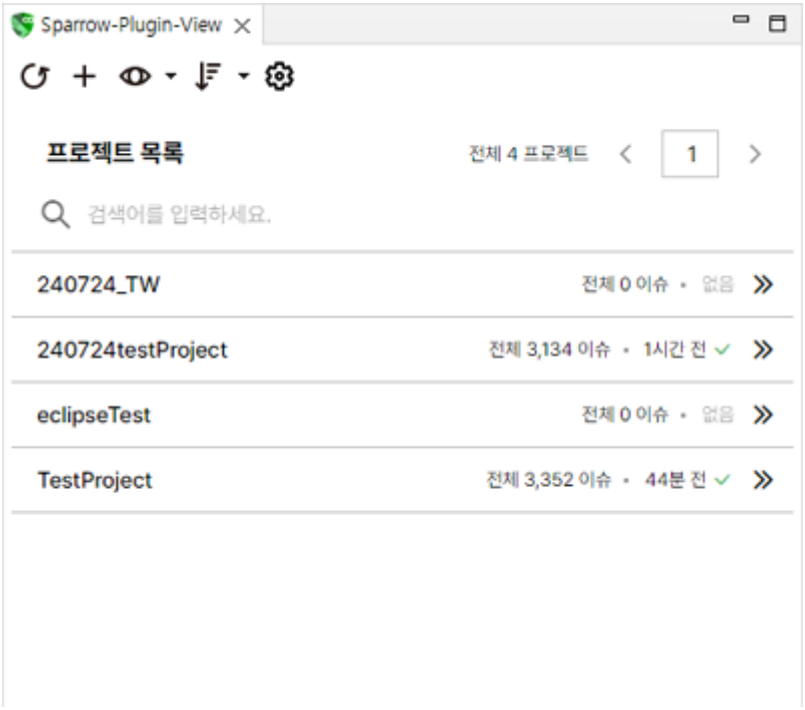
7. 이제 Eclipse 플러그인에서 Sparrow Enterprise에 로그인되었습니다.



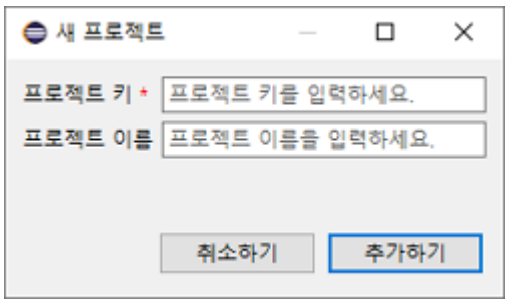
Eclipse 플러그인: 프로젝트 추가하기

먼저 분석을 수행할 프로젝트를 추가하겠습니다.

1. **프로젝트 목록** 창에서 **더하기** 아이콘을 클릭하세요.



2. **프로젝트 키**, **프로젝트 이름**을 입력하세요.



3. **추가하기** 버튼을 클릭하세요.

4. '**프로젝트를 생성했습니다.**'라는 메시지가 표시되면 **OK** 버튼을 클릭하세요.

Eclipse 플러그인: 분석하기

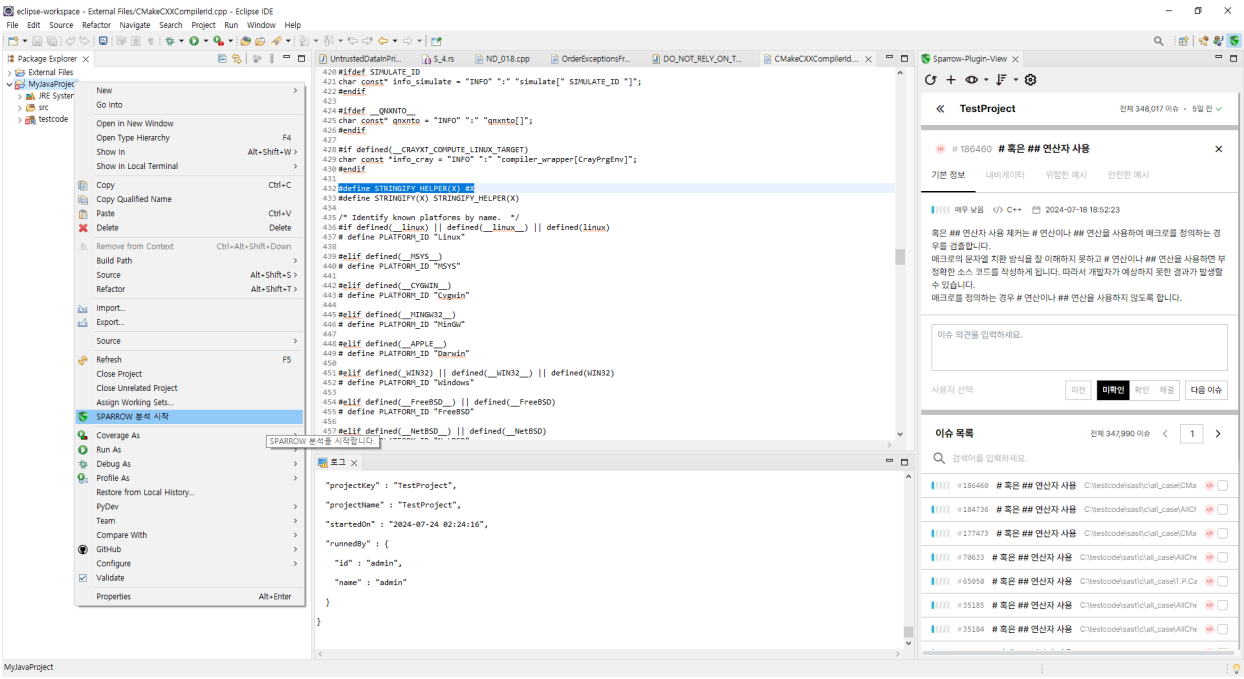
이제 Sparrow Enterprise 클라이언트에 연결된 Eclipse 플러그인을 사용하여 소스코드 이슈 및 컴포넌트 이슈를 분석할 수 있습니다. 분석할 때 프로젝트, 패키지, 파일 등 사용자가 원하는 분석 대상을 선택하여 분석할 수 있습니다.

1. **sparrow-plugin** 창의 **프로젝트 목록**에서 앞서 추가한 프로젝트를 선택하세요.

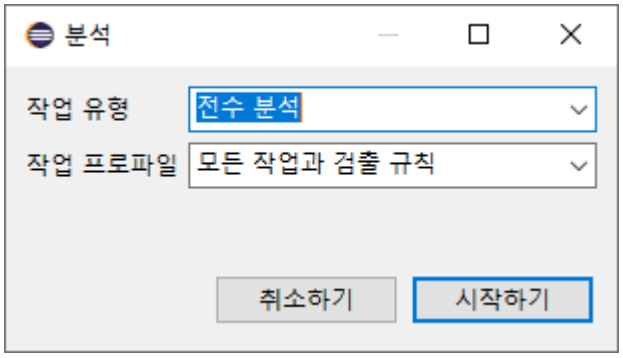
2. **Project** 창에서 분석할 대상을 선택하세요.

3. 마우스 오른쪽 버튼을 클릭하세요.

4. **SPARROW 분석 시작**을 클릭하세요.



5. **작업 유형**에서 **전수 분석** 또는 **수시 분석**을 선택하세요.



> **Tip**: **전수 분석**과 **수시 분석**에 대한 설명은 분석을 참고하세요.

6. **작업 프로파일**을 선택하세요.

> **Tip**: **작업 프로파일**은 이슈 검출 규칙과 작업 옵션 등 작업에 필요한 정보를 모아둔 데이터입니다. 자세한 내용은 작업 프로파일을 참고하세요.

7. **시작하기** 버튼을 클릭하세요.

8. 이제 분석이 시작됩니다.

> **Tip**: 분석이 수행되면 **로그** 창에 분석 로그가 표시됩니다.

Eclipse 플러그인: 결과 확인

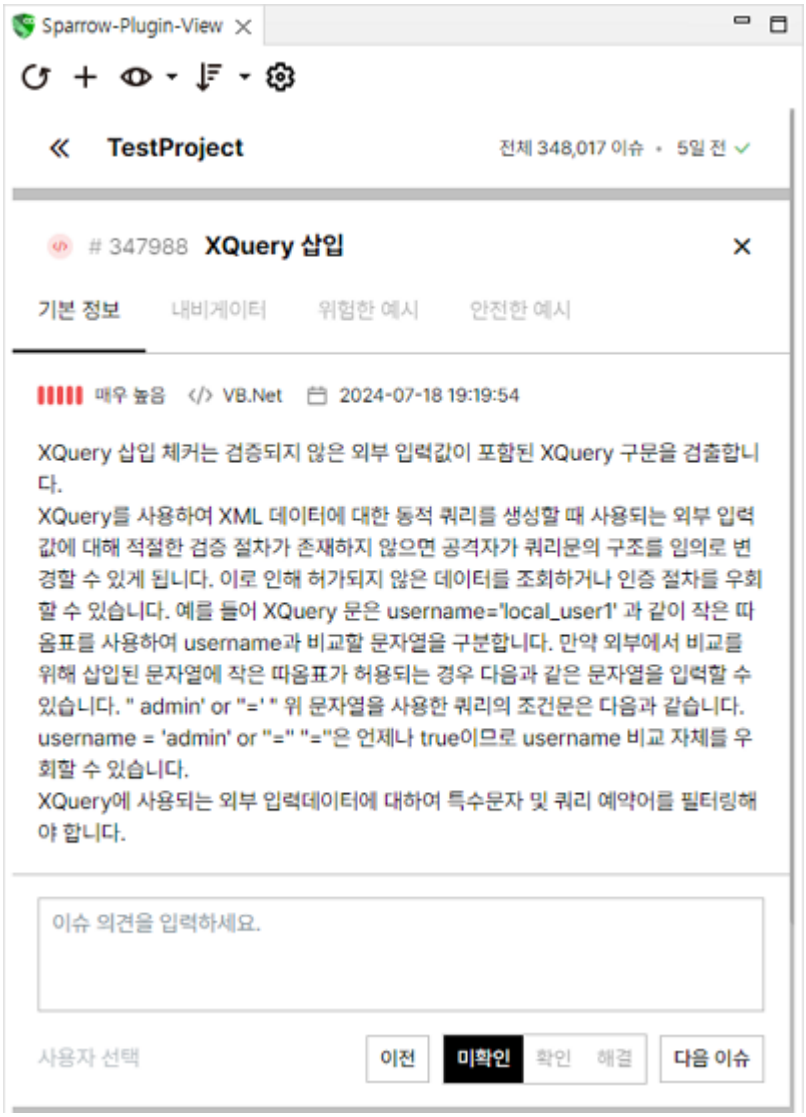
분석이 끝나고 결과를 확인하려면 **Sparrow-Plugin-View** 창의 **프로젝트 목록**에서 분석을 수행한 프로젝트를 클릭하세요. 해당 분석의 **이슈 목록**이 표시됩니다. 여기서 이슈에 대한 다양한 정보를 확인할 수 있습니다.

✓ 이슈 목록

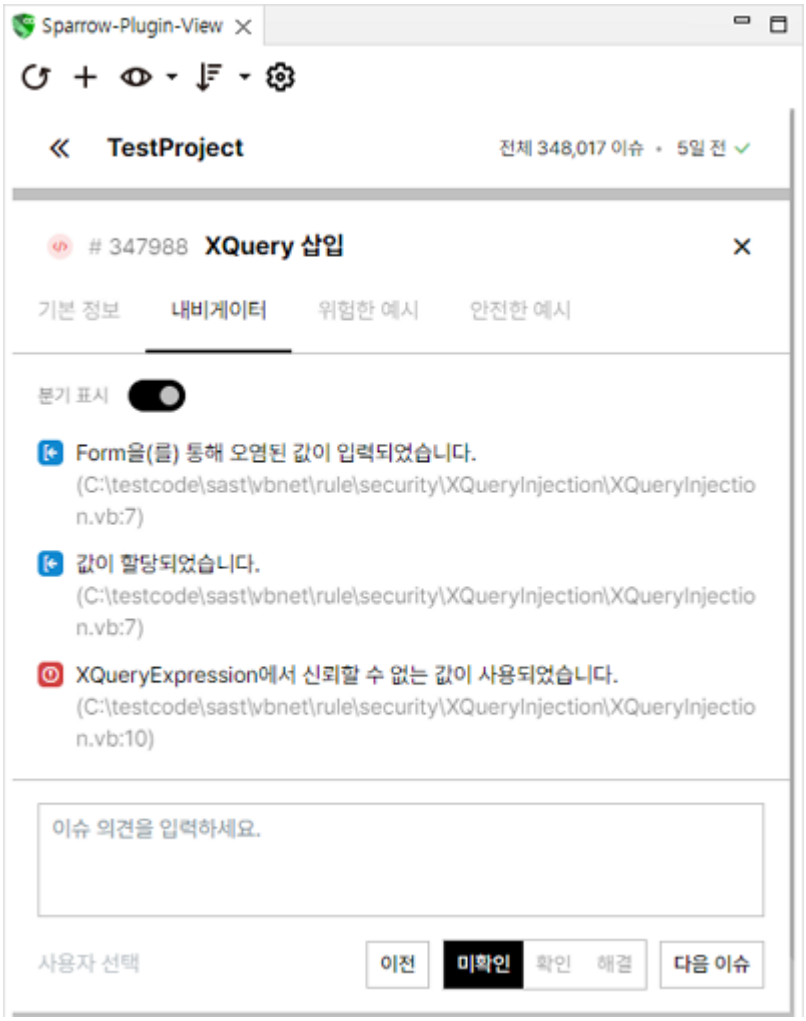
이슈 목록에서는 프로젝트의 최근 이슈 목록을 확인할 수 있습니다. 여기에는 이슈의 **ID**, **유형**, **이슈 이름**, 이슈가 검출된 **자산**, **위험도**, **이슈 상태**가 표시됩니다.

✓ 소스코드 이슈 상세 정보

검출한 이슈에 대한 정보를 표시합니다.



소스코드 이슈 상세 정보에는 이슈 검출 규칙에 대한 기본 정보, 검출된 이슈의 소스코드 라인에 대한 설명인 내비게이터, 해당 이슈에 대한 위험한 예시 및 안전한 예시가 탭으로 표시됩니다.



✓ 이슈 상태

이슈 상세 정보의 맨 아래에 있는 **이슈 톡**에서 **이슈 담당자**를 지정하거나 **이슈 상태**를 변경할 수 있습니다. **이슈 담당자**를 지정하거나 **이슈 상태**를 변경하려면 1) 프로젝트의 **프로젝트 구성원**으로써 프로젝트 권한 중 2) **이슈 참여** 권한을 포함한 프로젝트 역할을 가져야 합니다.

이슈 담당자

해당 이슈를 검토할 담당자를 표시합니다. 권한 있는 사용자 혹은 사용자 그룹 중에서 선택할 수 있으며 담당자를 지정하기 전에는 아무 것도 표시되지 않습니다.

이슈 상태

이슈가 검출되면 해당 이슈를 확인하고 해결하거나, 오탐 또는 다른 원인으로 인해 이슈에서 제외하도록 처리해야 합니다. 이슈를 어떻게 처리했는지 표시하기 위해서 이슈마다 **이슈 상태**를 다음과 같이 표시합니다.

- 미확인 : 담당자가 검출된 이슈를 아직 검토하지 않음
- 확인 : 담당자가 해당 이슈를 확인함
- 해결 : 담당자가 해당 이슈에서 발견된 문제를 해결함

Eclipse 플러그인: 삭제하기

1. Eclipse의 **Help** 메뉴에서 **About Eclipse IDE**를 클릭하세요.

2. **About Eclipse** 창이 표시되면 **Installation Details** 버튼을 클릭하세요.

3. **Sparrow Eclipse Plugin**을 선택한 후 **Uninstall** 버튼을 클릭하세요.

4. **Uninstall Details** 창에서 **Finish** 버튼을 클릭하세요.

5. **Restart Now** 버튼을 클릭하여 Eclipse 플러그인이 삭제되었는지 확인하세요.

6. 로컬에서 Eclipse의 워크스페이스가 있는 경로로 이동하세요.

7. 다음 폴더를 삭제하세요.

```
{Eclipse 워크스페이스 디렉토리}\.metadata\.plugins\com.sparrow.plugin\sparrow_client
```

8. 이제 삭제가 완료되었습니다.

Eclipse 플러그인에서 분석한 소스코드 및 컴포넌트 결과는 웹에서도 확인할 수 있습니다. 자세한 내용은 소스코드 이슈, 컴포넌트 이슈 및 최근 컴포넌트 확인하기를 참고하세요.

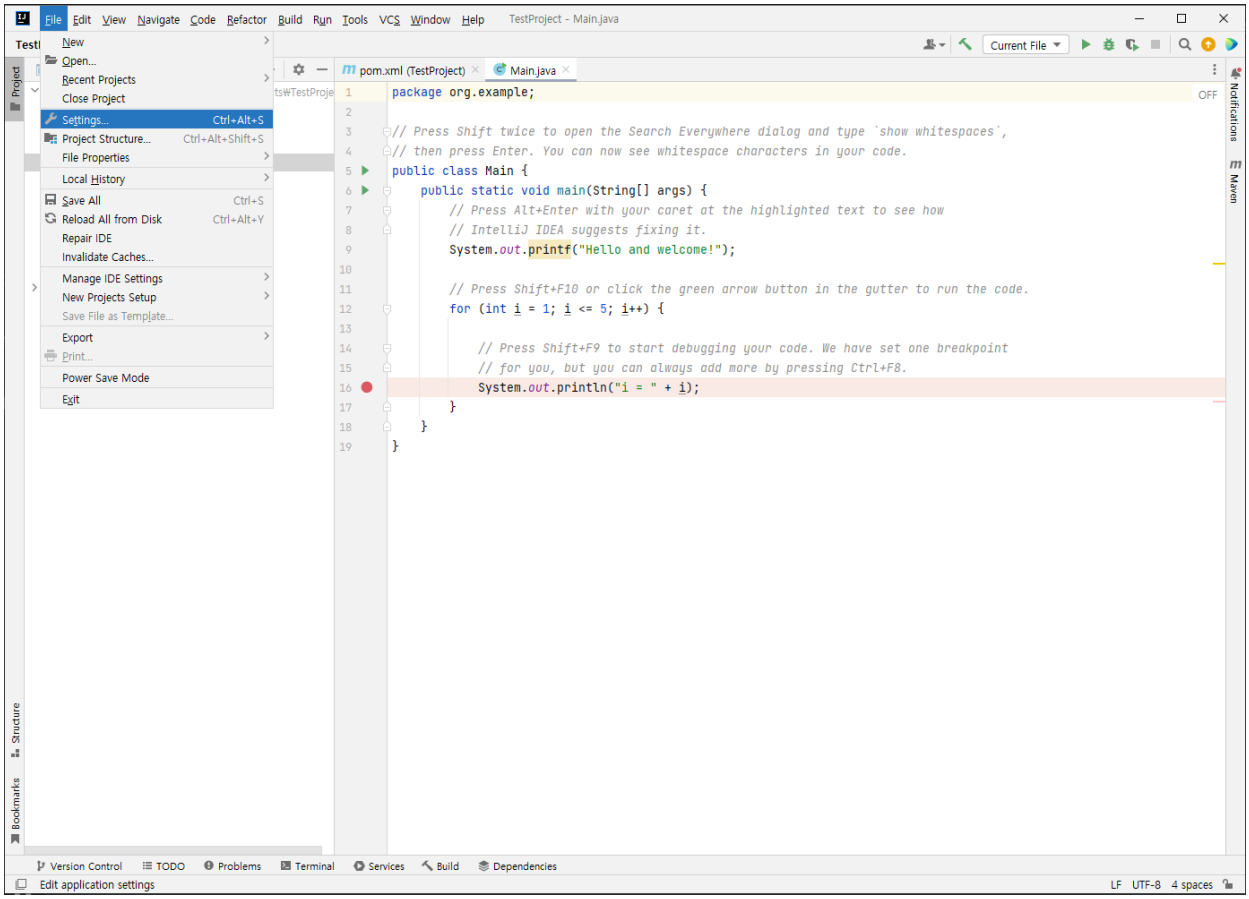
IntelliJ 플러그인

IntelliJ를 활용하고 있는 사용자라면 **Sparrow Enterprise IntelliJ 플러그인**을 설치해서 웹 서버나 GUI, CLI 클라이언트를 사용하는 것보다 편리하게 분석을 수행할 수 있습니다. IntelliJ 플러그인은 클라이언트를 사용하는 분석 방법이기 때문에 먼저 클라이언트를 설치해야 합니다. 클라이언트를 설치하는 방법은 클라이언트 설치하기를 참고하세요.

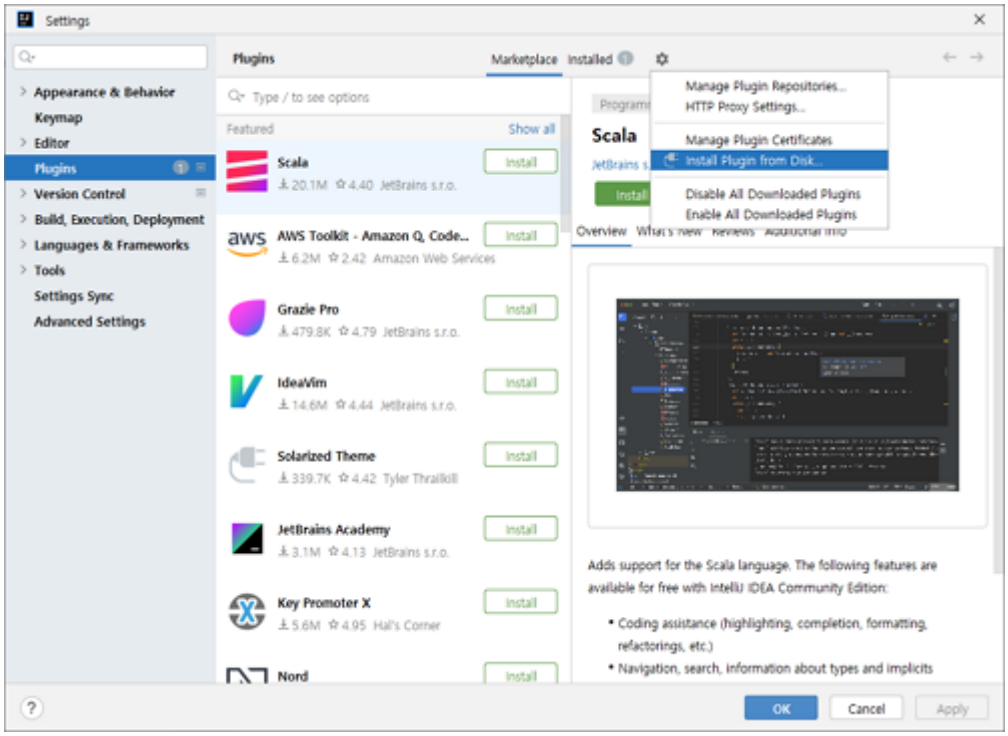
IntelliJ 플러그인: 설치하기

1. **IntelliJ**를 실행하세요.

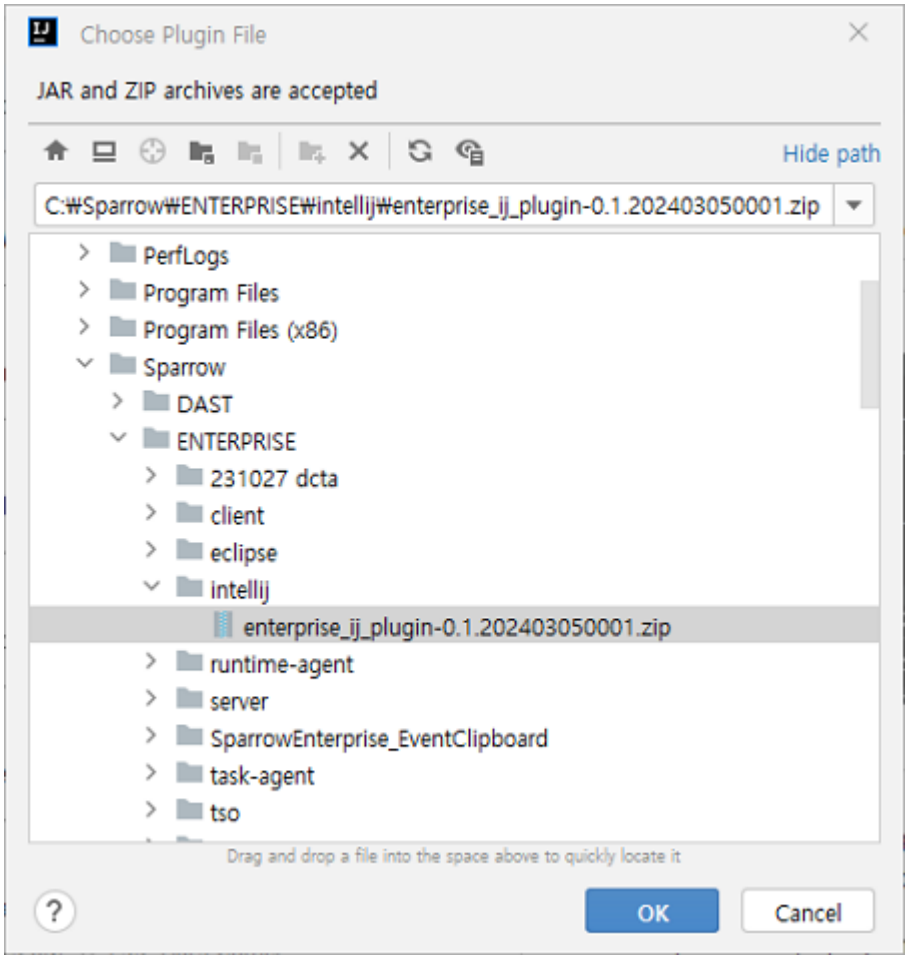
2. **File** 메뉴에서 **Settings**를 클릭하세요.



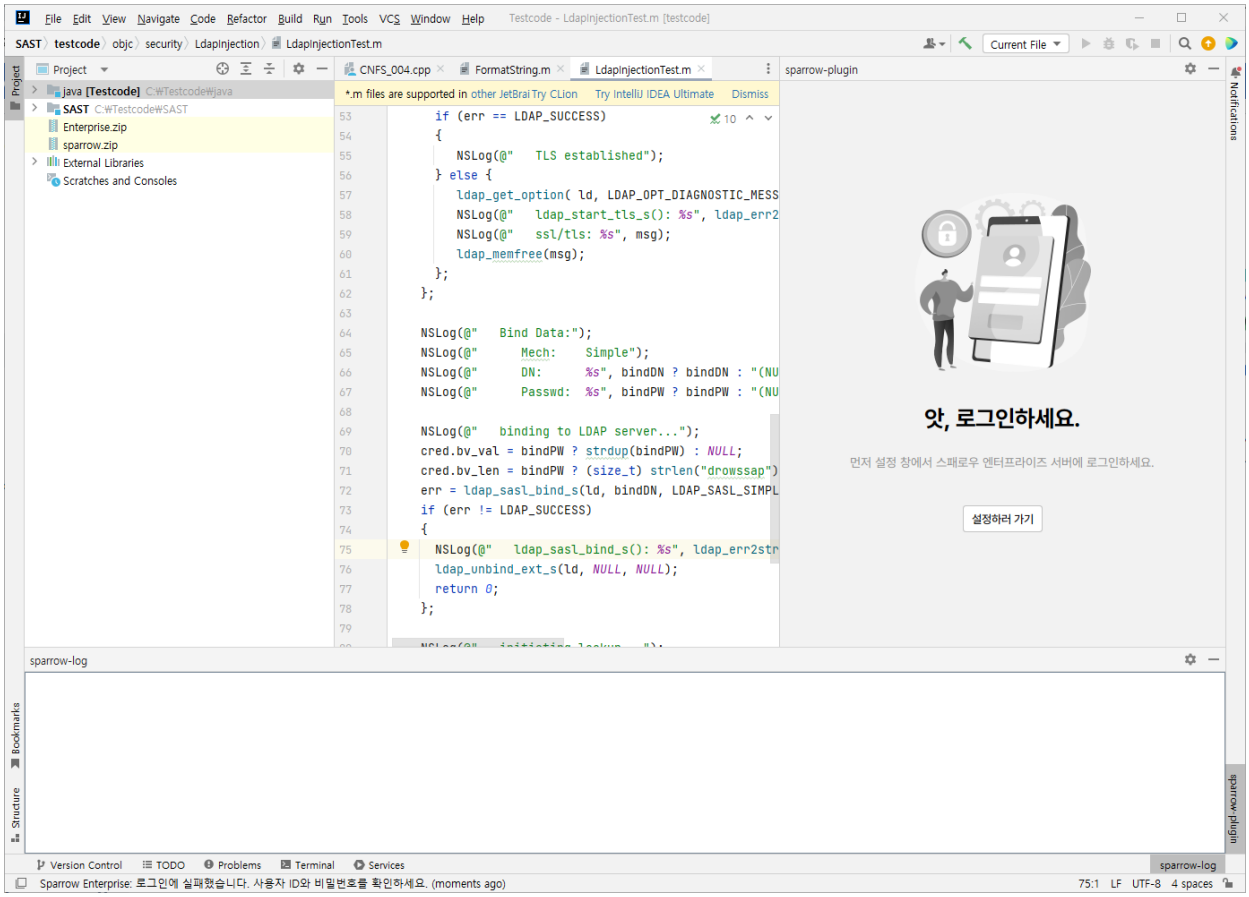
3. **Settings** 창의 **Plugin** 메뉴를 클릭하고 오른쪽 위에 있는 **설정** 아이콘을 클릭하세요.



4. **Install Plugin from Disk**..를 클릭하세요.

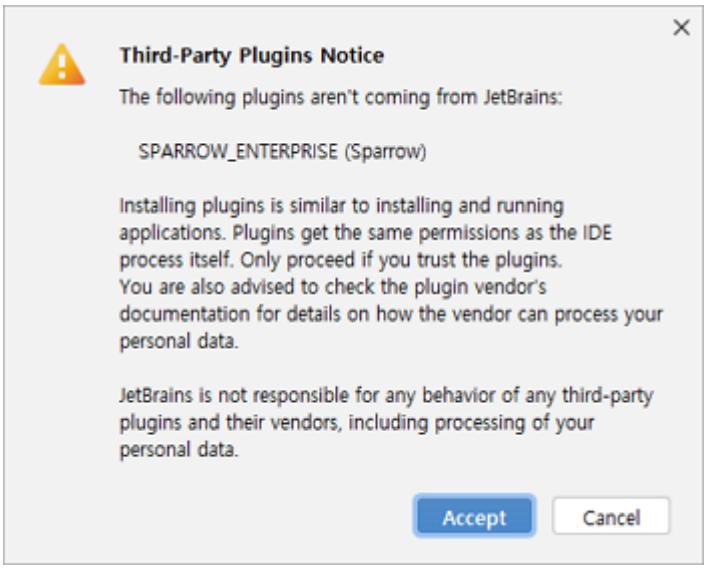


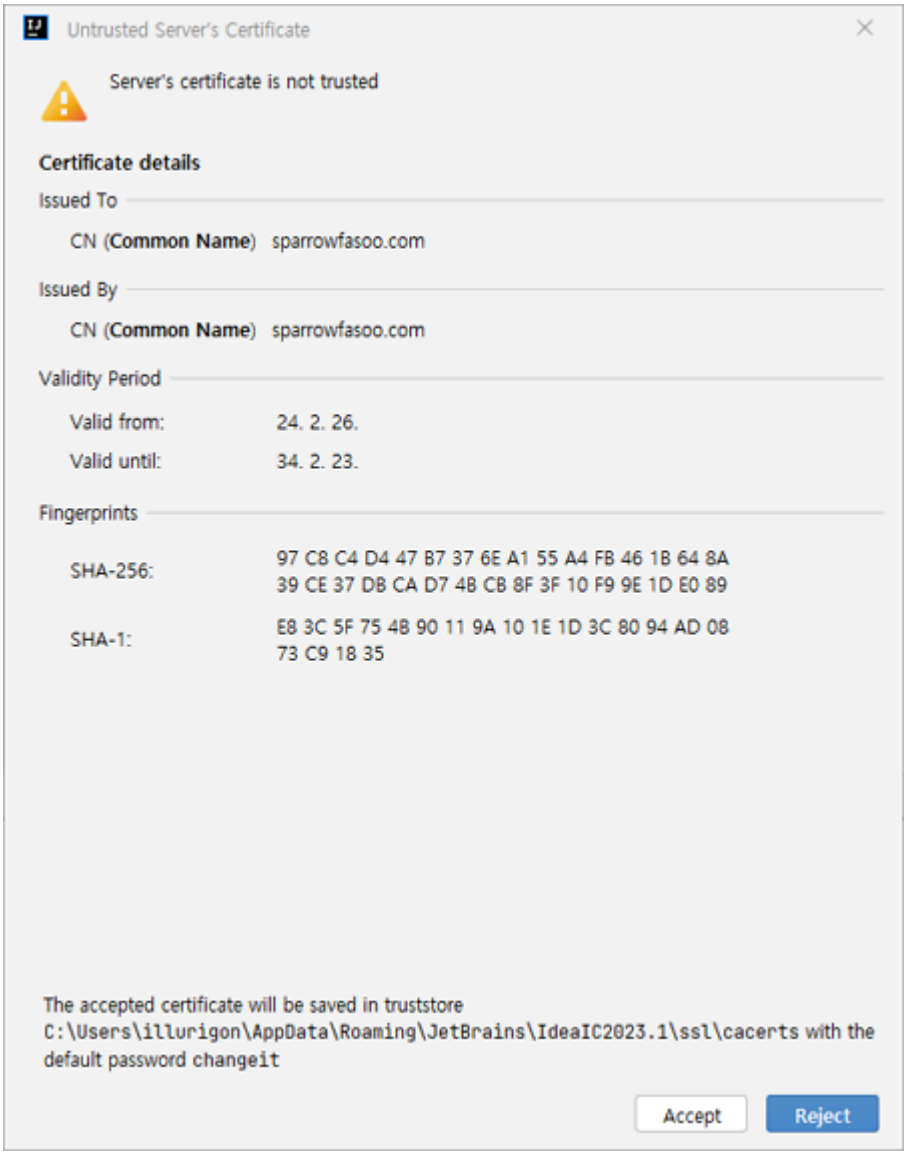
5. **Choose Plugin File** 창이 표시되면 경로에서 다운로드한 IntelliJ 플러그인 설치 파일을 선택하고 **OK** 버튼을 클릭하세요.



6. IntelliJ 플러그인 설치가 완료되었습니다.

> **Tip**: 플러그인을 생성한 주체를 확인하는 **Third-Party Plugins Notice** 창이 표시되는 경우 **Accept** 버튼을 클릭하세요. 플러그인의 인증서를 확인하는 **Untrusted Server's Certificate** 창이 표시되면 **Accept** 버튼을 클릭하여 플러그인을 실행하세요.

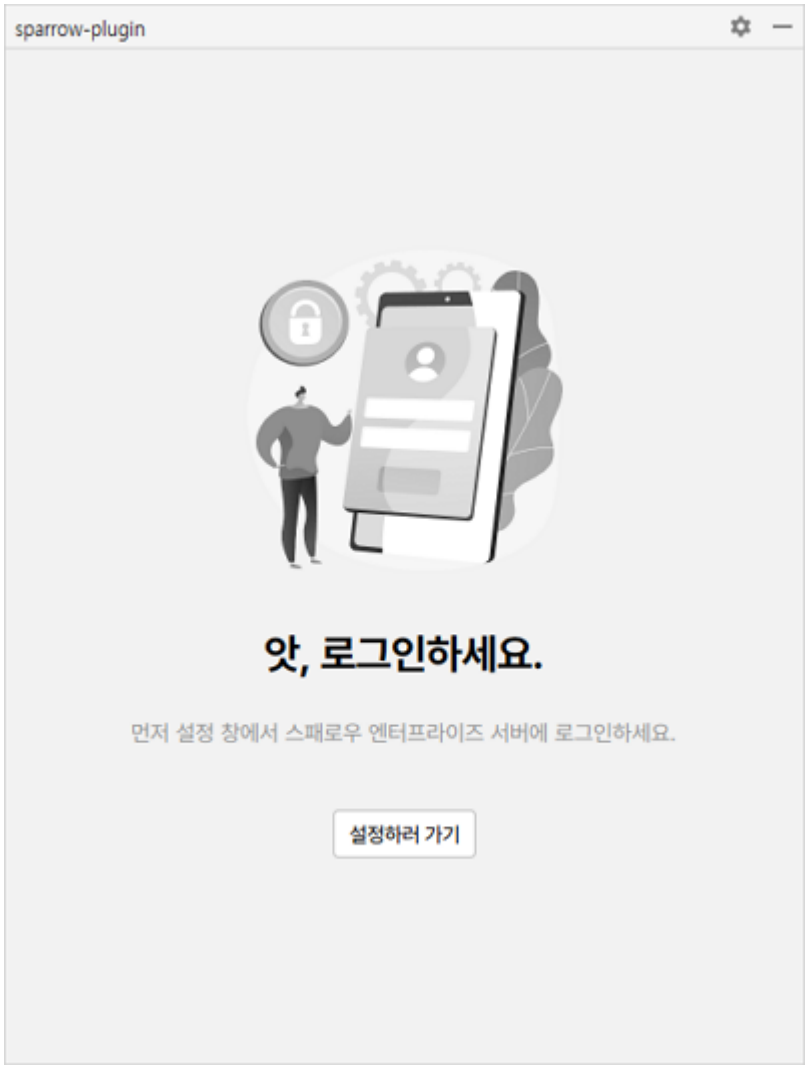




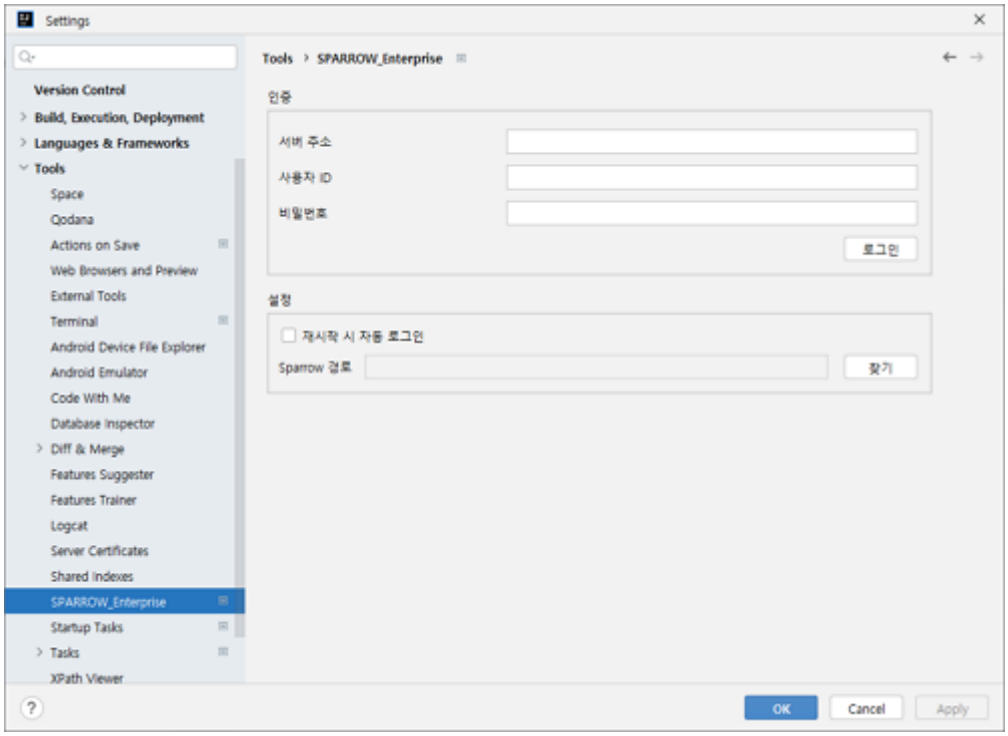
IntelliJ 플러그인: 로그인하기

Sparrow Enterprise 웹에 한 번도 로그인하지 않은 사용자 계정은 올바른 사용자 ID와 비밀번호를 입력하더라도 IntelliJ 플러그인과 같은 클라이언트에 로그인할 수 없습니다. 따라서 Sparrow Enterprise 웹에 먼저 로그인하여 비밀번호를 변경한 후, 변경한 비밀번호로 플러그인에 로그인해야 합니다.

1. **sparrow-plugin**의 **설정하러 가기** 버튼을 클릭하세요.



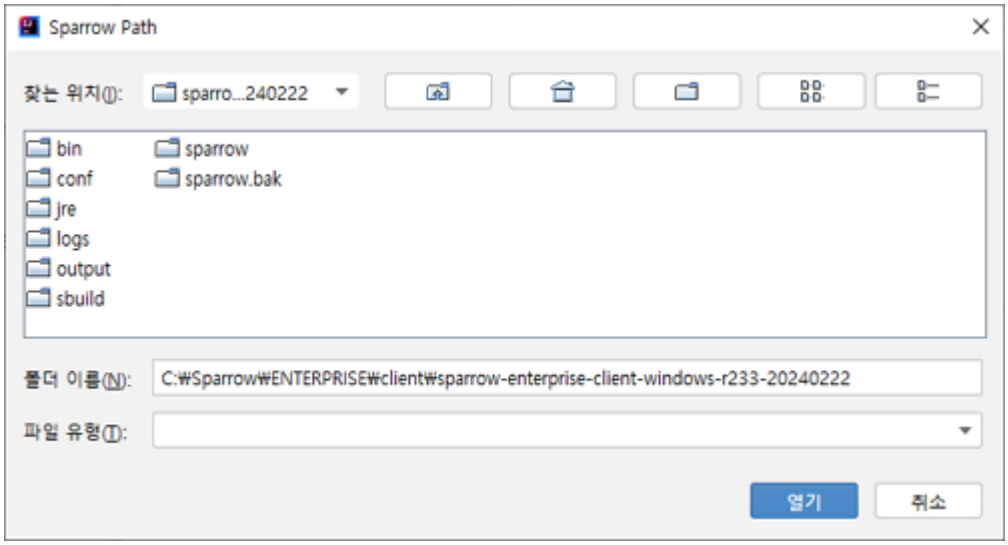
2. 혹은 **File** 메뉴에서 **Settings**를 클릭하고 **Settings** 창의 **Tools > SPARROW_Enterprise** 메뉴를 클릭하세요.



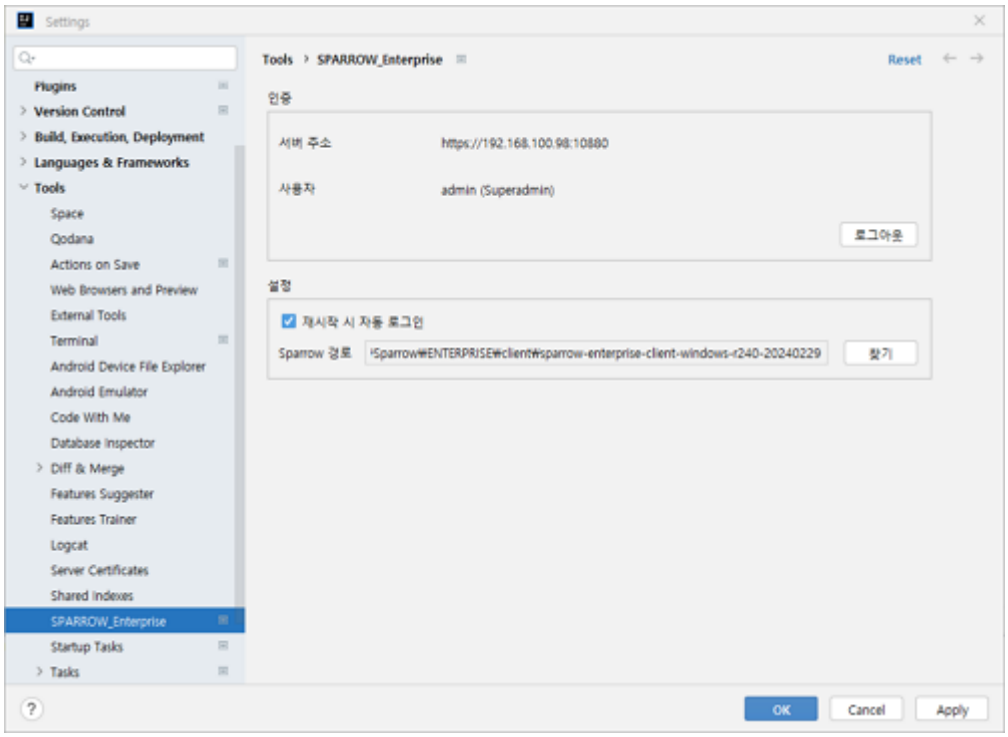
3. **서버 주소**, **사용자 ID**, **비밀번호**를 입력하고 **로그인** 버튼을 클릭하세요.

> **Tip**: **설정**에서 **자동 로그인** 체크 박스를 선택하면 IntelliJ를 실행할 때 자동으로 로그인하게 됩니다.

4. **SPARROW 경로**에서 **찾기** 버튼을 클릭하세요.



5. 로컬에 설치된 Sparrow Enterprise 클라이언트 경로를 선택하고 **열기**를 클릭하세요.



6. **OK** 버튼을 클릭하세요.

7. 이제 IntelliJ 플러그인에서 Sparrow Enterprise에 로그인되었습니다.

IntelliJ 플러그인: 프로젝트 추가하기

먼저 분석을 수행할 프로젝트를 추가하겠습니다.

1. **sparrow-plugin** 창의 **프로젝트 목록**에서 **더하기** 아이콘을 클릭하세요.

2. **프로젝트 키**, **프로젝트 이름**을 입력하세요.

3. **추가하기** 버튼을 클릭하세요.

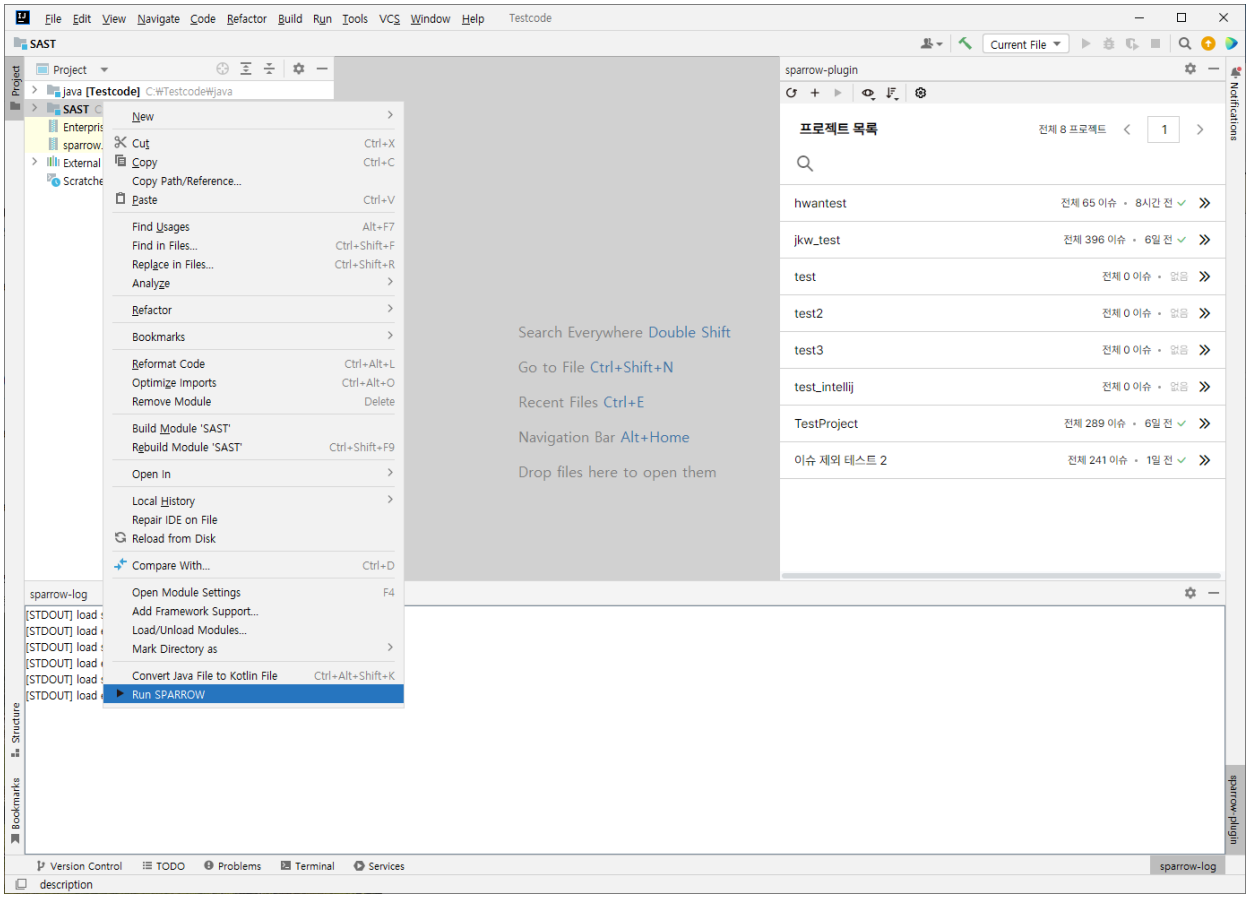
IntelliJ 플러그인: 분석하기

이제 Sparrow Enterprise 클라이언트에 연결된 IntelliJ 플러그인을 사용하여 소스코드 이슈 및 컴포넌트 이슈를 분석할 수 있습니다. 분석할 때 프로젝트, 패키지, 파일 등 사용자가 원하는 분석 대상을 선택하여 분석할 수 있습니다.

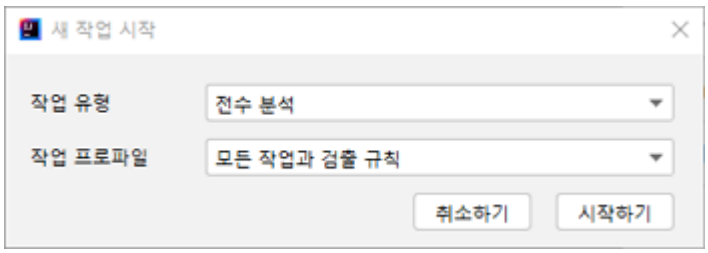
1. **sparrow-plugin** 창의 **프로젝트 목록**에서 앞서 추가한 프로젝트를 선택하세요.

2. **Project** 창에서 분석할 대상을 선택하세요.

3. 마우스 오른쪽 버튼을 클릭하세요.



4. **Run SPARROW**을 클릭하세요.



5. **작업 유형**에서 **전수 분석** 또는 **수시 분석**을 선택하세요.

> **Tip**: **전수 분석**과 **수시 분석**에 대한 설명은 분석을 참고하세요.

6. **작업 프로파일**을 선택하세요.

> **Tip**: **작업 프로파일**은 이슈 검출 규칙과 작업 옵션 등 작업에 필요한 정보를 모아둔 데이터입니다. 자세한 내용은 작업 프로파일을 참고하세요.

7. **시작하기** 버튼을 클릭하세요.

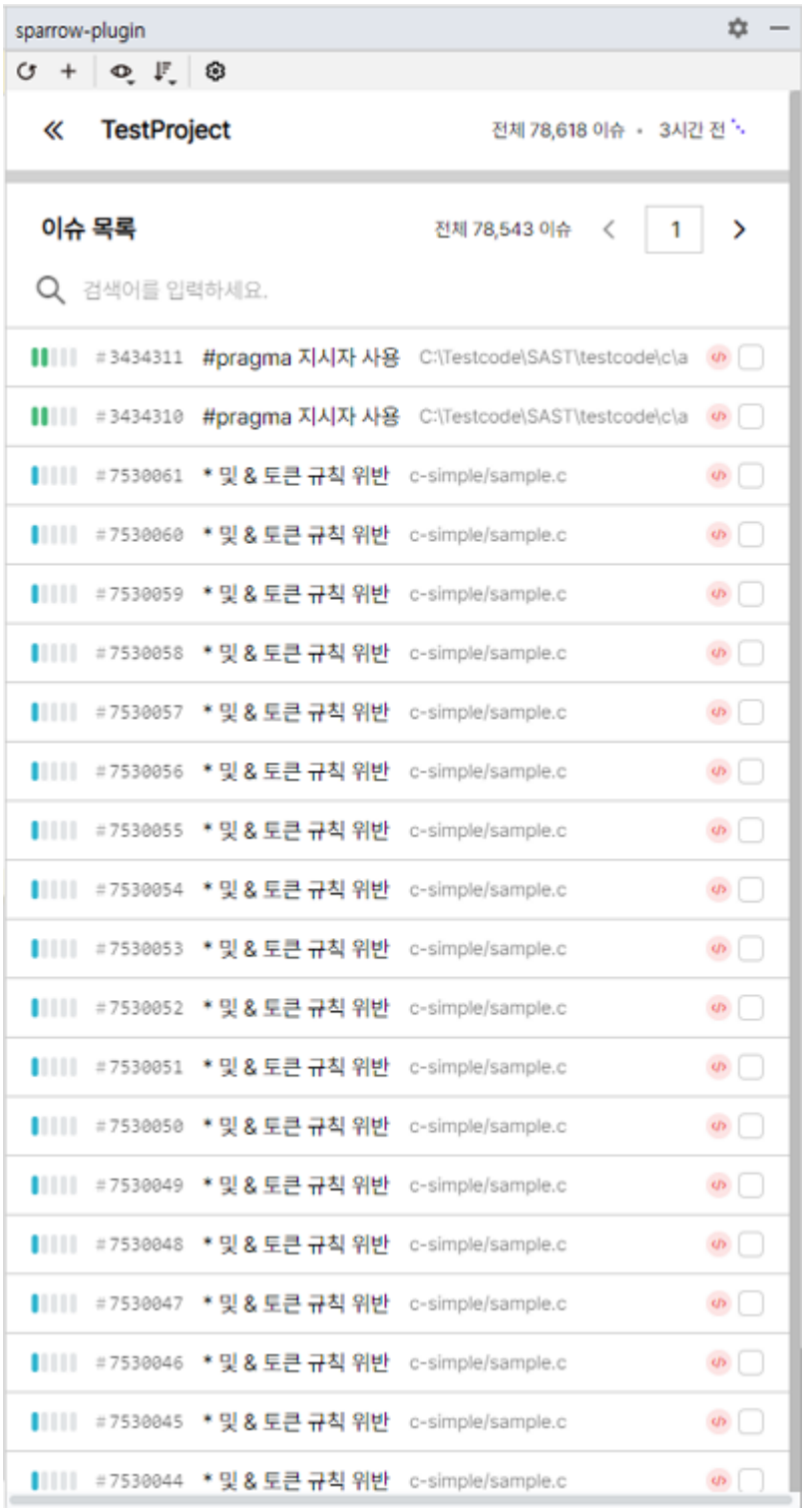
8. 이제 분석이 시작됩니다.

> **Tip**: 분석이 수행되면 **로그** 창에 분석 로그가 표시됩니다.

IntelliJ 플러그인: 결과 확인

분석이 끝나고 결과를 확인하려면 **sparrow-plugin** 창의 **프로젝트 목록**에서 분석을 수행한 프로젝트를 클릭하세요. 해당 분석의 **이슈 목록**이 표시됩니다. 여기서 이슈에 대한 다양한 정보를 확인할 수 있습니다.

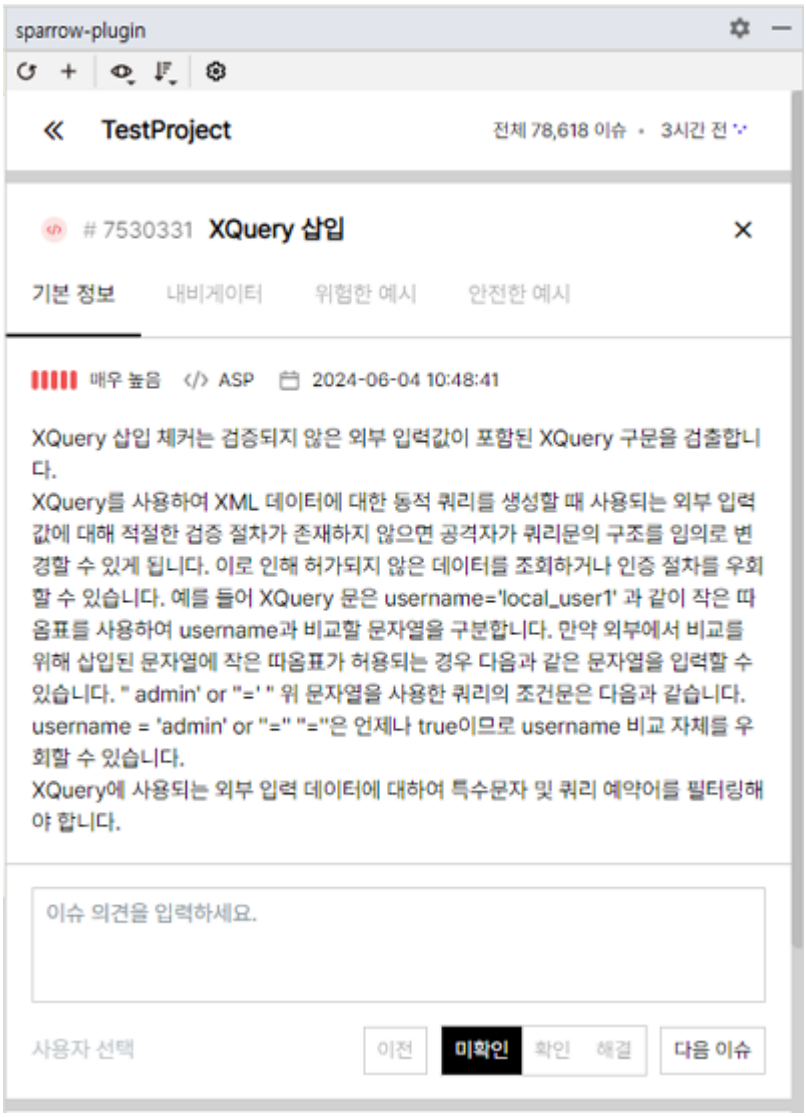
✓ 이슈 목록



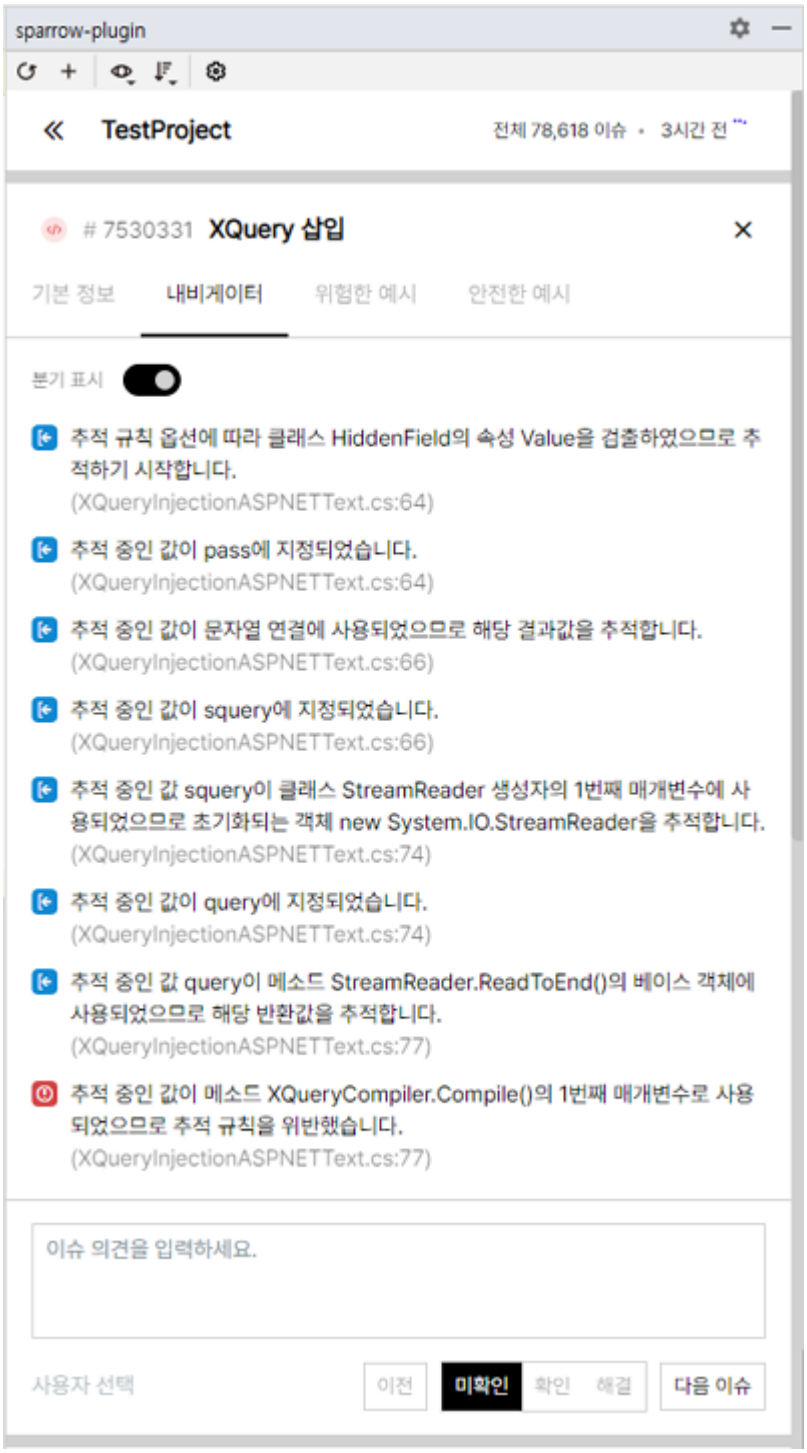
이슈 목록에서는 프로젝트의 최근 이슈 목록을 확인할 수 있습니다. 여기에는 이슈의 **ID**, **유형**, **이슈 이름**, 이슈가 검출된 **자산**, **위험도**, **이슈 상태**가 표시됩니다.

✓ 소스코드 이슈 상세 정보

검출한 이슈에 대한 정보를 표시합니다.



소스코드 이슈 상세 정보에는 이슈 검출 규칙에 대한 기본 정보, 검출된 이슈의 소스코드 라인에 대한 설명인 내비게이터, 해당 이슈에 대한 위험한 예시 및 안전한 예시가 탭으로 표시됩니다.



✓ 이슈 상태

이슈 상세 정보의 맨 아래에 있는 **이슈 톡**에서 **이슈 담당자**를 지정하거나 **이슈 상태**를 변경할 수 있습니다. **이슈 담당자**를 지정하거나 **이슈 상태**를 변경하려면 1) 프로젝트의 **프로젝트 구성원**으로써 프로젝트 권한 중 2) **이슈 참여** 권한을 포함한 프로젝트 역할을 가져야 합니다.

이슈 담당자

해당 이슈를 검토할 담당자를 표시합니다. 권한 있는 사용자 혹은 사용자 그룹 중에서 선택할 수 있으며 담당자를 지정하기 전에는 아무 것도 표시되지 않습니다.

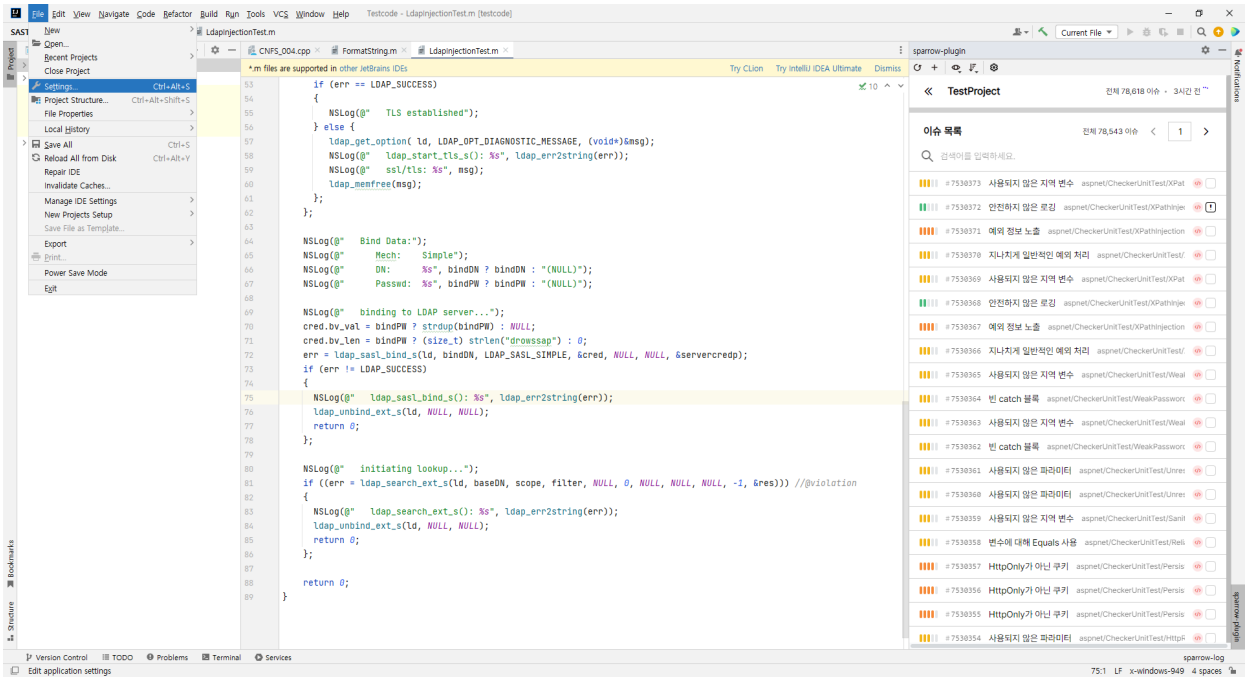
이슈 상태

이슈가 검출되면 해당 이슈를 확인하고 해결하거나, 오탐 또는 다른 원인으로 인해 이슈에서 제외하도록 처리해야 합니다. 이슈를 어떻게 처리했는지 표시하기 위해서 이슈마다 **이슈 상태**를 다음과 같이 표시합니다.

- 미확인 : 담당자가 검출된 이슈를 아직 검토하지 않음
- 확인 : 담당자가 해당 이슈를 확인함
- 해결 : 담당자가 해당 이슈에서 발견된 문제를 해결함

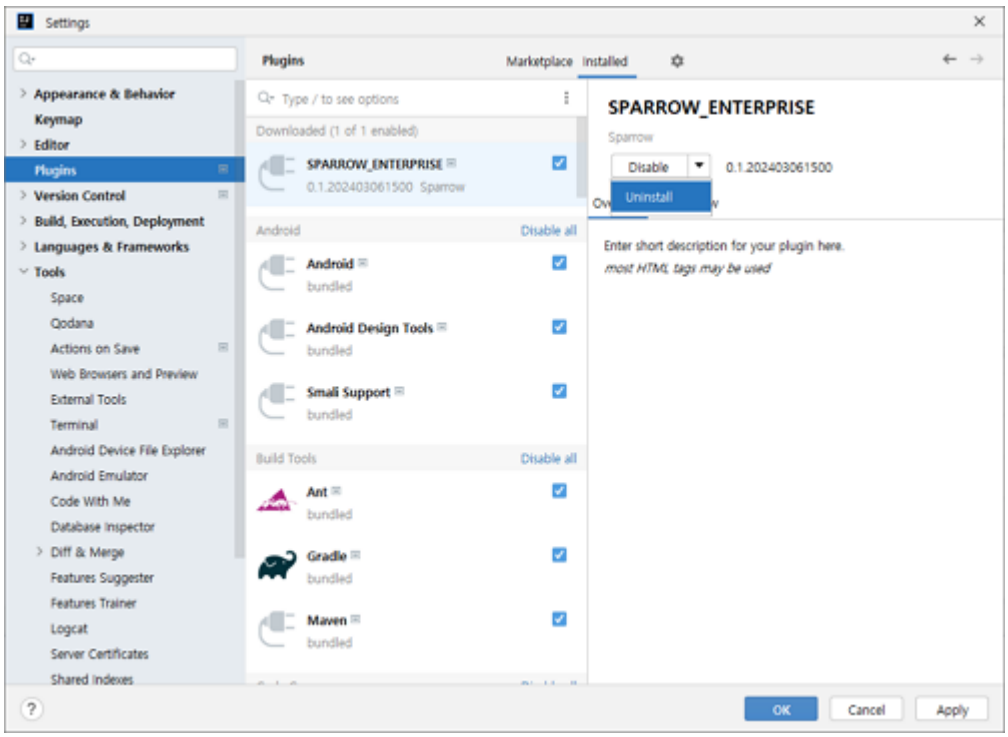
IntelliJ 플러그인: 삭제하기

1. IntelliJ의 **File** 메뉴에서 **Settings**를 클릭하세요.

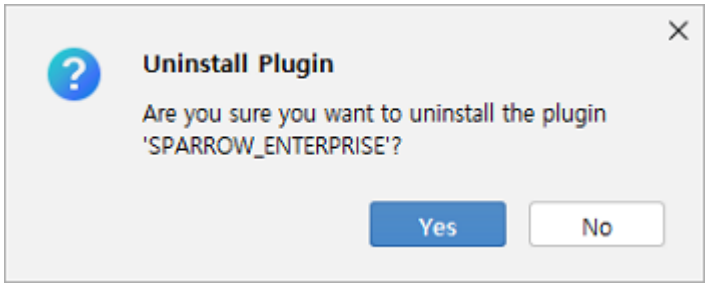


2. **Settings** 창이 표시되면 **Plugin > SPARROW Enterprise**로 이동하세요.

3. 오른쪽 위에 있는 **토글**을 클릭한 후 **Uninstall** 버튼을 클릭하세요.



4. **Plugin Uninstall** 창에서 **Yes** 버튼을 클릭하세요.



5. **OK** 버튼을 클릭하여 IntelliJ 플러그인을 삭제하세요.

6. 이제 삭제가 완료되었습니다.

Visual Stuido Code 플러그인

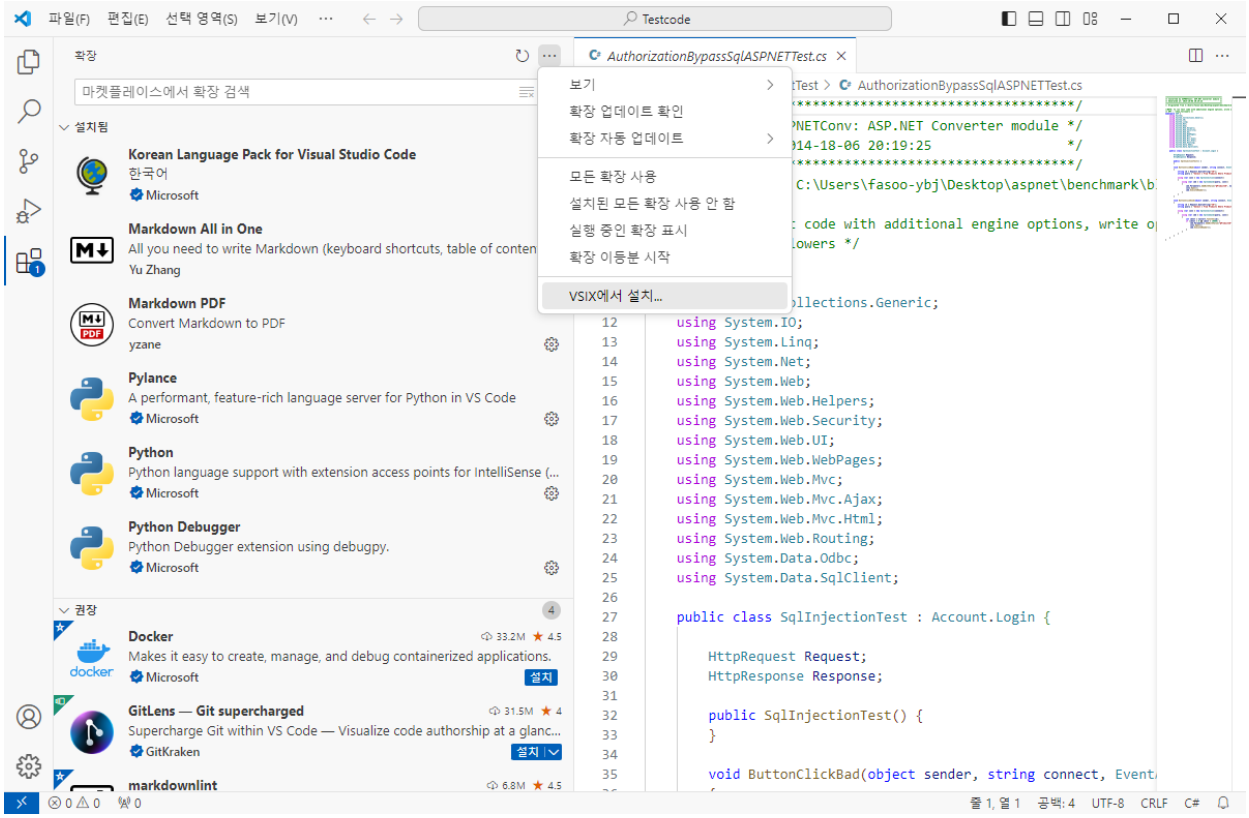
개발 단계에서 Visual Stuido Code를 주로 사용하신다면 Visual Stuido Code 플러그인을 설치해서 간단하게 분석을 수행할 수 있습니다. Visual Stuido Code 플러그인은 클라이언트를 사용하는 분석 방법이기 때문에 먼저 클라이언트를 설치해야 합니다. 클라이언트를 설치하는 방법은 클라이언트 설치하기를 참고하세요.

Visual Stuido Code 플러그인: 설치하기

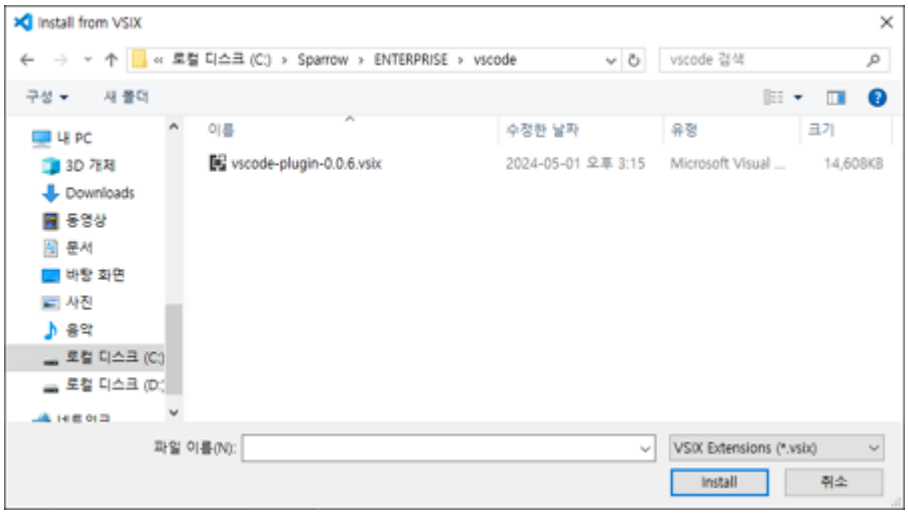
1. **Visual Stuido Code**를 실행하세요.

2. 왼쪽 사이드 메뉴에서 **확장** 아이콘을 클릭하세요.

3. **더보기** 아이콘을 클릭하고 **VSIX에서 설치**를 클릭하세요.



4. **Sparrow Enterprise 플러그인 파일**을 선택하세요.



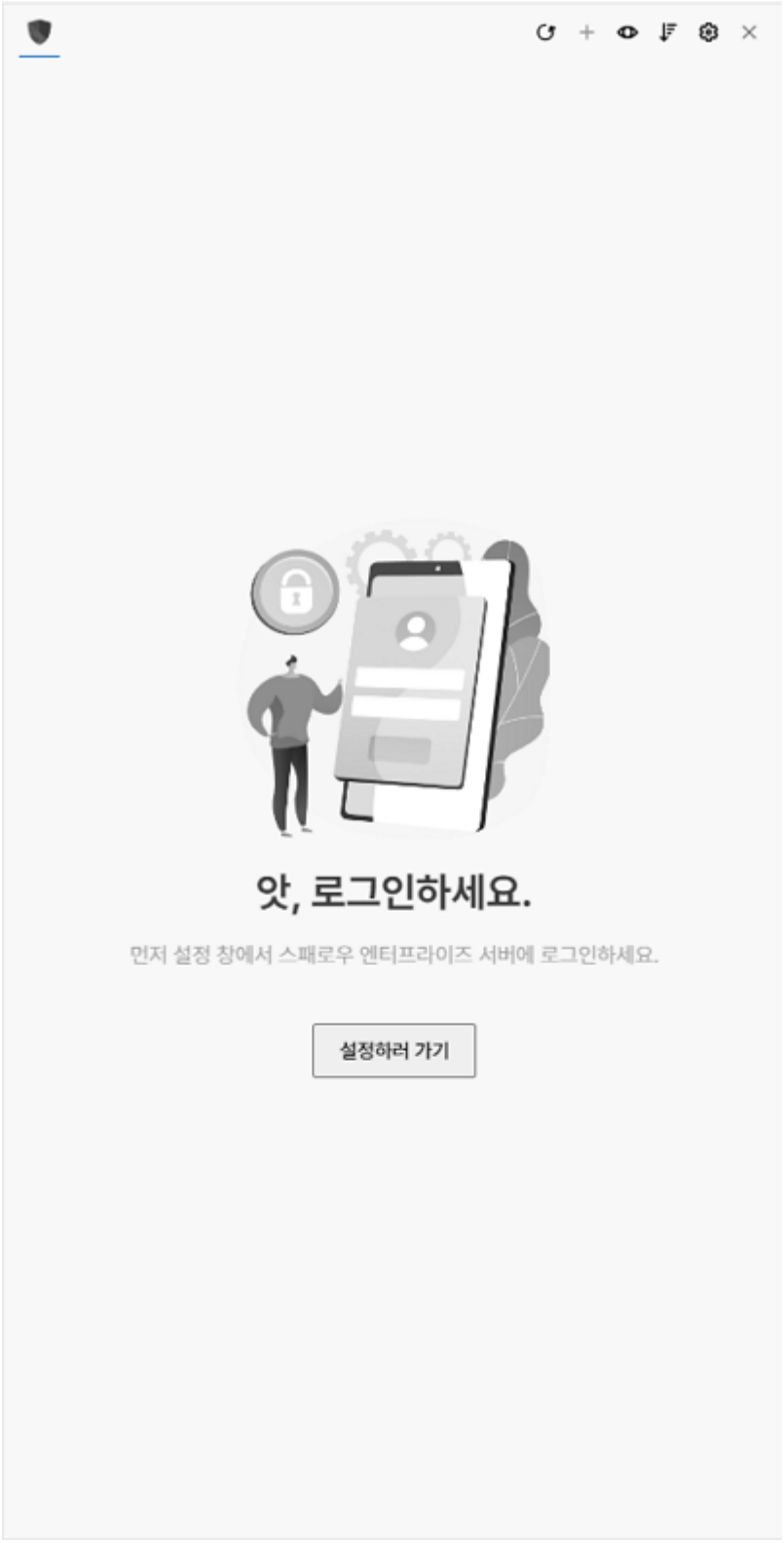
5. 플러그인이 설치되면 Visual Stuido Code를 다시 시작하세요

6. 설치가 완료되었습니다.

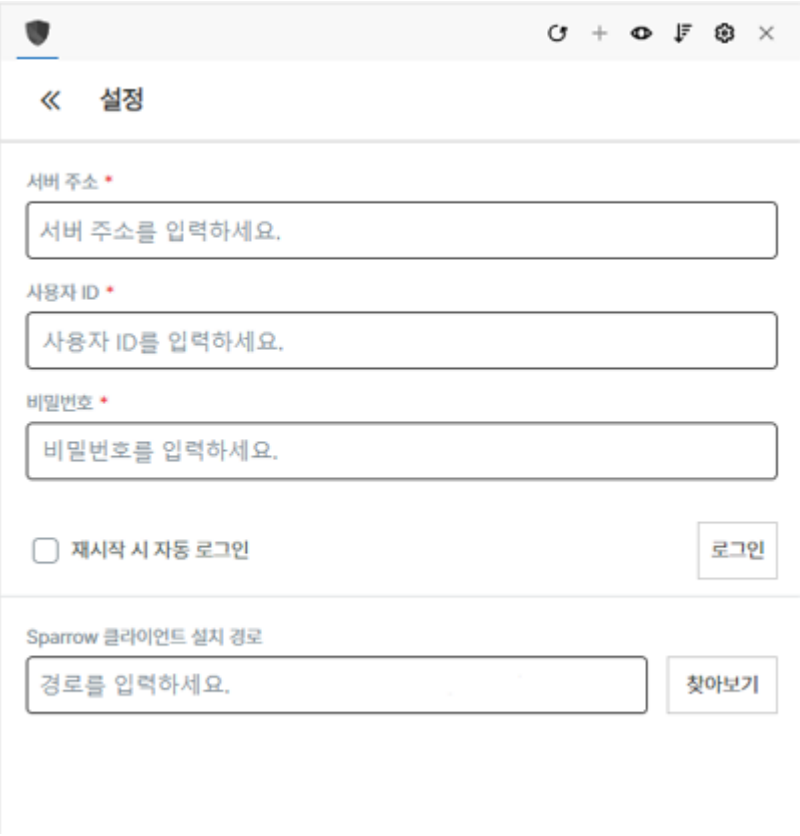
Visual Stuido Code 플러그인: 로그인하기

Sparrow Enterprise 웹에 한 번도 로그인하지 않은 사용자 계정은 올바른 사용자 ID와 비밀번호를 입력하더라도 Visual Stuido Code 플러그인과 같은 클라이언트에 로그인할 수 없습니다. 따라서 Sparrow Enterprise 웹에 먼저 로그인하여 비밀번호를 변경한 후, 변경한 비밀번호로 플러그인에 로그인해야 합니다.

1. **파일 탐색기** 창에서 가장 아래에 있는 **SPARROW ENTERPRISE** 섹션을 펼치세요.



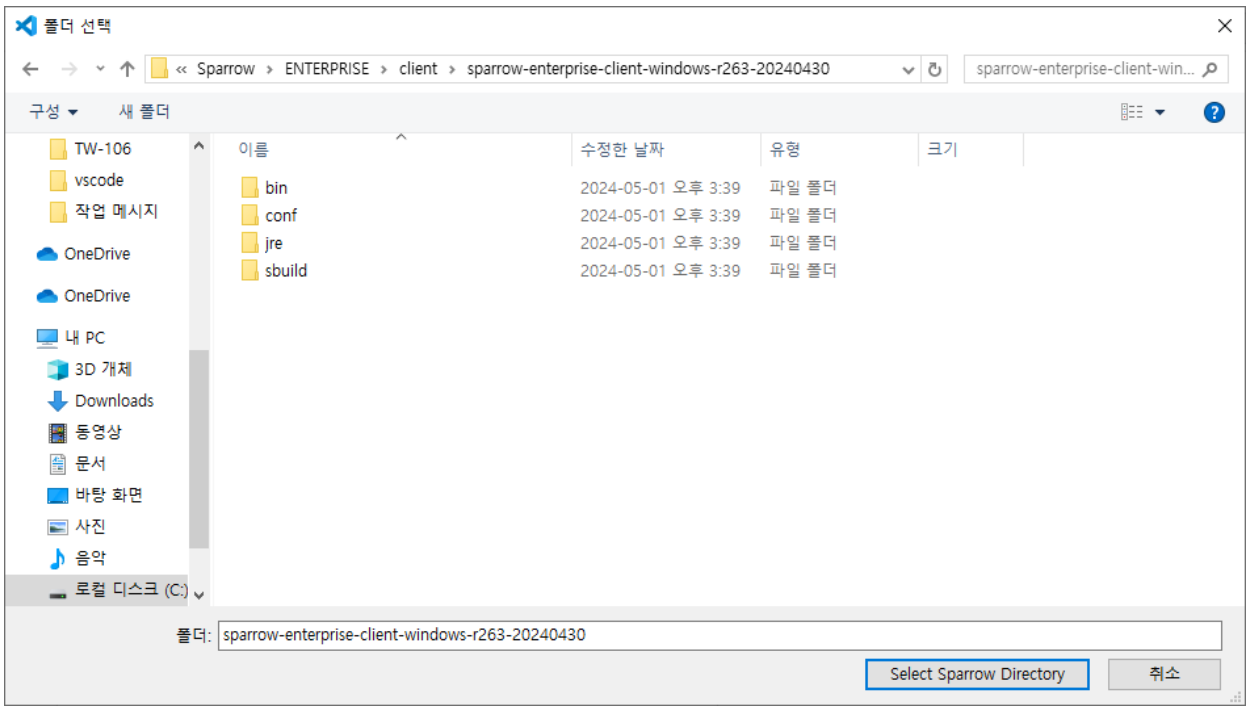
2. **SPARROW ENTERPRISE** 섹션에서 **설정하러 가기**를 클릭하세요.



3. **서버 주소**, **사용자 ID**, **비밀번호**를 입력하고 **로그인** 버튼을 클릭하세요.

> **Tip**: **재시작 시 자동 로그인** 체크 박스를 선택하면 Visual Stuido Code를 실행할 때 자동으로 로그인하게 됩니다.

4. **Sparrow 클라이언트 설치 경로**에서 **찾아보기** 버튼을 클릭하세요.



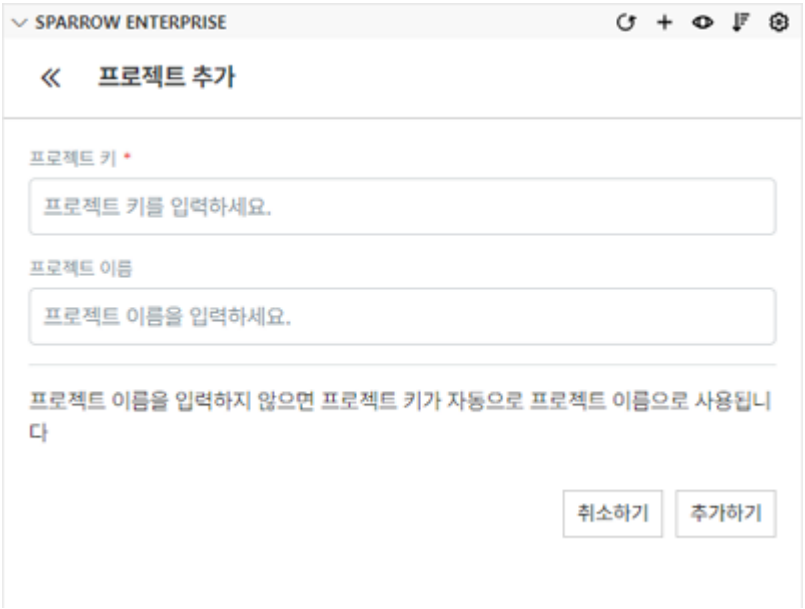
5. 로컬에 설치된 Sparrow Enterprise 클라이언트 경로를 선택하고 **Sparrow 경로 선택**을 클릭하세요.

6. 이제 Visual Stuido Code 플러그인에서 Sparrow Enterprise에 로그인되었습니다.

Visual Stuido Code 플러그인: 프로젝트 추가하기

먼저 분석을 수행할 프로젝트를 추가하겠습니다.

1. **SPARROW ENTERPRISE** 섹션의 **프로젝트 목록**에서 **더하기** 아이콘을 클릭하세요.
2. **프로젝트 키**, **프로젝트 이름**을 입력하세요.

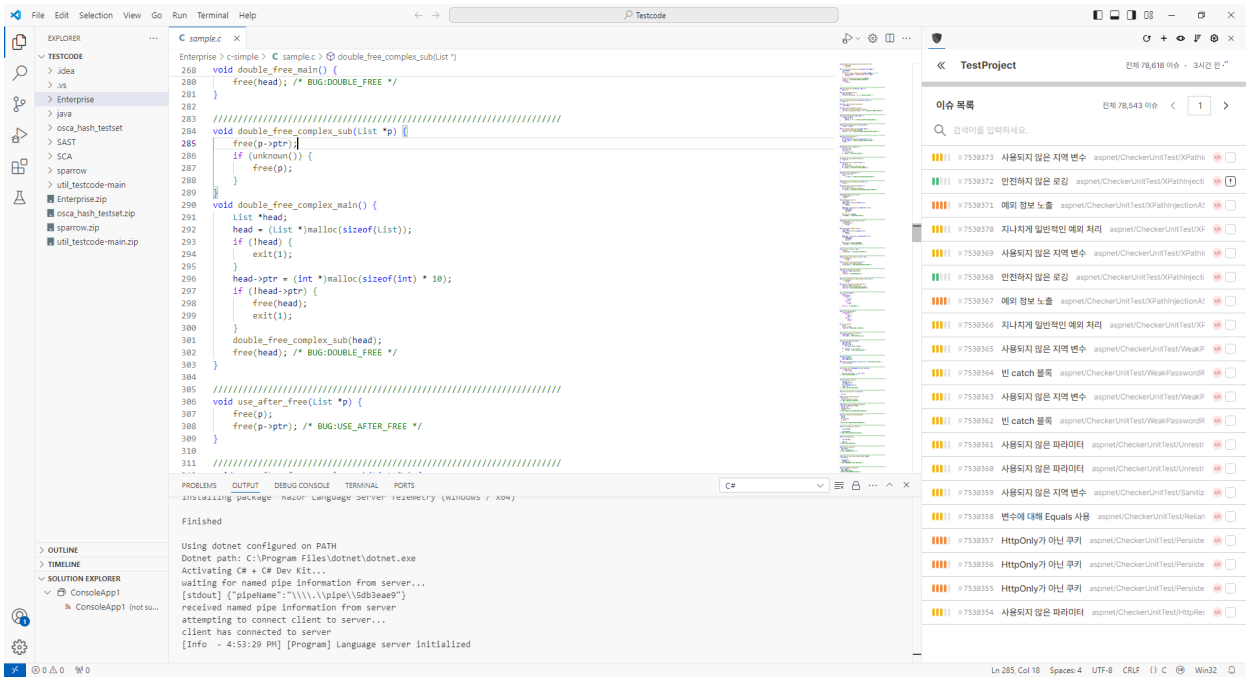


3. **추가하기** 버튼을 클릭하세요.

Visual Stuido Code 플러그인: 분석하기

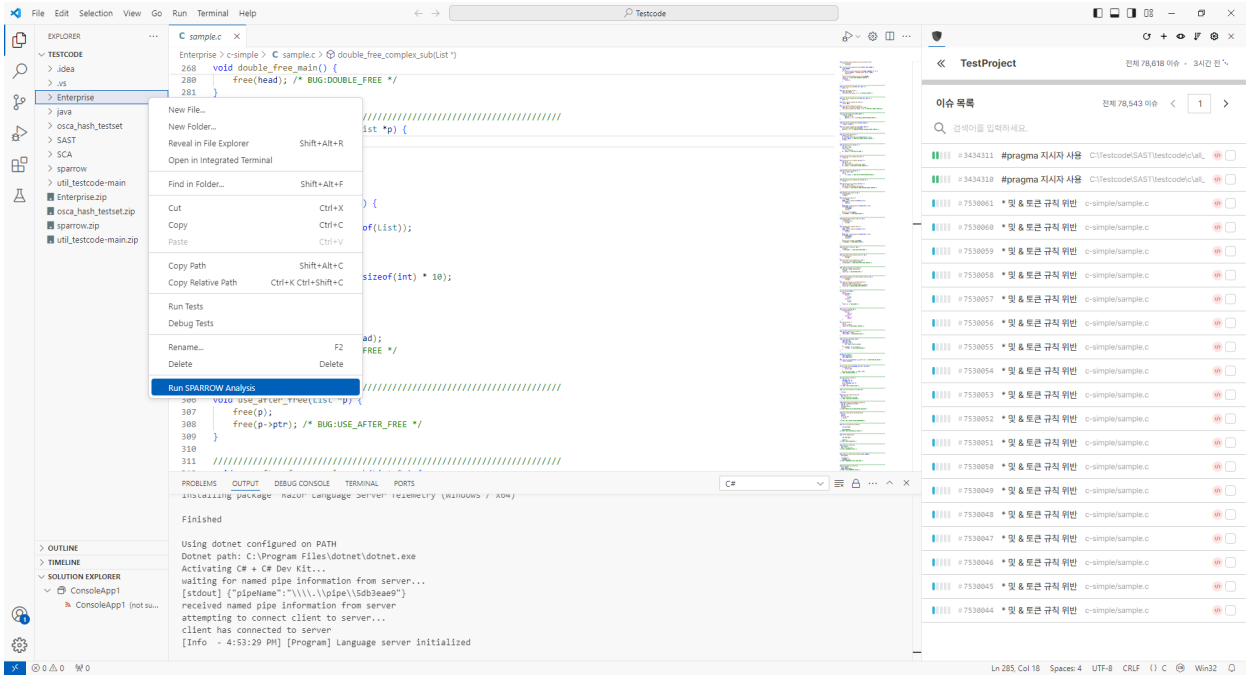
이제 Sparrow Enterprise 클라이언트에 연결된 Visual Stuido Code 플러그인을 사용하여 소스코드 이슈 및 컴포넌트 이슈를 분석할 수 있습니다. 분석할 때 프로젝트, 패키지, 파일 등 사용자가 원하는 분석 대상을 선택하여 분석할 수 있습니다.

1. **SPARROW ENTERPRISE** 섹션의 **프로젝트 목록**에서 앞서 추가한 프로젝트를 선택하세요.

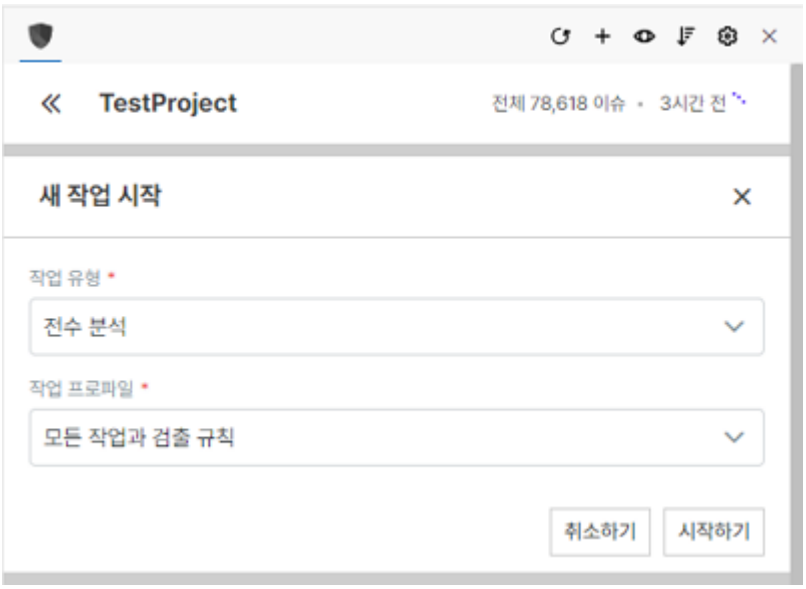


2. Visual Stuido Code의 **탐색기** 창에서 분석할 대상을 선택하세요.

3. 마우스 오른쪽 버튼을 클릭하세요.



4. **Run SPARROW Analysis**를 클릭하세요.



5. **작업 유형**에서 **전수 분석** 또는 **수시 분석**을 선택하세요.

> **Tip**: **전수 분석**과 **수시 분석**에 대한 설명은 분석을 참고하세요.

6. **작업 프로파일**을 선택하세요.

> **Tip**: **작업 프로파일**은 이슈 검출 규칙과 작업 옵션 등 작업에 필요한 정보를 모아둔 데이터입니다. 자세한 내용은 작업 프로파일을 참고하세요.

7. **시작하기** 버튼을 클릭하세요.

8. 이제 분석이 시작됩니다.

> **Tip**: 분석이 수행되면 **출력** 창에 분석 로그가 표시됩니다.

Visual Stuido Code 플러그인: 결과 확인

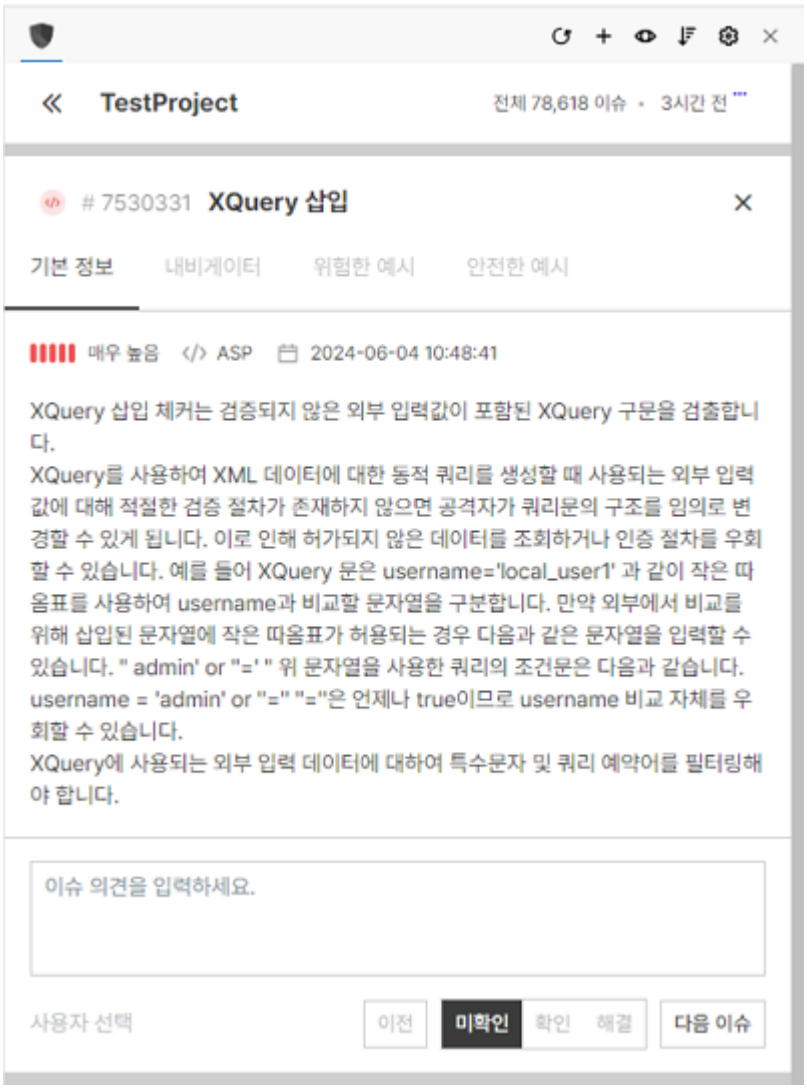
분석이 끝나고 결과를 확인하려면 **SPARROW ENTERPRISE** 섹션의 **프로젝트 목록**에서 분석을 수행한 프로젝트를 클릭하세요. 해당 분석의 **이슈 목록**이 표시됩니다. 여기서 이슈에 대한 다양한 정보를 확인할 수 있습니다.

✓ 이슈 목록

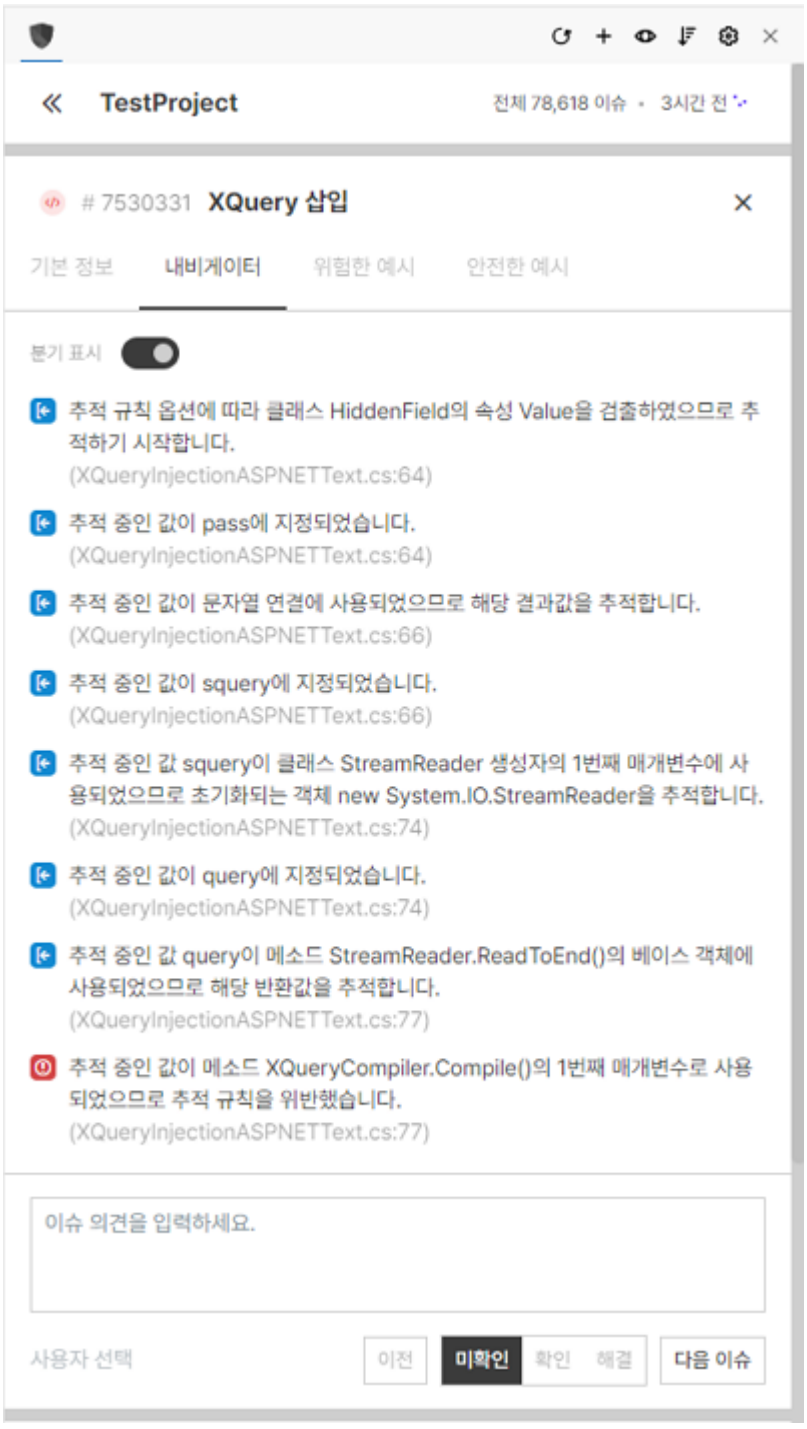
이슈 목록에서는 프로젝트의 최근 이슈 목록을 확인할 수 있습니다. 여기에는 이슈의 **ID**, **유형**, **이슈 이름**, 이슈가 검출된 **자산**, **위험도**, **이슈 상태**가 표시됩니다.

✓ 소스코드 이슈 상세 정보

검출한 이슈에 대한 정보를 표시합니다.



소스코드 이슈 상세 정보에는 이슈 검출 규칙에 대한 기본 정보, 검출된 이슈의 소스코드 라인에 대한 설명인 내비게이터, 해당 이슈에 대한 위험한 예시 및 안전한 예시가 탭으로 표시됩니다.



✓ 이슈 상태

이슈 상세 정보의 맨 아래에 있는 **이슈 톡**에서 **이슈 담당자**를 지정하거나 **이슈 상태**를 변경할 수 있습니다. **이슈 담당자**를 지정하거나 **이슈 상태**를 변경하려면 1) 프로젝트의 **프로젝트 구성원**으로써 프로젝트 권한 중 2) **이슈 참여** 권한을 포함한 프로젝트 역할을 가져야 합니다.

이슈 담당자

해당 이슈를 검토할 담당자를 표시합니다. 권한 있는 사용자 혹은 사용자 그룹 중에서 선택할 수 있으며 담당자를 지정하기 전에는 아무 것도 표시되지 않습니다.

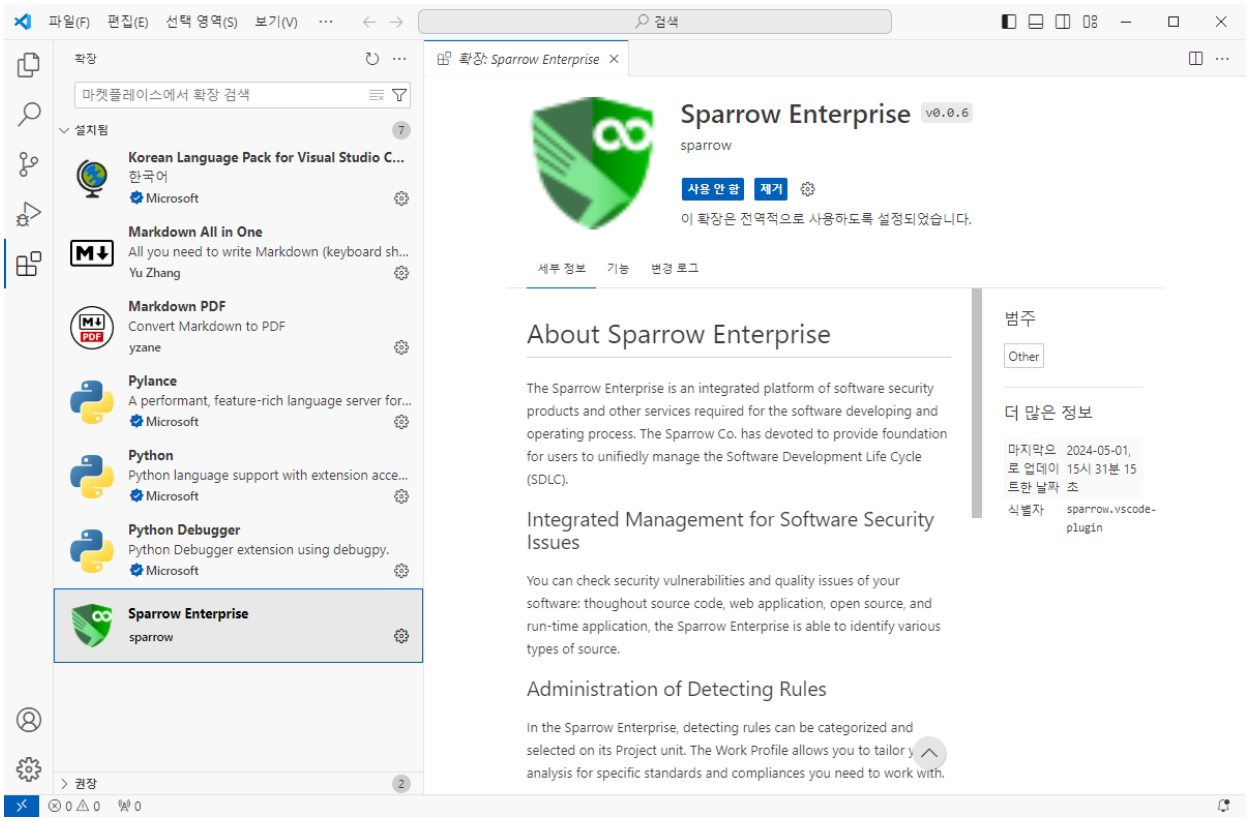
이슈 상태

이슈가 검출되면 해당 이슈를 확인하고 해결하거나, 오탐 또는 다른 원인으로 인해 이슈에서 제외하도록 처리해야 합니다. 이슈를 어떻게 처리했는지 표시하기 위해서 이슈마다 **이슈 상태**를 다음과 같이 표시합니다.

- 미확인 : 담당자가 검출된 이슈를 아직 검토하지 않음
- 확인 : 담당자가 해당 이슈를 확인함
- 해결 : 담당자가 해당 이슈에서 발견된 문제를 해결함

Visual Stuido Code 플러그인: 삭제하기

1. 왼쪽 사이드 메뉴에서 **확장** 아이콘을 클릭하세요.
2. **Sparrow Enterprise**를 클릭하세요.

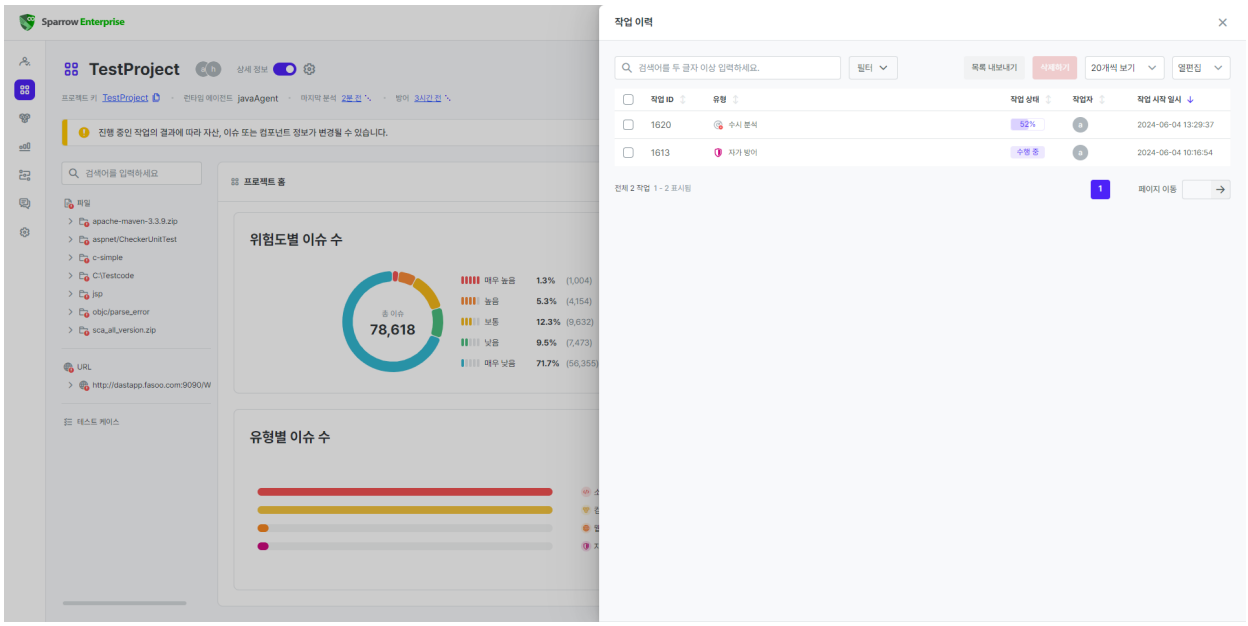


3. 오른쪽 창에서 **제거** 버튼을 클릭하세요.
4. 이제 삭제가 완료되었습니다.

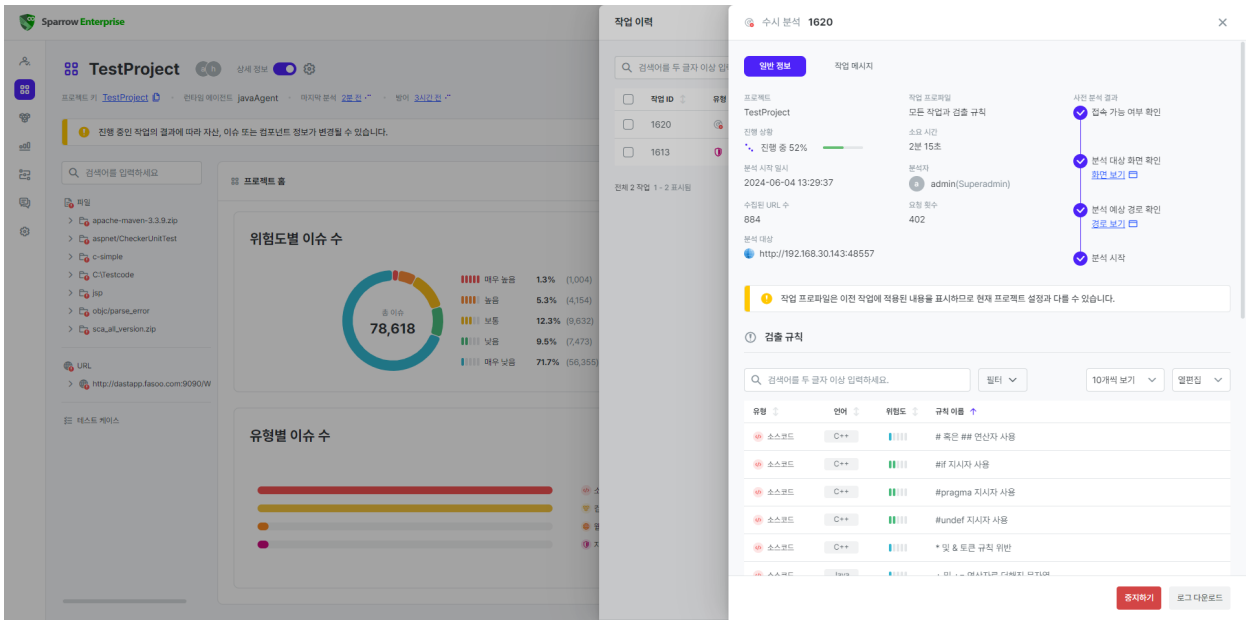
분석 중지하기

수행 중인 분석을 종료하려면 1) 프로젝트의 **프로젝트 구성원**으로써 프로젝트 권한 중 2) **작업 관리** 권한을 포함한 프로젝트 역할을 가져야 합니다. 자세한 내용은 다음을 참고하세요.

1. 프로젝트 상세 정보의 오른쪽 위에 있는 **작업 이력 보기** 버튼을 클릭하세요.



2. 진행 중인 **분석**을 선택하세요.



3. 슬라이드 아래에서 **중지하기** 버튼을 클릭하세요.

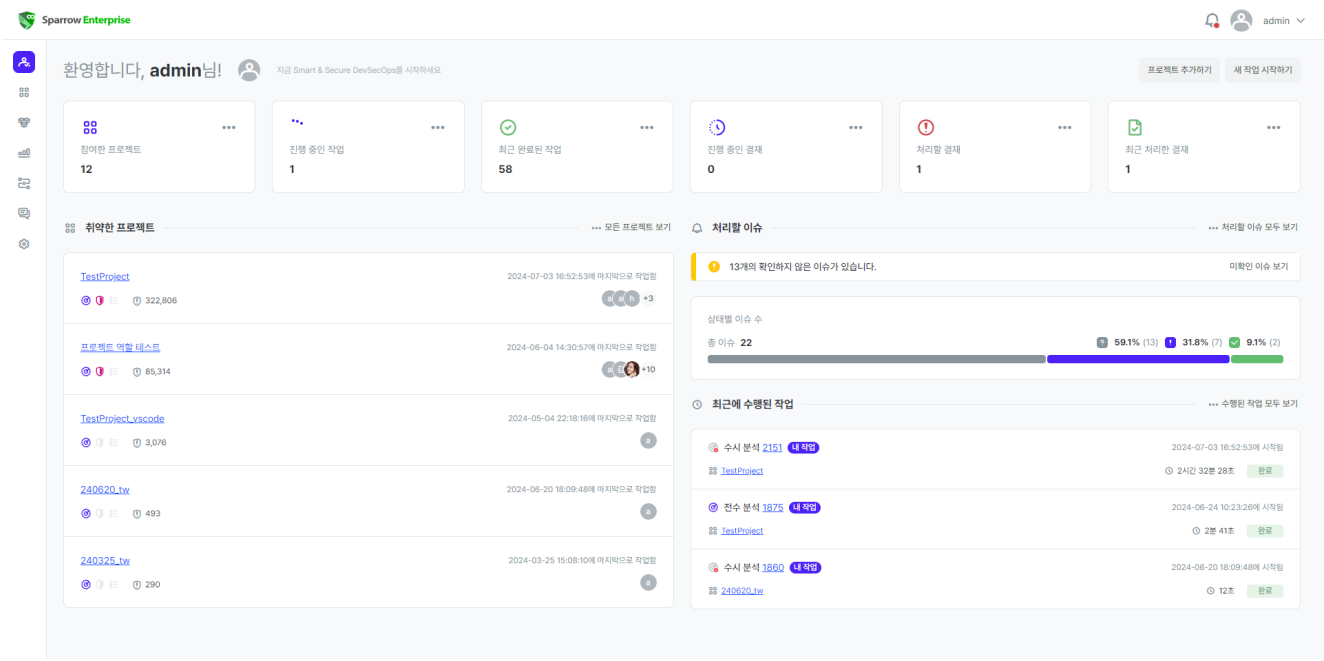
> **Tip**: 프로젝트의 **작업 관리** 권한이 있는 사용자는 **작업 이력** 슬라이드에서 분석을 삭제할 수도 있습니다. 자세한 내용은 분석 삭제하기를 참고하세요.

결과 확인

앞에서 수행한 분석 결과를 확인하기 위해서는 브라우저를 통해 Sparrow Enterprise 서버로 이동해야 합니다. CLI 명령어로도 프로젝트 결과를 간단히 확인할 수 있습니다. 자세한 내용은 클라이언트 CLI로 프로젝트 확인을 참고하세요.

마이페이지 확인하기

Sparrow Enterprise에 로그인하면 가장 먼저 표시되는 페이지가 마이페이지입니다. 마이페이지에서는 내 계정과 관련된 프로젝트 및 이슈에 대한 정보를 확인할 수 있습니다. 화면 왼쪽 위에 있는 **Sparrow Enterprise 로고**나 사이드 바에 있는 **마이페이지** 아이콘을 클릭하여 마이페이지로 이동하세요. 마이페이지는 다음과 같은 내용을 표시합니다.



✓ 내 요약 정보

참여한 프로젝트

사용자 계정이 구성원으로 포함된 프로젝트의 개수입니다. 더보기 아이콘을 클릭하면 **프로젝트 목록**으로 이동합니다.

진행 중인 작업

사용자 계정이 프로젝트에서 수행한 작업 중에서 현재 **준비** 중이거나 **진행 중**인 작업의 개수입니다. 더보기 아이콘을 클릭하면 **수행한 작업 목록**으로 이동합니다.

최근 완료된 작업

사용자 계정이 프로젝트에서 수행한 작업 중에서 최근 30일 동안 **완료**된 작업의 개수입니다. 더보기 아이콘을 클릭하면 **수행한 작업 목록**으로 이동합니다.

진행 중인 결재

사용자 계정이 요청한 결재 중에서 현재 **진행 중**인 결재의 개수입니다. 더보기 아이콘을 클릭하면 **요청한 결재 목록**으로 이동합니다.

처리할 결재

사용자 계정이 처리할 수 있는 결재의 개수입니다. 더보기 아이콘을 클릭하면 **처리할 결재 목록**으로 이동합니다.

최근 처리한 결재

사용자 계정이 최근 30일 동안 처리한 결재의 개수입니다. 더보기 아이콘을 클릭하면 **처리한 결재 목록**으로 이동합니다.

> **Tip**: **결재**에 대한 설명은 이슈 제외하기를 참고하세요.

✓ 취약한 프로젝트

사용자 계정이 구성원으로 포함된 프로젝트 중 이슈를 기준으로 가장 많은 이슈가 검출된 5개 프로젝트를 카드로 표시합니다. 카드 오른쪽 위에 있는 **모든 프로젝트 보기**를 클릭하면 **전체 프로젝트 목록**으로 이동합니다.

✓ 처리할 이슈

사용자 계정이 담당자로 지정된 이슈의 상태 및 개수를 그래프로 표시합니다. 그래프 오른쪽 위에 있는 **처리할 이슈 모두 보기**를 클릭하면 **처리할 이슈 목록**으로 이동합니다.

✓ 최근에 수행된 작업

사용자 계정이 구성원으로 포함된 프로젝트에서 수행된 작업 중 최근 3개 작업을 카드로 표시합니다. 카드를 클릭하면 해당 작업의 요약 정보 페이지로 이동합니다. 카드 오른쪽 위에 있는 **수행된 작업 모두 보기**를 클릭하면 **수행한 작업 목록**으로 이동합니다.

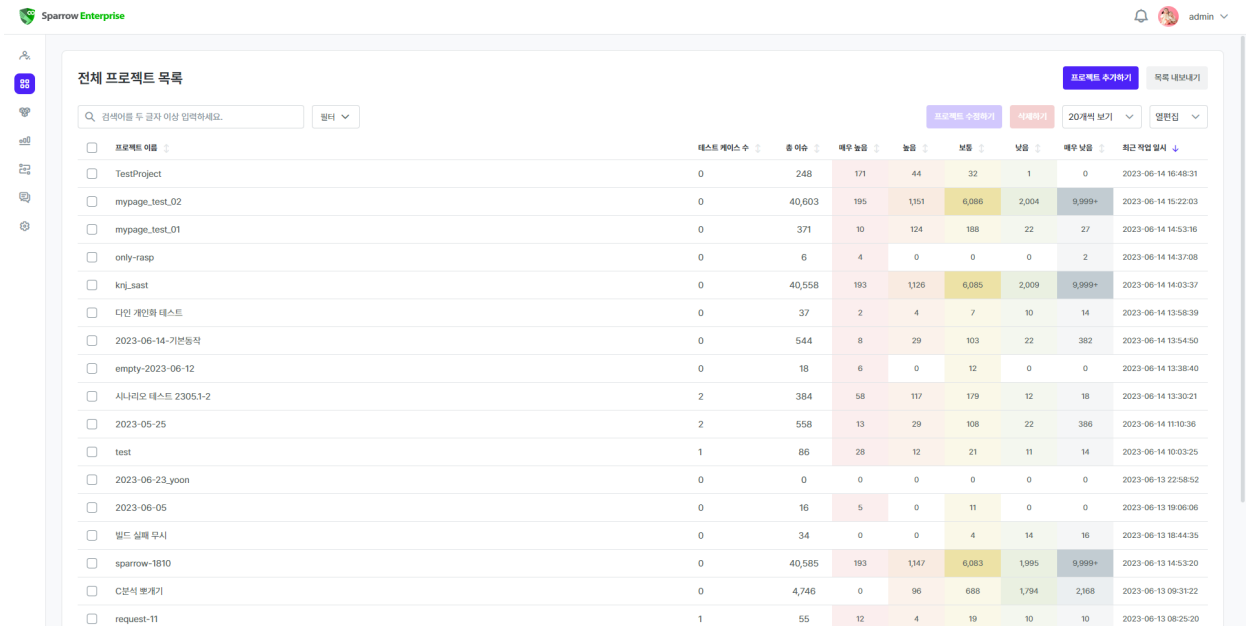
프로젝트 확인하기

이제 본격적으로 Sparrow Enterprise에서 만든 프로젝트와 수행한 분석에 대한 결과를 확인하고 이슈가 무엇인지 알아보도록 하겠습니다.

웹 서버에서 프로젝트 확인

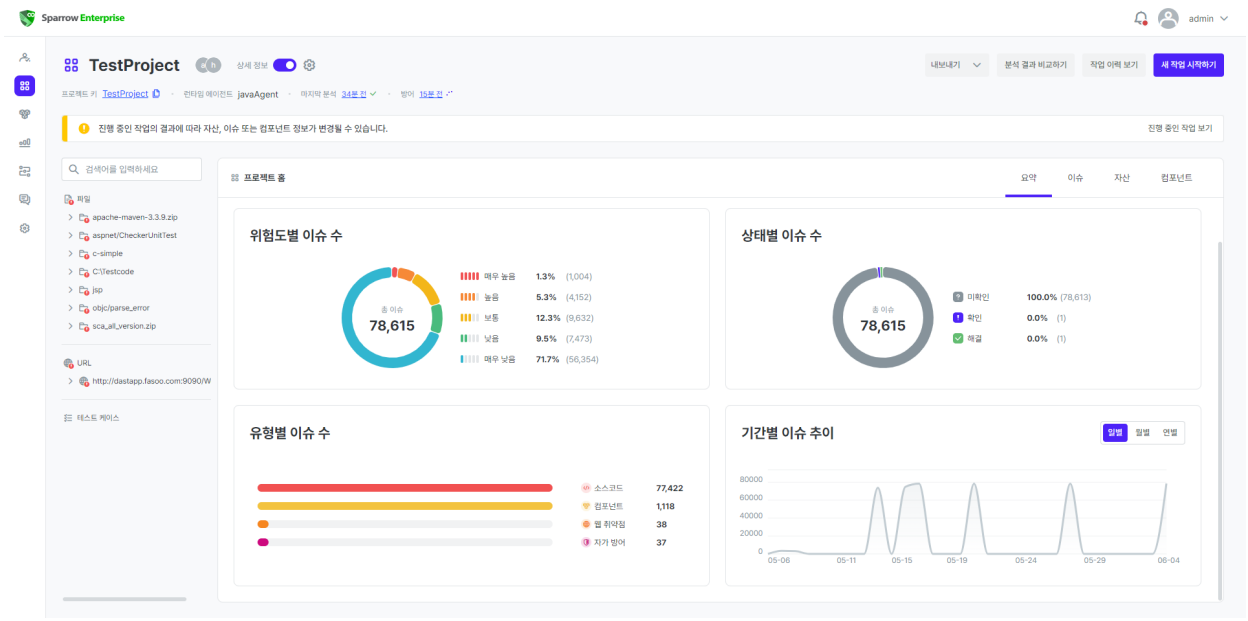
프로젝트를 확인하기 위해서는 다음을 참고하세요.

1. 사이드 바에서 **프로젝트 목록** 아이콘을 클릭하세요.

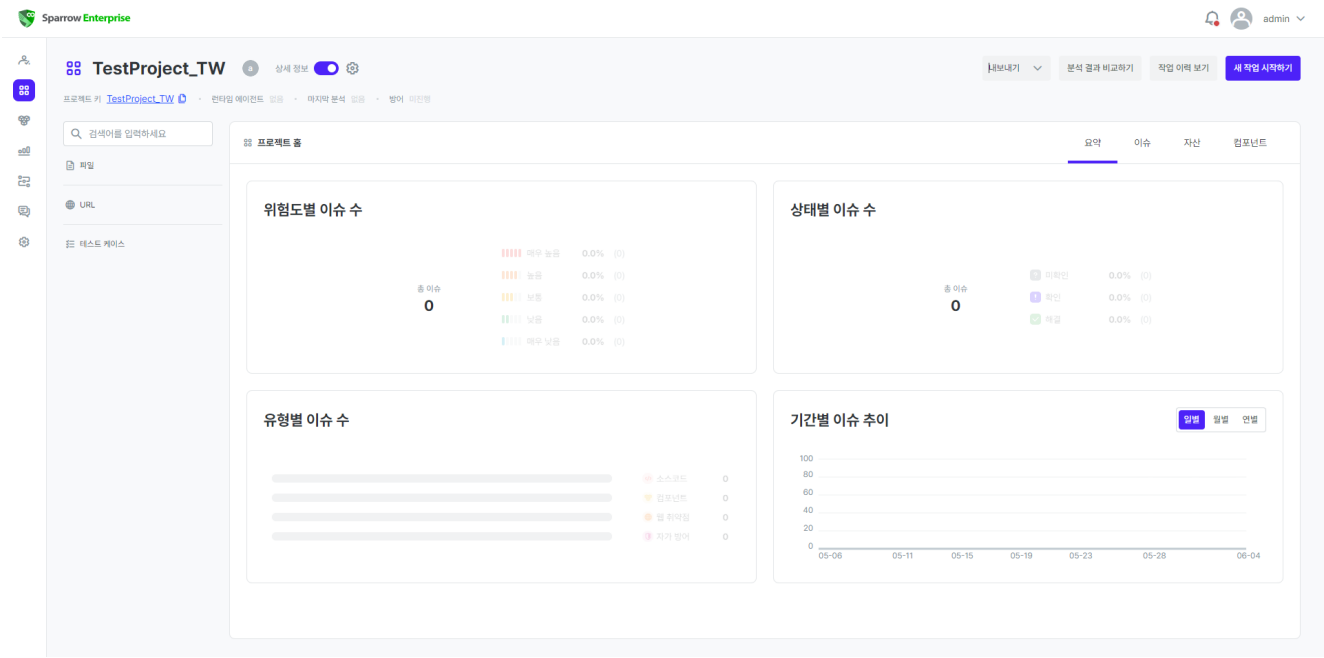


2. **전체 프로젝트 목록** 페이지에서 확인하려는 프로젝트 이름을 클릭하세요.

3. 그러면 해당 프로젝트의 **프로젝트 상세 정보**로 이동합니다.



Tip: 작업을 수행하기 전에는 다음과 같이 결과가 표시되지 않습니다.



프로젝트 상세 정보 페이지에 표시되는 항목은 아래 내용을 참고하세요.

✓ SBOM

오른쪽 위에 있는 **SBOM 내보내기** 버튼을 클릭해서 프로젝트에서 수집한 SBOM을 출력할 수 있습니다. 자세한 내용은 SBOM 내보내기를 참고하세요.

✓ 프로젝트 기본 정보, 구성원, 작업 프로파일, 웹훅

권한 있는 사용자는 오른쪽 위에 있는 **프로젝트 수정하기** 버튼을 클릭해서 프로젝트에 대한 정보를 확인하고 변경할 수 있습니다. 자세한 내용은 프로젝트 수정하기를 참고하세요.

✓ 작업 이력

오른쪽 위에 있는 **작업 이력 보기**를 클릭하면 프로젝트에서 수행한 모든 작업에 대한 정보를 확인할 수 있습니다. 자세한 내용은 작업 이력 확인하기를 참고하세요.

✓ 자산 트리

왼쪽에는 분석 작업에서 사용된 분석 대상인 **파일**, **URL**을 **자산**이라는 정보가 표시됩니다. **자산**에 표시된 파일이나 URL을 클릭하면 클릭한 자산에서 검출된 이슈가 **이슈** 목록에 표시됩니다. 프로젝트 상세 정보의 탭에도 **자산** 탭이 추가되었습니다.

✓ 요약

요약 탭에서는 프로젝트에서 검출한 최근 이슈를 다음과 같은 네 개의 그래프로 표시합니다. 단, Sparrow TSO 제품 라이선스만 소유한 경우에는 테스트 케이스에 대한 데이터를 테이블로 표시합니다.

위험도별 이슈 수

프로젝트에서 검출된 최근 이슈의 개수를 **매우 높음**, **높음**, **보통**, **낮음**, **매우 낮음**이라는 위험도에 따라 5단계로 구분합니다.

상태별 이슈 수

프로젝트에서 검출된 최근 이슈의 개수를 **미확인**, **확인**, **해결**이라는 상태에 따라 3개로 구분합니다.

유형별 이슈 수

프로젝트에서 검출된 최근 이슈의 개수를 **소스코드**, **컴포넌트**, **웹 취약점**, **자가 방어**라는 분석 도구에 따라 4개로 구분합니다.

기간별 이슈 추이

프로젝트에서 검출된 최근 이슈가 검출된 날짜와 이슈의 개수를 그래프로 표시합니다.

> **Tip**: 프로젝트 상세 정보에 표시되는 이슈는 모두 **최근 이슈**입니다. **최근 이슈**에 대한 자세한 내용은 최근 이슈 확인하기를 참고하세요.

✓ 이슈

이슈 탭에서는 프로젝트에서 검출한 최근 이슈를 목록으로 표시합니다. 자세한 내용은 최근 이슈 확인하기를 참고하세요.

✓ 자산

자산 탭에서는 분석에 사용한 분석 대상인 **파일**과 **URL**을 목록으로 표시합니다. 자세한 내용은 최근 자산 확인하기를 참고하세요.

✓ 컴포넌트

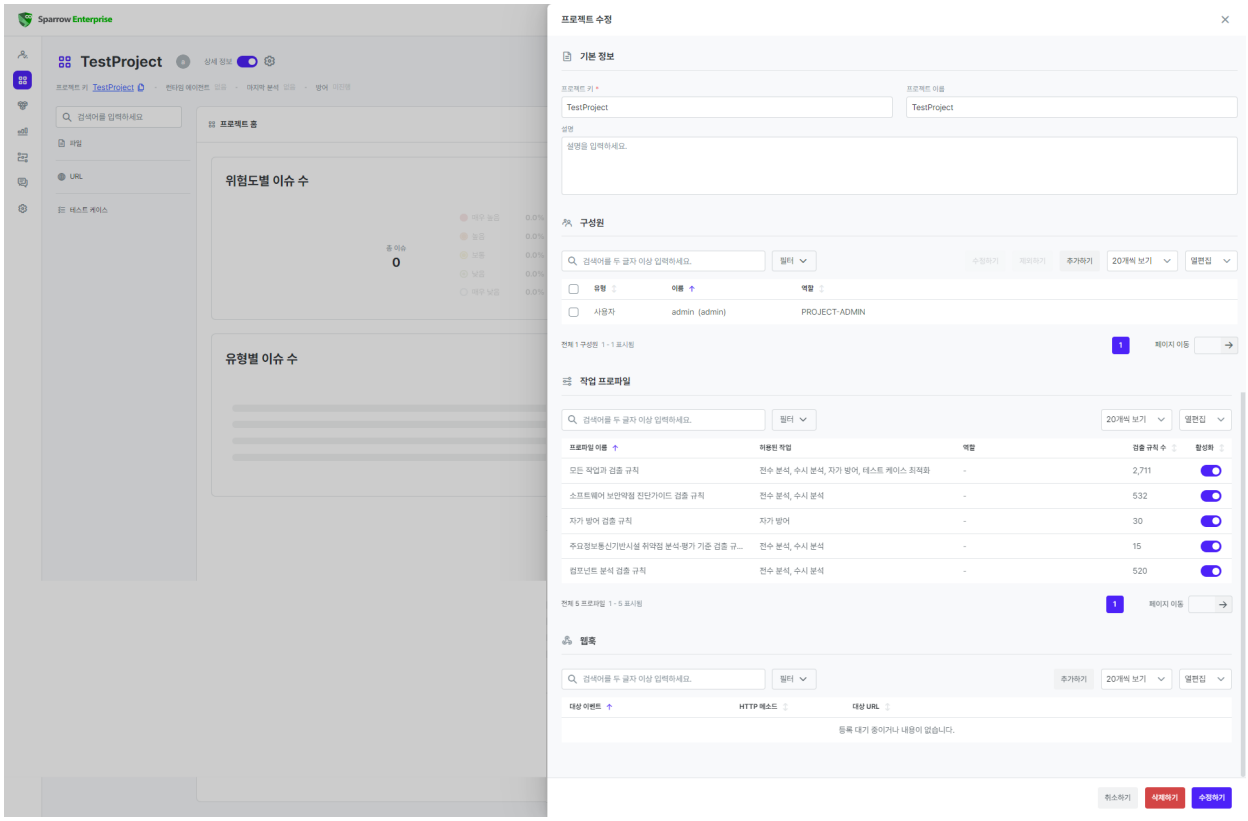
컴포넌트 탭에서는 프로젝트에서 검출한 최근 컴포넌트를 목록으로 표시합니다. 자세한 내용은 최근 컴포넌트 확인하기를 참고하세요.

프로젝트 수정하기

프로젝트에서는 **프로젝트 키**, **프로젝트 이름**, **프로젝트 설명**과 같은 **기본 정보**를 변경할 수 있습니다. 또한 프로젝트에서 사용할 **작업 프로파일**을 활성화하거나 프로젝트의 **구성원**, **웹훅**을 추가하고 삭제할 수 있습니다.

프로젝트 설정을 수정하려면 1) 프로젝트의 **프로젝트 구성원**으로써 프로젝트 권한 중 2) **프로젝트 수정** 권한을 포함한 프로젝트 역할을 가져야 합니다. 혹은 시스템의 **프로젝트 관리** 권한이 있는 관리자도 프로젝트 설정을 수정할 수 있습니다. 자세한 내용은 다음을 참고하세요.

1. 프로젝트 상세 정보 페이지로 이동하세요.
2. 오른쪽 위에 있는 **프로젝트 수정하기** 버튼을 클릭하세요.



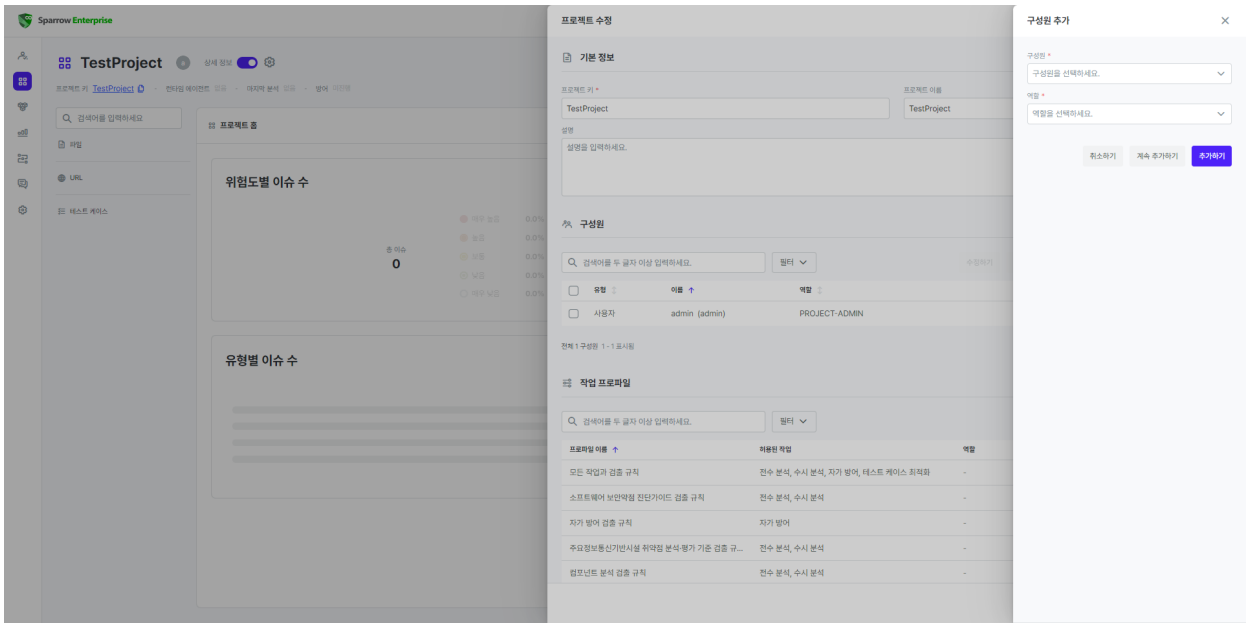
3. 슬라이드에서 프로젝트 키나 프로젝트 이름을 수정하세요.

4. 아래에 있는 **수정하기** 버튼을 클릭하세요.

프로젝트 구성원 추가하기

1. **프로젝트 수정** 슬라이드로 이동하세요.

2. **구성원**에 있는 **추가하기** 버튼을 클릭하세요.



3. 아래를 참고하여 구성원 정보를 입력하세요.

4. **추가하기** 버튼을 클릭하세요.

5. **프로젝트 수정** 슬라이드에서 **수정하기** 버튼을 클릭하세요.

구성원*

프로젝트에 구성원으로 추가할 사용자 또는 사용자 그룹입니다.

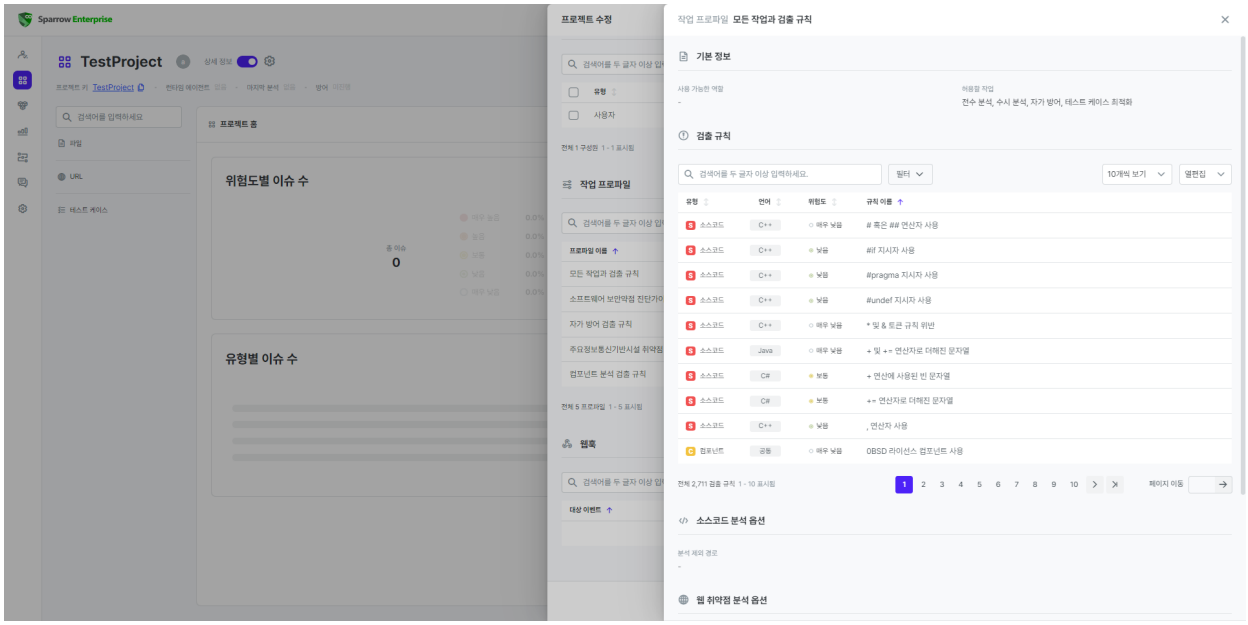
역할*

프로젝트 구성원으로 추가할 사용자 또는 사용자 그룹의 역할입니다. 프로젝트 역할을 추가하는 방법은 프로젝트 역할를 참고하세요.

프로젝트 작업 프로파일 설정하기

1. **프로젝트 수정** 슬라이드로 이동하세요.

2. **작업 프로파일** 목록에는 사용 가능한 모든 작업 프로파일이 있습니다.



3. **선택** 토글 버튼을 활성화하거나 비활성화하세요.

4. 이제 작업을 시작하세요.

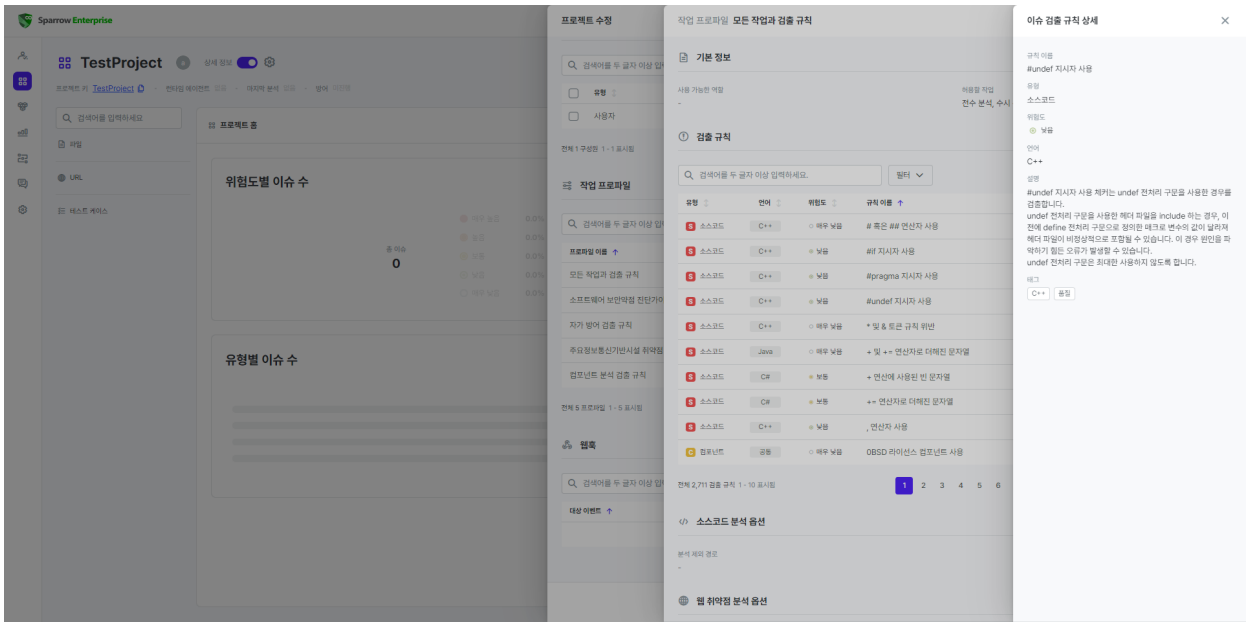
작업 프로파일*

작업 프로파일은 이슈 검출 규칙과 작업 옵션 등 작업에 필요한 정보를 모아둔 데이터입니다. 작업 프로파일을 추가하는 방법은 작업 프로파일 추가하기를 참고하세요.

이슈 검출 규칙 확인하기

프로젝트 수정 페이지의 **작업 프로파일**에서는 분석 작업에서 이슈를 검출하는 이슈 검출 규칙의 상세 정보를 확인할 수도 있습니다. 다음을 참고하세요.

1. **프로젝트 수정** 슬라이드로 이동하세요.
2. **작업 프로파일** 목록에서 분석 작업에 사용한 항목을 클릭하세요.
3. **검출 규칙** 목록에서 확인하려는 **이슈 검출 규칙**을 클릭하세요.



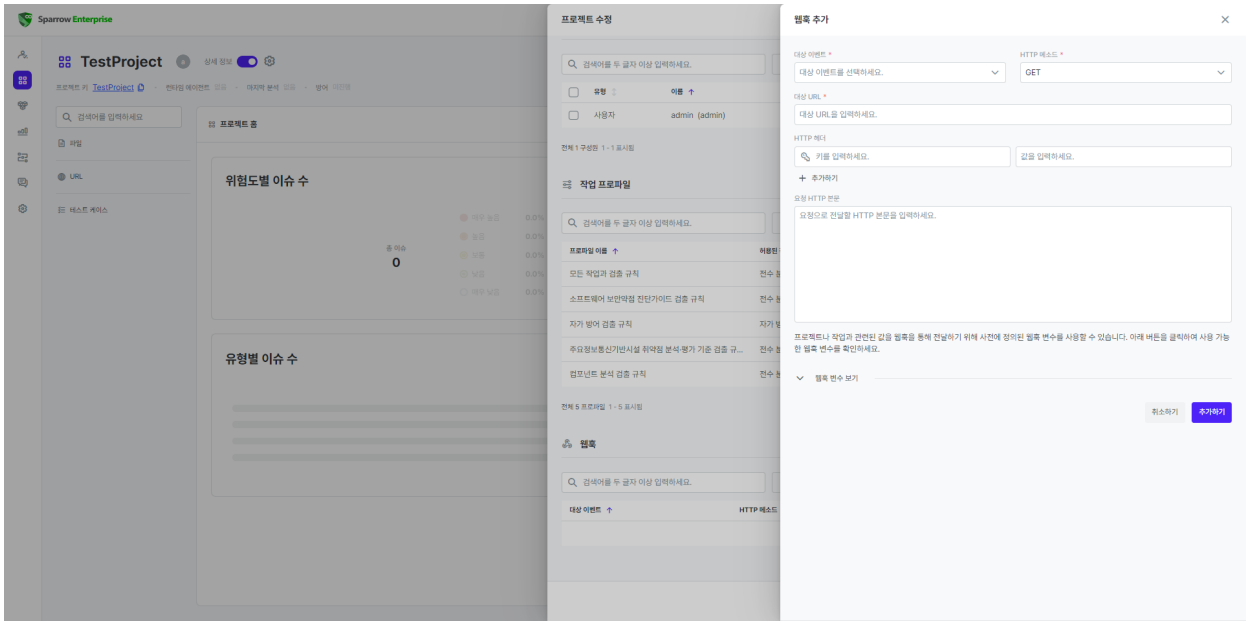
4. 이슈 검출 규칙의 정보를 확인하세요.

> **Tip**: 이슈 검출 규칙을 수정하거나 추가하려면 이슈 검출 규칙 관리하기를 참고하세요.

프로젝트 웹훅 설정하기

프로젝트 수정 슬라이드에서는 프로젝트의 특정 이벤트에 **웹훅**을 설정하는 것도 가능합니다. 다음 내용을 참고하세요.

1. **프로젝트 수정** 슬라이드로 이동하세요.
2. **웹훅**에 있는 **추가하기** 버튼을 클릭하세요.



3. 아래를 참고하여 웹훅 정보를 입력하세요.

4. **추가하기** 버튼을 클릭하세요.

5. **프로젝트 수정** 슬라이드에서 **수정하기** 버튼을 클릭하세요.

대상 이벤트*

웹훅을 실행할 프로젝트의 이벤트입니다. **작업 시작**, **작업 실패**, **작업 완료** 중에서 하나 이상을 선택할 수 있습니다.

HTTP 메소드*

실행할 웹훅 요청에서 사용할 HTTP 메소드입니다. `GET`, `HEAD`, `POST`, `PUT`, `DELETE`, `OPTIONS`, `TRACE`, `PATCH` 중에 하나를 선택할 수 있습니다.(기본값: `GET`)

대상 URL*

웹훅을 실행할 대상 URL입니다. 이 옵션은 `http://` 혹은 `https://`로 시작하는 URL 형식으로 입력해야 합니다.

HTTP 헤더

웹훅을 실행할 때 대상 URL로 보내는 HTTP 요청에 추가할 헤더의 키와 값 목록입니다. 키와 값의 쌍으로 되어있으며 목록의 아래에 있는 **+ 추가하기** 버튼을 클릭하여 하나 이상의 키값을 입력할 수 있습니다.

요청 HTTP 본문

웹훅을 실행할 때 대상 URL에 대한 요청으로 전송할 HTTP 본문입니다. 값이 존재하지 않는 경우 별도의 본문을 전달하지 않습니다. **웹훅 변수 보기**에 있는 변수를 이 옵션에 입력할 수 있습니다.

웹훅 변수 보기

웹훅을 실행할 때 요청 HTTP 본문에 사용할 수 있는 변수의 목록입니다. **프로젝트 키**, **작업 ID**, **작업 유형**, **작업 시작 일시**, **작업 완료 일시**, **작업 수행자 ID**, **작업 수행자 이름**, **총 이슈 수**, **위험도별 이슈 수**와 같은 정

보를 사용할 수 있습니다.

작업 이력 확인하기

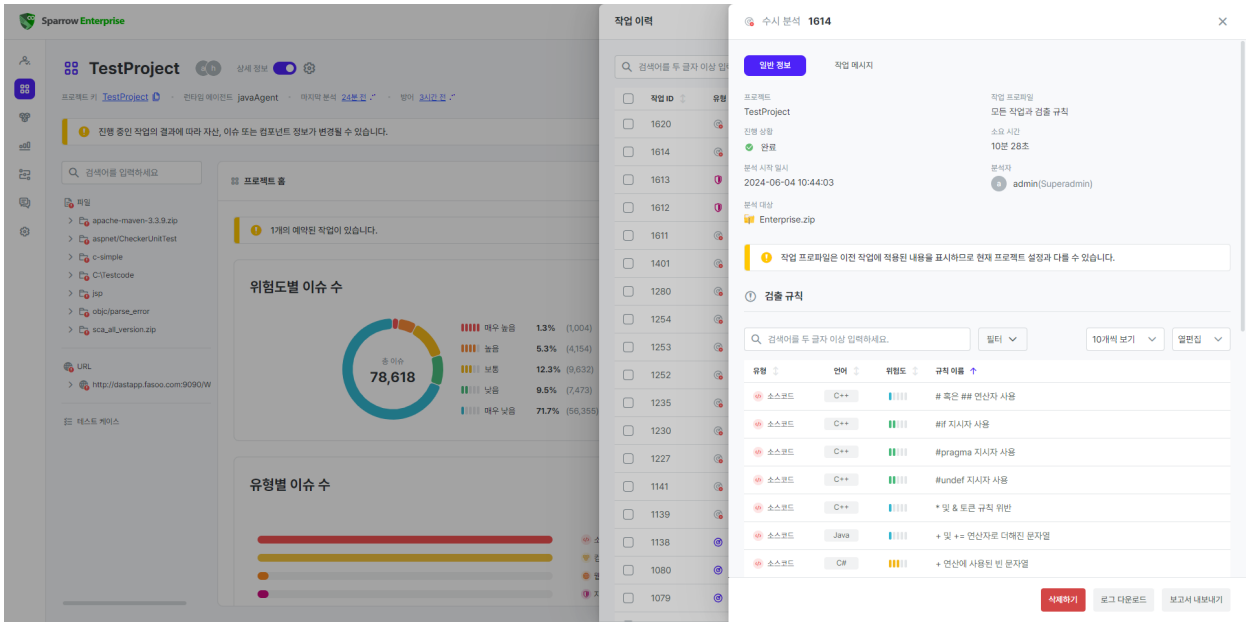
사용자가 가진 제품 라이선스에 따라 Sparrow Enterprise에서 수행한 동작 중 **분석**, **자가 방어**, **테스트 케이스 최적화**를 작업이라고 부릅니다. **작업 이력**에서는 프로젝트에서 수행한 모든 작업의 목록에 표시됩니다. 여기서 작업에 대한 주요 정보를 확인하실 수 있습니다.

작업 이력에서는 분석 로그를 다운로드 받거나 완료된 분석의 분석 보고서를 다운로드 받을 수도 있습니다. 자세한 내용은 분석 로그 다운로드 및 분석 보고서를 참고하세요.

분석을 중지하거나 삭제하는 것도 **작업 이력** 페이지에서 하실 수 있습니다. 만약 분석을 중지하면 다시 해당 분석을 시작할 수 없습니다. 또한 분석을 삭제하는 경우에도 분석 결과를 복구할 수 없다는 점에 유의하세요. 자세한 내용은 분석 중지하기 및 분석 삭제하기를 참고하세요.

분석 로그 다운로드

1. **작업 이력**에서 로그를 다운로드하려는 분석을 선택하세요.
2. 분석 슬라이드로 이동합니다.



3. 아래쪽에 있는 **로그 다운로드** 버튼을 클릭하세요.

> **Tip**: 자가 방어 및 최적화의 경우 분석 로그를 다운로드할 수 없습니다.

분석 삭제하기

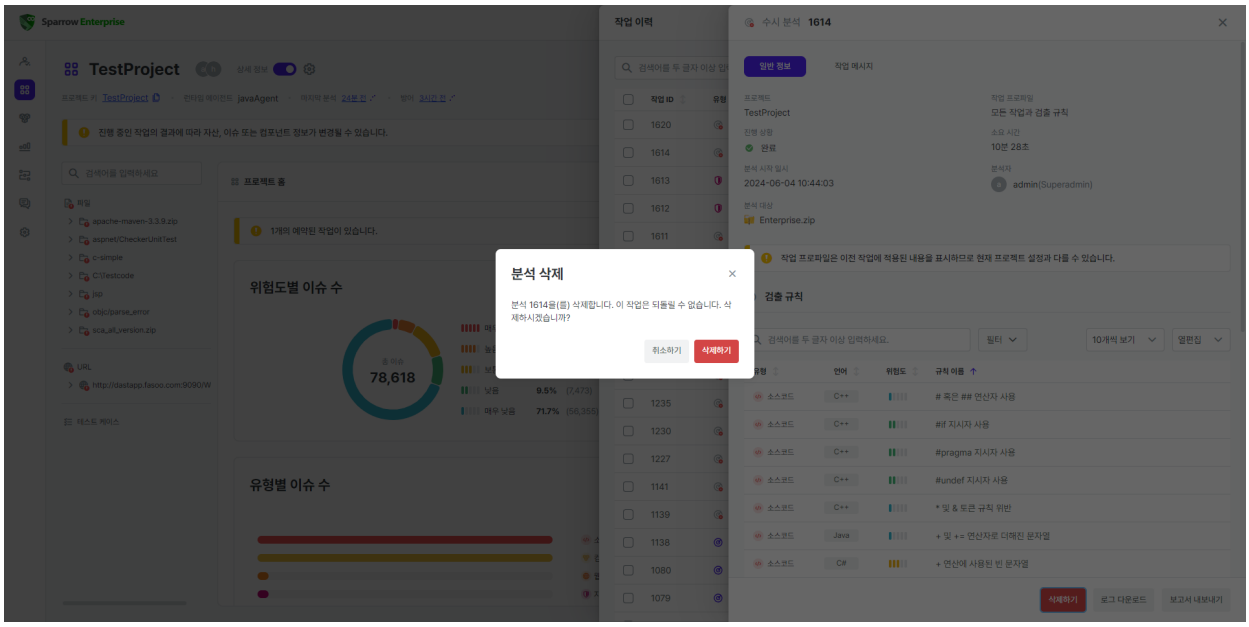
분석 작업의 경우, 가장 최근의 분석에서 검출한 이슈를 비롯한 분석 결과는 프로젝트의 탭에서 자세하게 확인할 수 있습니다. 하지만 이전에 수행한 분석 결과 중 이슈나 자산, 컴포넌트와 같은 상세 결과의 내용은 표시되지 않습니다.

따라서 만약 이전 작업과 관련된 결과를 자세히 확인하려면 해당 작업의 이후에 수행한 동일한 유형의 작업을 모두 삭제해야 합니다. 단, 방어의 경우 이미 수행된 작업을 삭제하는 것이 불가능합니다.

> **Warning**: 삭제된 데이터는 복구할 수 없다는 점에 유의하세요.

수행이 종료된 분석을 삭제하려면 1) 프로젝트의 **프로젝트 구성원**으로써 프로젝트 권한 중 2) **작업 관리** 권한을 포함한 프로젝트 역할을 가져야 합니다. 자세한 내용은 다음을 참고하세요.

1. 프로젝트 상세 정보 페이지로 이동하세요.
2. 오른쪽 위에 있는 **작업 이력 보기** 버튼을 클릭하세요.
3. 삭제할 분석의 체크박스를 선택하고 목록 오른쪽 위에 있는 **삭제하기** 버튼을 클릭하세요.
4. 혹은 삭제하려는 분석의 상세 정보 슬라이드에서 아래에 있는 **삭제하기** 버튼을 클릭하세요.

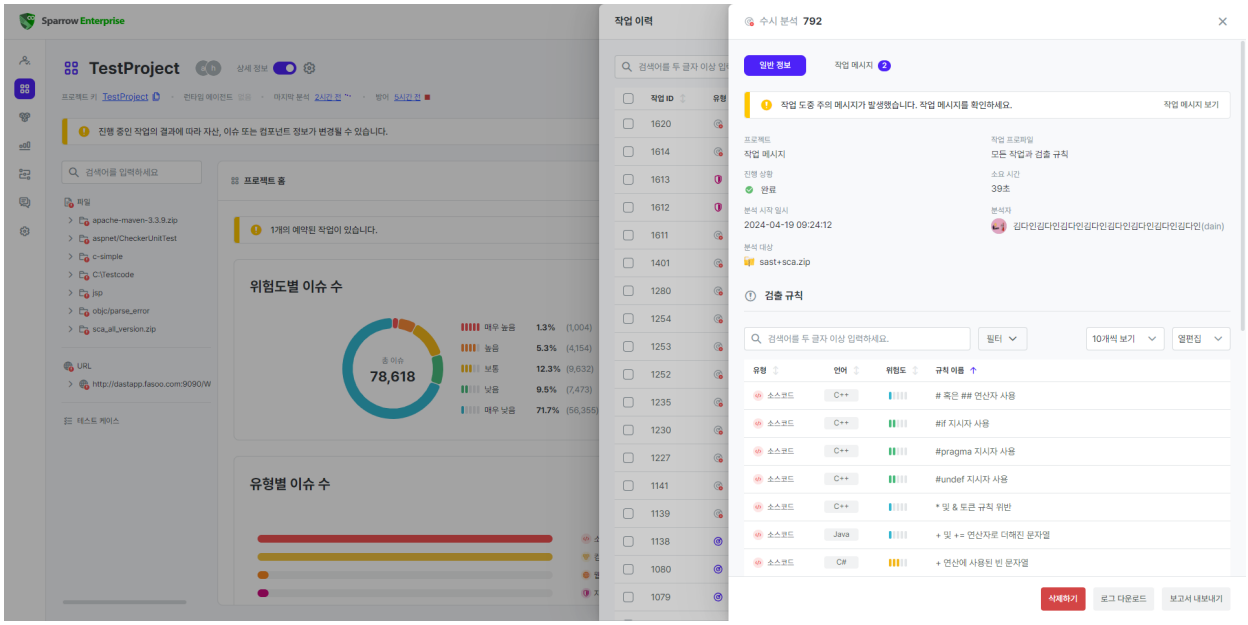


> **Tip**: 자가 방어 및 최적화의 경우 작업을 삭제할 수 없습니다.

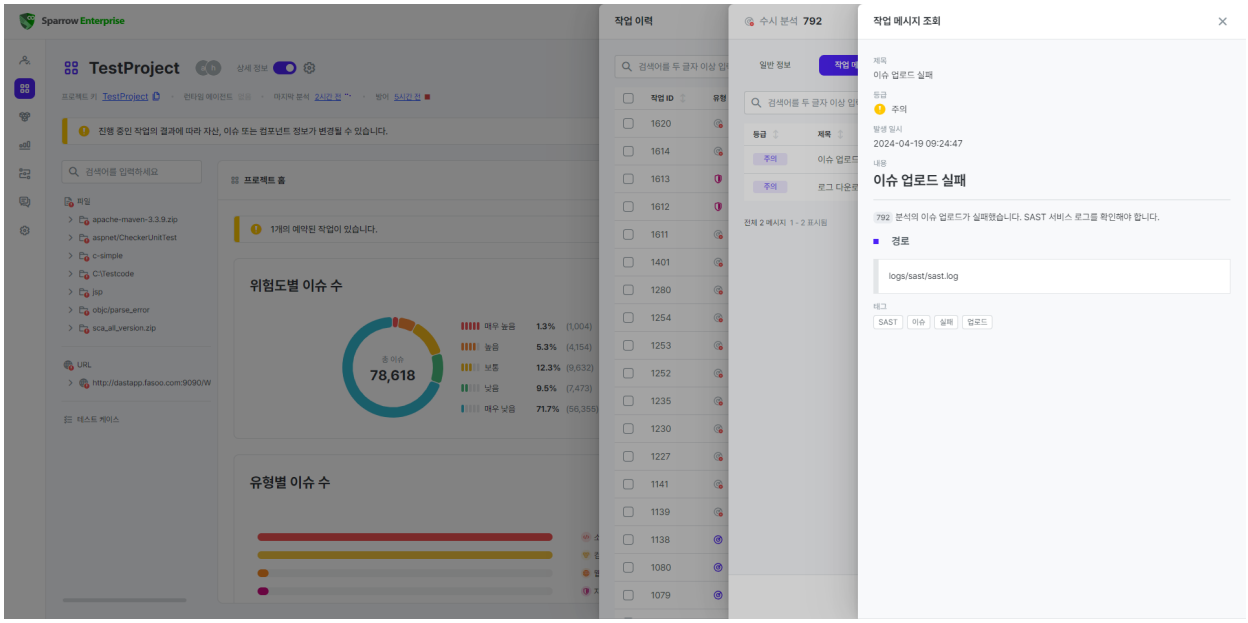
작업 메시지 확인하기

작업을 진행하는 과정에서 사용자가 알아야 할 중요한 문제가 발생하는 경우 작업 이력에 알림이 표시됩니다. 이 알림에서 **작업 메시지 보기**를 클릭하면 해당 메시지 목록으로 이동할 수 있습니다.

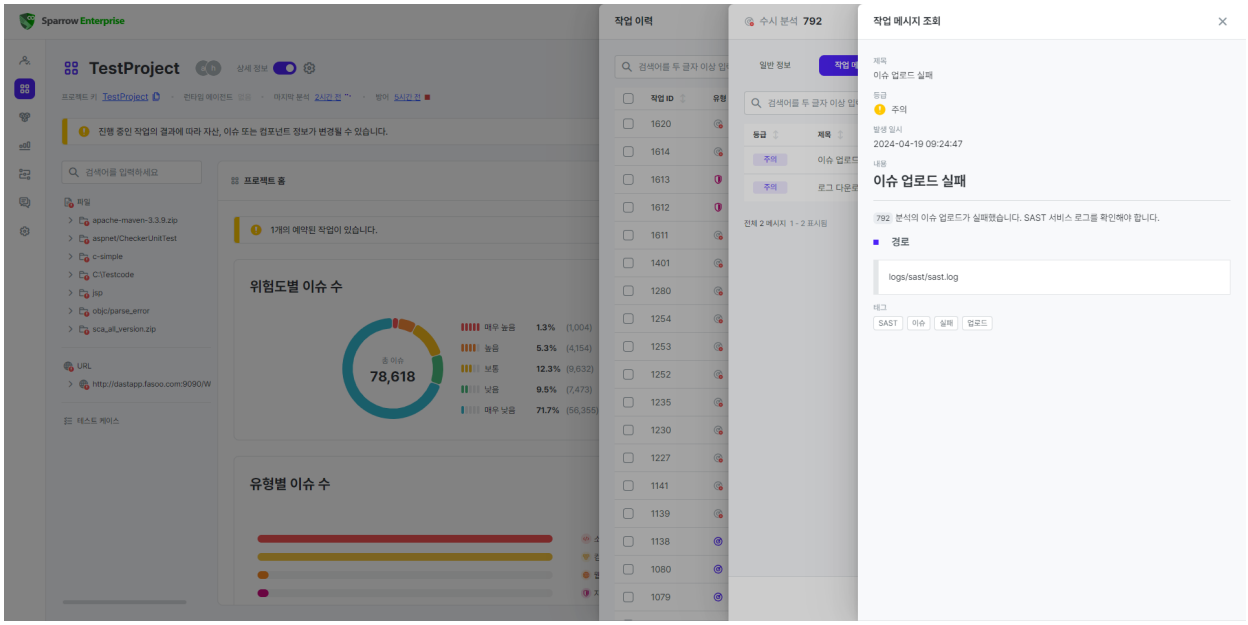
1. **작업 이력**에서 작업 메시지를 확인하려는 분석을 선택하세요.
2. 분석 슬라이드로 이동합니다.



3. 알림에서 **작업 메시지 보기**를 클릭하거나 **작업 메시지** 탭을 클릭하세요.



4. 목록에서 확인할 항목을 클릭하세요.



제목

표시된 작업 메시지의 제목입니다.

등급

표시된 작업 메시지는 **주의** 혹은 **경고**라는 등급으로 분류됩니다. **주의**는 작업에 포함된 일부 분석 결과에 이상이 있을 수 있는 경우이고 **경고**는 작업이 정상적으로 진행되지 않고 전체 분석 결과를 확인할 수 없는 경우를 의미합니다.

발생 일시

표시된 작업 메시지가 발생한 일시입니다.

내용

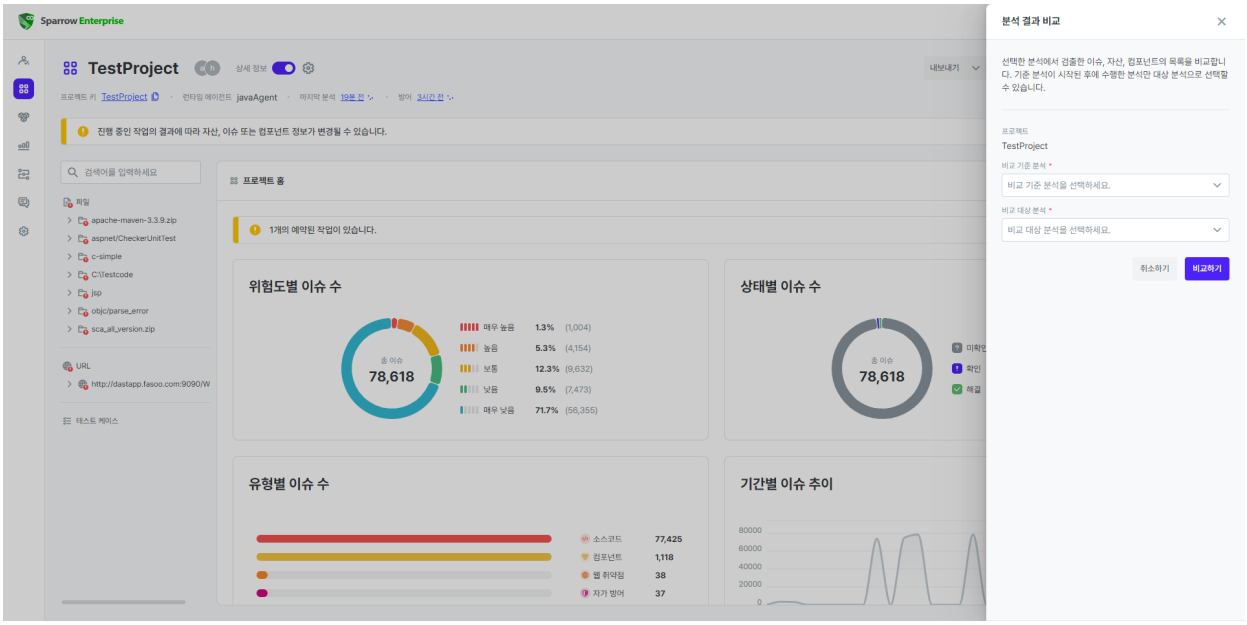
표시된 작업 메시지의 내용입니다. 여기에는 작업 메시지에 대한 설명이나 더 자세한 로그를 확인할 수 있는 위치 등 구체적인 정보가 포함됩니다.

태그

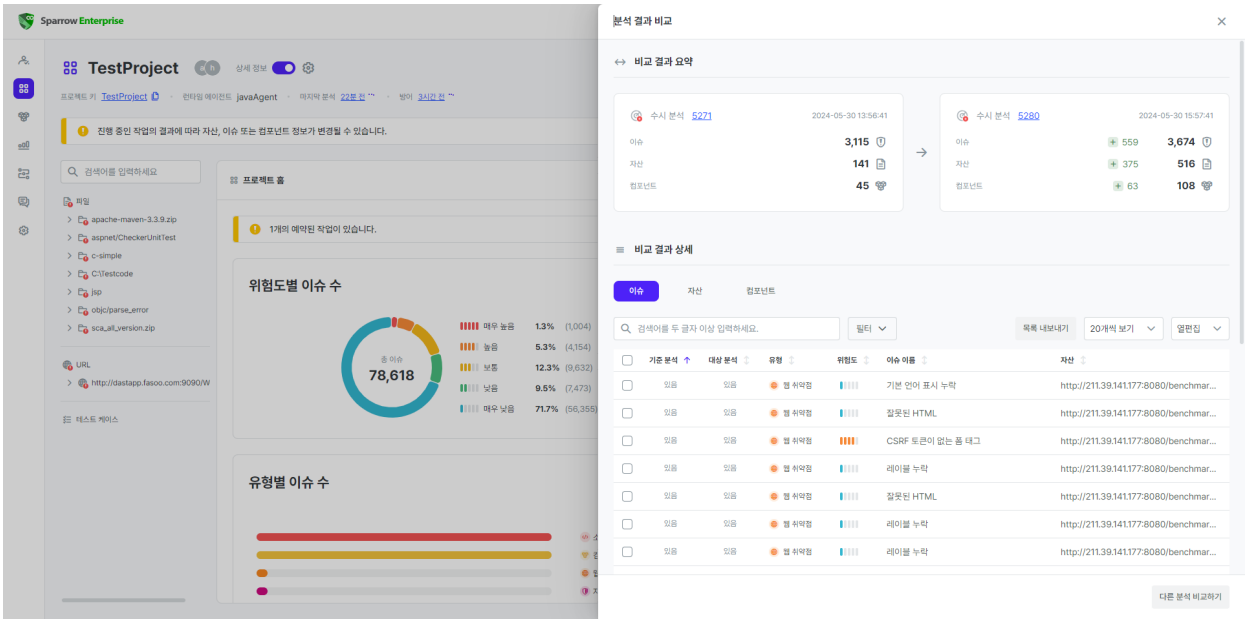
표시된 작업 메시지와 관련된 태그입니다.

분석 결과 비교하기

1. 비교할 분석의 프로젝트 상세 정보 페이지로 이동하세요.
2. 오른쪽 위에 있는 **분석 결과 비교하기** 버튼을 클릭하세요.
3. 아래 내용을 참고하여 분석 결과 비교 슬라이드에서 **비교 기준 분석** 및 **비교 대상 분석**을 선택하세요. (*는 필수 입력 항목)



4. **비교하기** 버튼을 클릭하세요.



비교 기준 분석*

분석 결과를 비교할 기준으로써 해당 프로젝트의 분석 중 **진행 중**, **중지**, **완료**된 분석을 선택할 수 있습니다.

비교 대상 분석*

분석 결과를 비교할 대상으로써 해당 프로젝트의 분석 중 **비교 기준 분석** 이후에 수행한 **진행 중**, **중지**, **완료**된 분석을 선택할 수 있습니다.

> **Warning**: **진행 중**인 분석을 선택하는 경우 진행 정도에 따라 비교 결과가 다를 수 있다는 점에 유의하세요.

클라이언트 CLI로 프로젝트 확인

클라이언트 CLI: 프로젝트 목록 확인하기

Sparrow Enterprise 클라이언트 CLI에서 프로젝트 목록을 확인하는 방법은 다음과 같습니다.

1. 명령 프롬프트를 실행하세요.
2. **{Sparrow Enterprise 클라이언트 설치 디렉토리}**로 이동하세요.
3. Linux 환경에서는 **sparrow-cli** 파일과 `list project` 명령어 및 **옵션**을 입력하세요.

```
./sparrow-cli list project -s https://localhost:10880 -u admin -p
/home/user/workspace/password.txt
```

4. Windows 환경에서는 **sparrow-cli.cmd** 파일과 `list project` 명령어 및 **옵션**을 입력하세요.

```
sparrow-cli.cmd list project -s https://localhost:10880 -u admin -p
C:\workspace\password.txt
```

5. 아래 내용을 참고하여 **옵션**을 입력하고 실행하세요.(*는 필수 입력 항목)

-s 또는 --server*

연결하려는 Sparrow Enterprise 서버의 IP 주소 및 포트 번호입니다.(예시: `-s {Sparrow Enterprise 서버 IP 주소}:{포트 번호}`)

-u 또는 -–user*

프로젝트 목록을 확인하려는 사용자 계정의 ID입니다.(예시: `-u {사용자 ID}`)

-p 또는 -–password

분석을 수행하려는 사용자 계정의 비밀번호를 저장한 txt 파일의 위치입니다. 이 옵션에 값을 입력하지 않은 경우 사용자 계정의 비밀번호를 입력하라는 메시지가 추가로 표시되며 해당 메시지에 비밀번호를 입력하면 됩니다.(예시: `-p {txt 파일 경로}`)

그러면 프로젝트 이름, 프로젝트 키, 마지막 작업, 마지막 작업의 작업 시작 일시, 프로젝트 생성 일시가 표시됩니다.

클라이언트 CLI: 프로젝트 상세 정보 확인하기

Sparrow Enterprise 클라이언트 CLI에서 프로젝트 상세 정보를 확인하는 방법은 다음과 같습니다.

1. 명령 프롬프트를 실행하세요.

2. **{Sparrow Enterprise 클라이언트 설치 디렉토리}**로 이동하세요.

3. Linux 환경에서는 **sparrow-cli** 파일과 `get project` 명령어 및 **옵션**을 입력하세요.

```
./sparrow-cli get project -s https://localhost:10880 -u admin -p
/home/user/workspace/password.txt -k myapp
```

4. Windows 환경에서는 **sparrow-cli.cmd** 파일과 `get project` 명령어 및 **옵션**을 입력하세요.

```
sparrow-cli.cmd get project -s https://localhost:10880 -u admin -p
C:\workspace\password.txt -k myapp
```

5. 아래 내용을 참고하여 **옵션**을 입력하고 실행하세요.(*는 필수 입력 항목)

-s 또는 --server*

연결하려는 Sparrow Enterprise 서버의 IP 주소 및 포트 번호입니다.(예시: `-s {Sparrow Enterprise 서버 IP 주소}:{포트 번호}`)

-u 또는 -–user*

프로젝트 상세 정보를 확인하려는 사용자 계정의 ID입니다.(예시: `-u {사용자 ID}`)

-p 또는 -–password

분석을 수행하려는 사용자 계정의 비밀번호를 저장한 txt 파일의 위치입니다. 이 옵션에 값을 입력하지 않은 경우 사용자 계정의 비밀번호를 입력하라는 메시지가 추가로 표시되며 해당 메시지에 비밀번호를 입력하면 됩니다.(예시: `-p {txt 파일 경로}`)

-k 또는 --key*

확인할 프로젝트의 프로젝트 키입니다.(예시: `-k {프로젝트 키}`)

그러면 프로젝트 키, 프로젝트 이름, 생성 시간, 마지막 작업, 마지막 작업의 작업 ID, 작업 유형, 작업 시작 일시, 작업 완료 일시, 작업 상태, 총 이슈 수, 분석을 수행한 사용자 ID, 사용자 이름이 표시됩니다.

클라이언트 CLI로 작업 확인

클라이언트 CLI: 작업 이력 확인하기

Sparrow Enterprise 클라이언트 CLI에서 최근 작업 이력을 확인하는 방법은 다음과 같습니다.

1. 명령 프롬프트를 실행하세요.

2. **{Sparrow Enterprise 클라이언트 설치 디렉토리}**로 이동하세요.

3. Linux 환경에서는 **sparrow-cli** 파일과 `list analysis` 명령어 및 **옵션**을 입력하세요.

```
./sparrow-cli list analysis -s https://localhost:10880 -u admin -p
/home/user/workspace/password.txt -k myapp
```

4. Windows 환경에서는 **sparrow-cli.cmd** 파일과 `list analysis` 명령어 및 **옵션**을 입력하세요.

```
sparrow-cli.cmd list analysis -s https://localhost:10880 -u admin -p
C:\workspace\password.txt -k myapp
```

5. 아래 내용을 참고하여 **옵션**을 입력하고 실행하세요.(*는 필수 입력 항목)

-s 또는 --server*

연결하려는 Sparrow Enterprise 서버의 IP 주소 및 포트 번호입니다.(예시: `-s {Sparrow Enterprise 서버 IP 주소}:{포트 번호}`)

-u 또는 -–user*

작업 이력을 확인하려는 사용자 계정의 ID입니다.(예시: `-u {사용자 ID}`)

-p 또는 -–password

분석을 수행하려는 사용자 계정의 비밀번호를 저장한 txt 파일의 위치입니다. 이 옵션에 값을 입력하지 않은 경우 사용자 계정의 비밀번호를 입력하라는 메시지가 추가로 표시되며 해당 메시지에 비밀번호를 입력하면 됩니다.(예시: `-p {txt 파일 경로}`)

-k 또는 --key

분석 작업을 수행할 프로젝트의 프로젝트 키입니다. 이 옵션을 입력하면 해당 프로젝트에서 수행된 최근 작업을 표시합니다. 이 옵션에 값을 입력하지 않으면 모든 프로젝트에서 수행된 최근 작업을 표시합니다.(예시: `-k {프로젝트 키}`)

그러면 작업 ID, 프로젝트 키, 작업의 작업 유형, 작업 상태, 진행률, 작업에서 검출된 총 이슈 수, 작업 시작 일시, 작업 완료 일시가 표시됩니다.

클라이언트 CLI: 작업 상세 정보 확인하기

Sparrow Enterprise 클라이언트 CLI에서 작업 상세 정보를 확인하는 방법은 다음과 같습니다.

1. 명령 프롬프트를 실행하세요.

2. **{Sparrow Enterprise 클라이언트 설치 디렉토리}**로 이동하세요.

3. Linux 환경에서는 **sparrow-cli** 파일과 `get analysis` 명령어 및 **옵션**을 입력하세요.

```
./sparrow-cli get analysis -i 49 -s https://localhost:10880 -u admin -p
/home/user/workspace/password.txt
```

4. Windows 환경에서는 **sparrow-cli.cmd** 파일과 `get analysis` 명령어 및 **옵션**을 입력하세요.

```
sparrow-cli.cmd get analysis -i 49 -s https://localhost:10880 -u admin -p
C:\workspace\password.txt
```

5. 아래 내용을 참고하여 **옵션**을 입력하고 실행하세요.(*는 필수 입력 항목)

-i 또는 --id*

확인할 작업의 고유한 ID입니다.(예시: `-i {작업 ID}`)

-s 또는 --server*

연결하려는 Sparrow Enterprise 서버의 IP 주소 및 포트 번호입니다.(예시: `-s {Sparrow Enterprise 서버 IP 주소}:{포트 번호}`)

-u 또는 --user*

작업 상세 정보를 확인하려는 사용자 계정의 ID입니다.(예시: `-u {사용자 ID}`)

-p 또는 --password

분석을 수행하려는 사용자 계정의 비밀번호를 저장한 txt 파일의 위치입니다. 이 옵션에 값을 입력하지 않은 경우 사용자 계정의 비밀번호를 입력하라는 메시지가 추가로 표시되며 해당 메시지에 비밀번호를 입력하면 됩니다.(예시: `-p {txt 파일 경로}`)

그러면 프로젝트 키, 프로젝트 이름, 마지막 작업의 작업 ID, 작업 유형, 작업 시작 일시, 작업 완료 일시, 작업 상태, 총 이슈 수, 분석을 수행한 사용자 ID, 사용자 이름이 표시됩니다.

최근 이슈 확인하기

이슈 목록에는 Sparrow Enterprise에서 1) 마지막으로 시작한 전수 분석 및 해당 전수 분석의 수시 분석 2) 마지막으로 완료되거나 수행 중인 방어 작업에서 검출된 이슈가 표시됩니다.

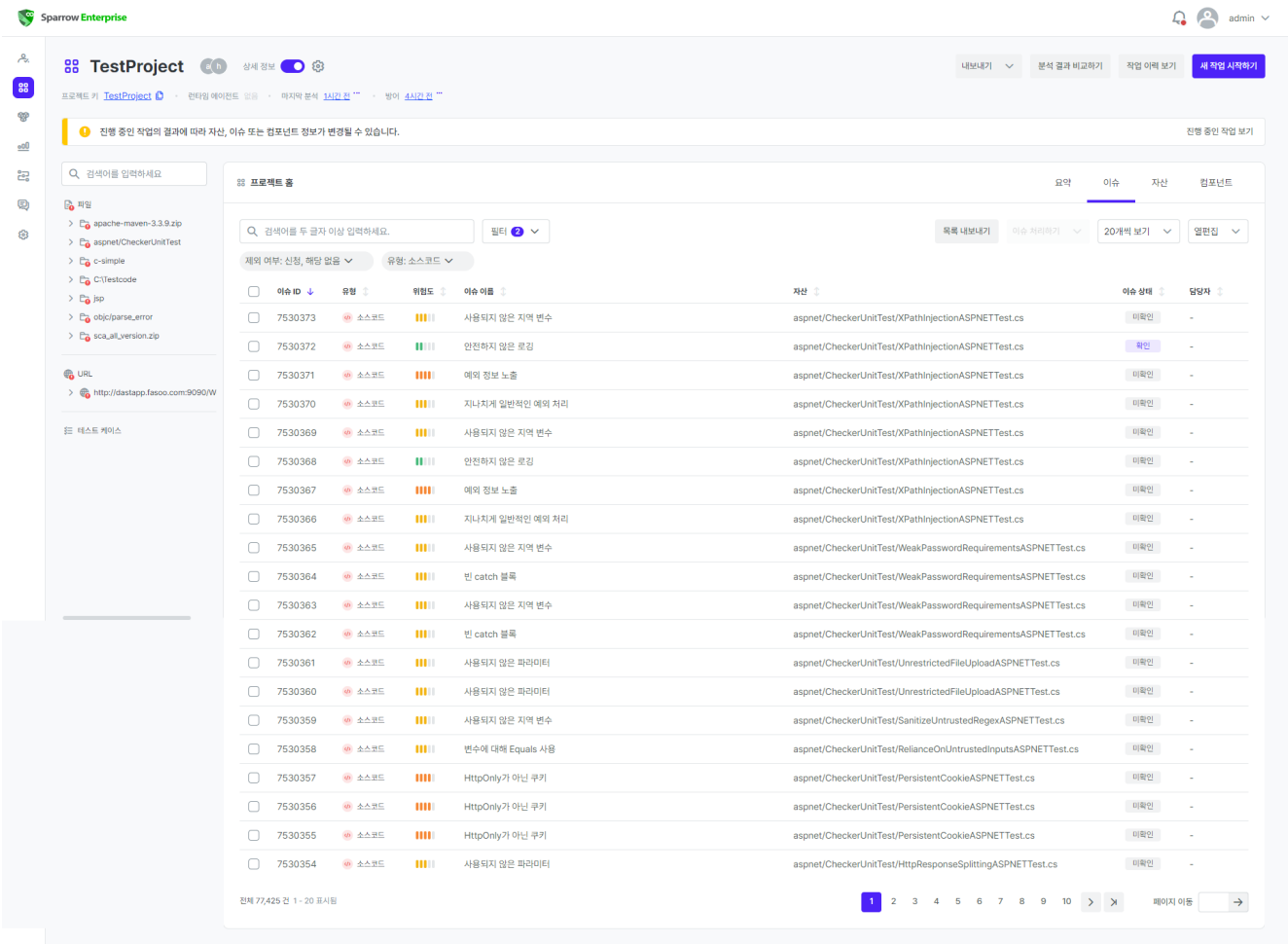
> **Tip**: 전수 분석의 이전에 수행된 분석의 상세 데이터를 확인하는 방법은 작업 이력 확인하기를 참고하세요.

따라서 이슈 목록을 확인할 때 주의해야 할 점이 있습니다. 먼저, 이슈 목록에는 하나 이상의 작업, 즉, 하나의 전수 분석과 다수의 수시 분석의 결과가 포함될 수 있습니다. 앞서 분석에서 설명한 것처럼 **수시 분석**이 이전에 수행한 **전수 분석**의 결과를 업데이트하기 때문입니다.

또한, 여러 분석에서 동일한 이슈 검출 규칙으로 특정 자산을 분석한 경우 검출되는 이슈의 구분자가 동일한 상황이 발생할 수 있습니다. 이 경우에 이전 분석에서 발견한 이슈가 새로 시작한 분석에서도 발견된다면 하나의 이슈로 표시합니다. 하지만 이전 분석의 이슈가 새로운 분석에서 발견되지 않는다면 해당 이슈가 사라졌다고 판단하고 이슈 목록에 표시하지 않습니다.

> **Tip**: 만약 프로젝트를 진행하는 도중 파일의 이름을 변경하거나 파일을 삭제했다면 전수 분석을 수행하는 것이 정확한 결과를 확인하는데 도움이 됩니다.

소스코드 이슈



Sparrow SAST/SAQT를 통해 소스코드를 검사하면 이슈 검출 규칙에 따라 잠재적인 취약점이나 품질 관련 문제를 찾아낼 수 있습니다. 이 이슈를 **소스코드 이슈**라고 하고 이슈 탭에서 확인할 수 있습니다. **최근 이슈**에서 **소스코드 이슈**에 표시되는 내용은 다음과 같습니다.

이슈 ID

이슈의 고유한 구분 ID입니다.

이슈 유형

이슈를 검출한 분석 방법을 검출한 도구별로 구분하여 **소스코드**, **컴포넌트**, **웹 취약점**, **자가 방어** 중에 하나로 표시합니다. 여기서는 소스코드 이슈이므로 **소스코드**로 표시됩니다.

위험도

소스코드에서 검출된 이슈의 위험도이며 **매우 높음**, **높음**, **보통**, **낮음**, **매우 낮음**이라는 5단계로 구분합니다.

이슈 이름

소스코드에서 검출된 이슈의 이름입니다. 이슈 이름은 이슈를 검출한 이슈 검출 규칙의 이름을 그대로 사용합니다. 따라서 같은 이슈 검출 규칙으로 찾아낸 이슈의 이름이 동일하게 표시됩니다.

자산

이슈가 검출된 분석 대상이며 **파일** 또는 **URL**의 형태로 표시됩니다. **파일** 자산을 표시할 때 **웹 분석**의 경우 분석 대상으로 선택한 zip 파일의 이름을 제외한 상대 경로로 표시되고, **클라이언트 GUI 및 CLI 분석**의 경우 해당 파일의 절대 경로로 표시됩니다.

이슈 상태

해당 이슈의 검토 상태를 **미확인**, **확인**, **해결** 중 하나로 표시됩니다.(기본값: 미확인)

담당자

해당 이슈를 검토할 담당자를 표시합니다. 담당자를 지정하기 전에는 아무 것도 표시되지 않습니다.

이슈 검출 일시

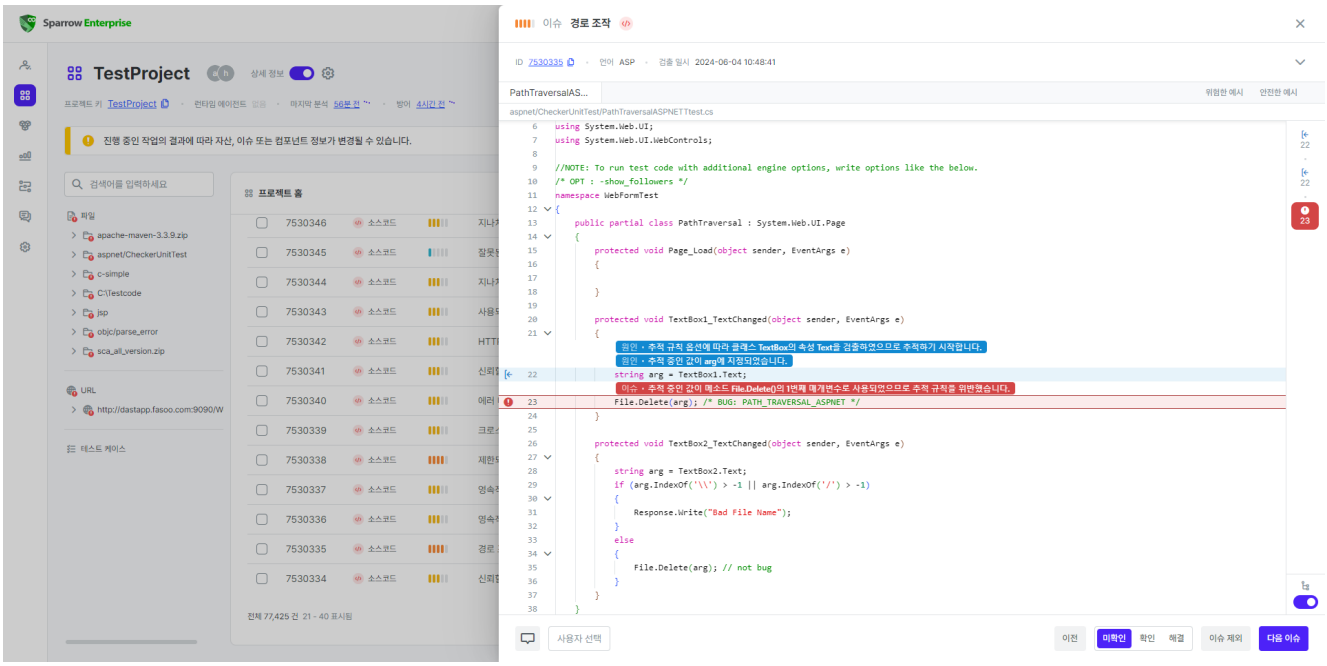
소스코드 분석에서 해당 이슈를 검출한 일시입니다.

제외 여부

해당 이슈가 이슈 목록에서 제외되었는지 표시합니다. 제외하도록 신청된 경우 **신청**으로 표시되고 신청이 승인된 경우 **제외**로 표시됩니다. 이슈를 제외하는 방법은 이슈 제외하기를 참고하세요.

소스코드 이슈 상세 정보

소스코드 이슈 목록에서 이슈를 클릭하면 해당 이슈의 **상세 정보** 페이지로 이동합니다. 여기에는 소스코드를 검출한 이슈 검출 규칙에 대한 정보, 이슈의 발생 원인을 찾아가는 내비게이터, 이슈가 검출된 파일의 소스코드가 표시됩니다. 자세한 내용은 아래를 참고해주세요.



✓ 이슈 검출 규칙

이슈 검출 규칙의 이름과 위험도, 언어 및 설명이 표시됩니다. 이슈 검출 규칙에 대한 더 자세한 설명은 **프로젝트 설정**의 **작업 프로파일**에서 확인할 수 있습니다. 자세한 내용은 이슈 검출 규칙 확인하기를 참고하세요.

✓ 소스코드 파일

이슈가 검출된 파일의 실제 소스코드가 표시됩니다. 하나의 파일당 하나의 탭으로 구성되어 이슈가 여러 파일에 걸쳐서 발생하는 경우 여러 개의 탭이 표시됩니다.

여기서는 소스코드 상에 이슈와 관련된 내용을 메시지로 확인할 수 있습니다. 또한 오른쪽에 있는 **내비게이터**와 연결되어 내비게이터에 표시된 특정 아이콘을 클릭하면 **소스코드**의 해당하는 라인으로 이동합니다. 내비게이터와 동일하게 **이슈**는 빨강색, **원인**은 파랑색, **분기**는 회색, **프레임워크**는 녹색으로 표시됩니다. 각 정보에 대한 자세한 내용은 아래를 참고하세요.

이슈

소스코드에서 이슈가 발생하는 결정적인 지점이며 **빨강색** 메시지가 표시됩니다. 내비게이터에서는 빨강색 경고 아이콘으로 표시됩니다.

원인

이슈가 발생하는 원인이며 **파랑색** 메시지가 표시됩니다. 내비게이터에서는 파랑색 삽입 아이콘으로 표시됩니다.

분기

이슈와 연관된 부분 실행 코드가 있는 부분이며 **회색** 메시지가 표시됩니다. 내비게이터에서는 회색 분기 아이콘으로 표시됩니다.

프레임워크

이슈의 원인에서 발생 지점으로 전개되는 과정이며 **녹색** 메시지가 표시됩니다. 내비게이터에서는 녹색 프레임워크 아이콘으로 표시됩니다.

✓ 예시 및 수정 방법

위험한 예시

위험한 예시 버튼을 클릭하면 이슈 검출 규칙에서 검출하는 소스코드 예시와 함께 해당하는 라인에 대한 설명을 표시합니다.

안전한 예시

안전한 예시 버튼을 클릭하면 **위험한 예시**를 수정한 소스코드 예시와 함께 해당하는 라인에 대한 설명을 표시합니다.

수정 방법

수정 방법 버튼이 있는 경우 해당 버튼을 클릭하면 이슈를 수정할 수 있는 방법과 함께 설명을 표시합니다.

✓ 내비게이터

소스코드 오른쪽에 있는 바에 이슈가 발생한 원인부터 이슈가 발생한 지점까지의 과정을 소스코드 라인 및 아이콘으로 표시합니다. 아이콘에 마우스를 이동하면 해당하는 메시지가 표시되고, 아이콘을 클릭하면 왼쪽에 있는 **소스코드**에서 해당하는 라인으로 이동하게 됩니다.

✓ 이슈 톡

발견된 이슈를 어떻게 처리했는지를 확인하기 위해 사용하며 **이슈 의견**, **이슈 담당자**, **이슈 상태**, **이슈 제외**가 표시됩니다.

이슈 담당자를 지정하거나 **이슈 상태**를 변경하려면 1) 프로젝트의 **프로젝트 구성원**으로써 프로젝트 권한 중 2) **이슈 참여** 권한을 포함한 프로젝트 역할을 가져야 합니다.

이슈 의견

해당 이슈에 대한 검토 의견을 입력하거나 입력된 의견을 표시합니다.

이슈 담당자

해당 이슈를 검토할 담당자를 표시합니다. 권한 있는 사용자 혹은 사용자 그룹 중에서 선택할 수 있으며 담당자를 지정하기 전에는 아무 것도 표시되지 않습니다.

이슈 상태

이슈가 검출되면 해당 이슈를 확인하고 해결하거나, 오탐 또는 다른 원인으로 인해 이슈에서 제외하도록 처리해야 합니다. 이슈를 어떻게 처리했는지 표시하기 위해서 이슈마다 **이슈 상태**를 다음과 같이 표시합니다.

- 미확인 : 담당자가 검출된 이슈를 아직 검토하지 않음
- 확인 : 담당자가 해당 이슈를 확인함

- 해결 : 담당자가 해당 이슈에서 발견된 문제를 해결함

이슈 제외

해당 이슈가 오탐이거나 다른 이유로 인해 이슈 목록에서 제외하려는 경우 이슈 제외 버튼을 클릭하여 이슈를 제외하도록 신청하거나 신청을 수락 또는 거절할 수 있습니다. 자세한 내용은 이슈 제외하기를 참고하세요.

> **Warning**: 이슈 목록에서는 제외된 이슈를 표시하지 않도록 기본값으로 필터링합니다. 이슈 목록에서 제외된 이슈를 확인하려면 해당 필터를 제거하세요.

이전 및 다음 이슈

이슈 목록에 표시된 **이전 이슈** 또는 **다음 이슈**로 이동합니다.

이슈 제외 | 결재

Sparrow Enterprise에서는 소스코드 이슈, 컴포넌트 이슈, 웹 취약점 이슈 및 자가 방어 이슈를 검출합니다. 하지만 이슈 중에는 잠재적으로 문제가 될 가능성이 있을 뿐 실제로 보안 취약점 혹은 품질 문제라고 볼 수 없는 경우가 있습니다. 이러한 경우 보안 진단원 혹은 동일한 자격의 전문가라고 할 수 있는 사용자가 특정 이슈를 문제에서 제외시킬 수 있도록 만든 기능이 **이슈 제외**입니다.

이 기능을 통해 제외된 이슈는 기본적으로 이슈 목록에 표시되지 않도록 설계되어 있습니다. 또한 프로젝트나 작업의 이슈 수에도 포함되지 않습니다. 작업 보고서를 출력할 때도 이슈 목록에는 포함되지 않고 제외된 이슈라는 별도 목록에만 표시됩니다.

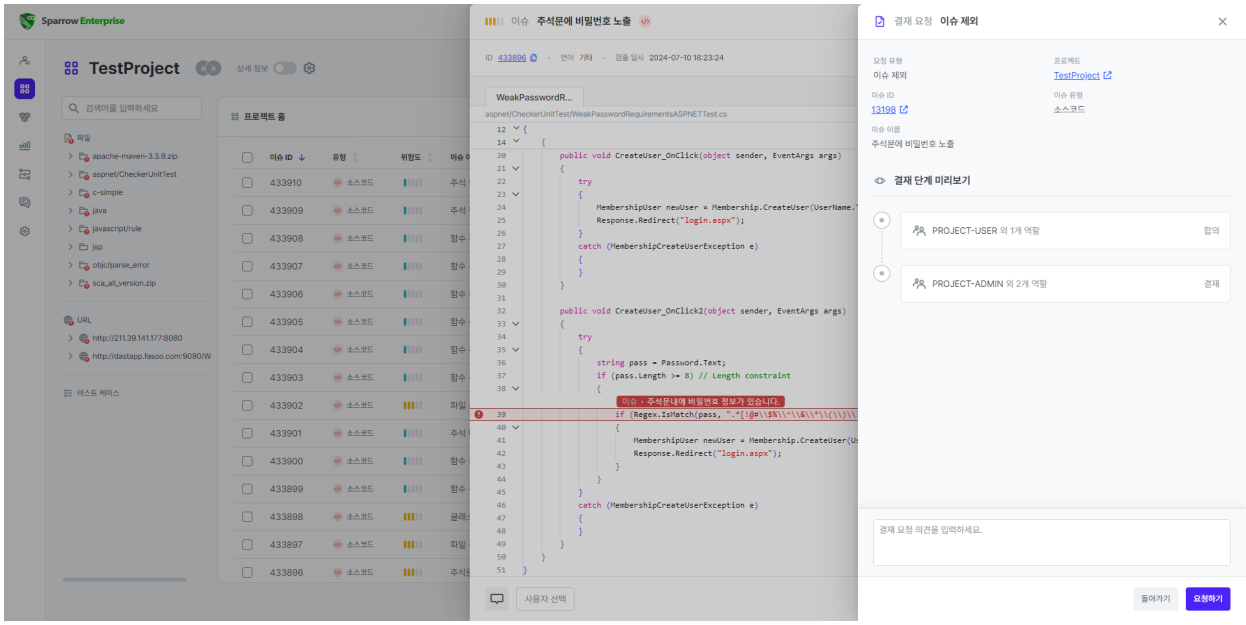
이슈 제외는 문제가 되지 않는 이슈를 발견했을 때 해당 **이슈를 제외하도록 결재를 요청한 후 요청된 결재를 처리**하는 방식으로 동작합니다. 만약 제외가 요청된 이슈에 여전히 문제의 소지가 있다고 판단하는 경우 **이슈 제외를 반려할 수도 있습니다**. 이렇게 결재를 요청하고 처리하려면 먼저 결재선을 설정해야 합니다. 결재선을 설정하지 않는 경우 사용자가 이슈 제외를 요청하는 즉시 이슈가 목록에서 제외됩니다. 자세한 내용은 결재선 관리하기를 참고하세요.

> **Warning**: 일단 이슈 제외 결재가 완료된 이슈는 **제외된 이슈**에서 제외되지 않은 이슈로 변경될 수 없다는 점에 유의하세요.

이슈 제외 요청하기

이슈 목록에서 이슈 제외를 요청하려는 사용자는, 해당 이슈가 포함된 1) 프로젝트의 **프로젝트 구성원**으로써 **결재선**에서 설정한 2) **요청 가능 역할** 옵션에 포함된 프로젝트 역할을 가져야 합니다.

1. 이슈 목록에서 이슈 제외를 요청할 이슈를 선택하세요.
2. 오른쪽 아래에 있는 **이슈 제외** 버튼을 클릭하세요.



3. **결재 단계**를 확인하고 이슈를 제외해야 하는 **요청 의견**을 작성하세요.

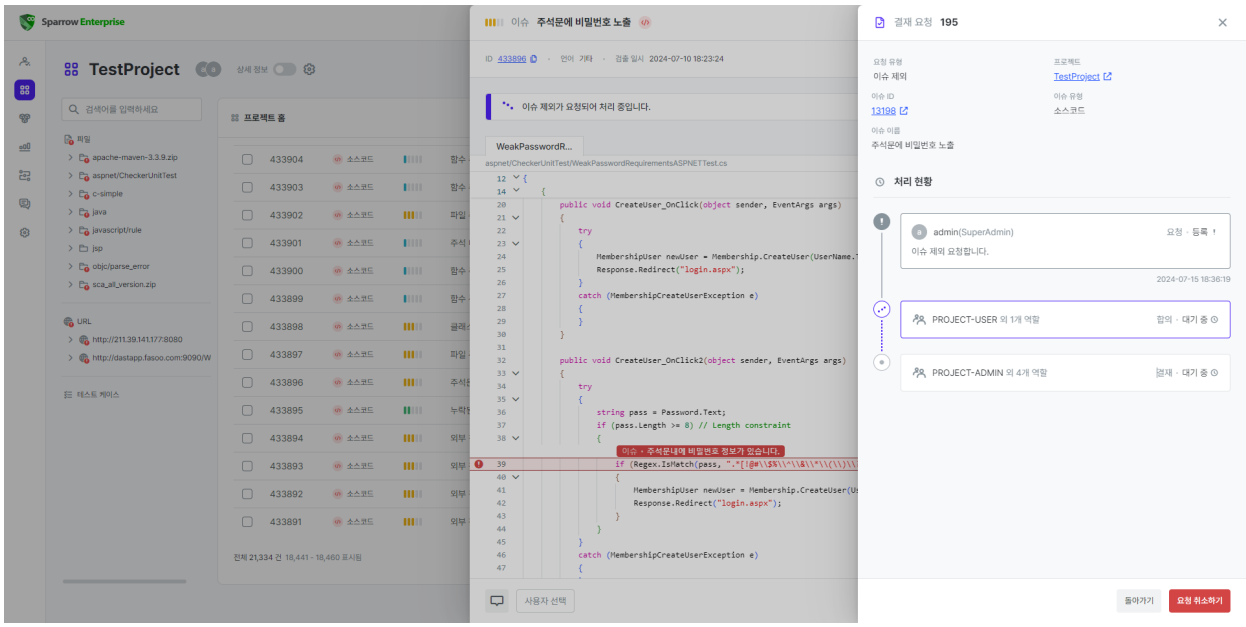
> **Tip**: 요청 의견을 입력하지 않아도 결재를 요청할 수 있습니다.

4. **요청하기** 버튼을 클릭하세요.

이슈 제외 요청 취소하기

이슈 제외 결재를 요청한 사용자는 이슈의 **처리 내역** 슬라이드에서 신청한 결재를 취소할 수도 있습니다.

1. 이슈 목록에서 이슈 제외 요청을 취소할 이슈를 선택하세요.
2. 오른쪽 아래에 있는 **처리 내역** 버튼을 클릭하세요.

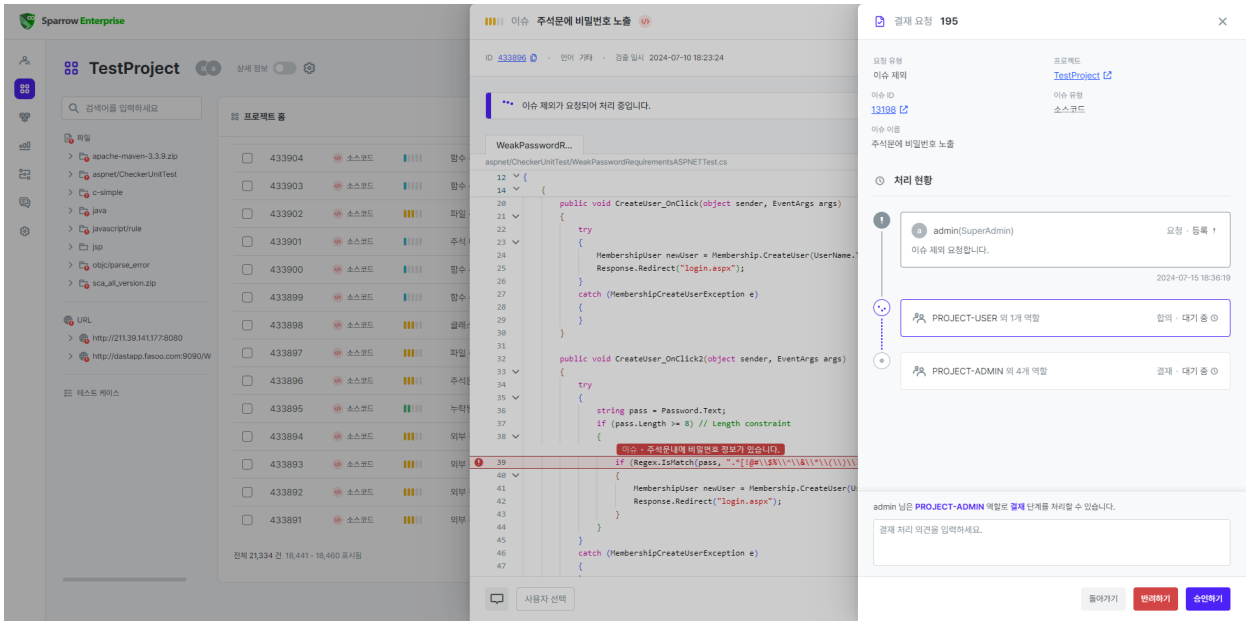


3. **요청 취소하기** 버튼을 클릭하세요.

이슈 제외 요청 처리하기

이슈 제외를 승인하거나 반려하려면 해당 이슈가 포함된 1) 프로젝트의 **프로젝트 구성원**으로써 **결재선**에서 설정한 2) **처리 가능 역할** 옵션에 포함된 프로젝트 역할을 가져야 합니다.

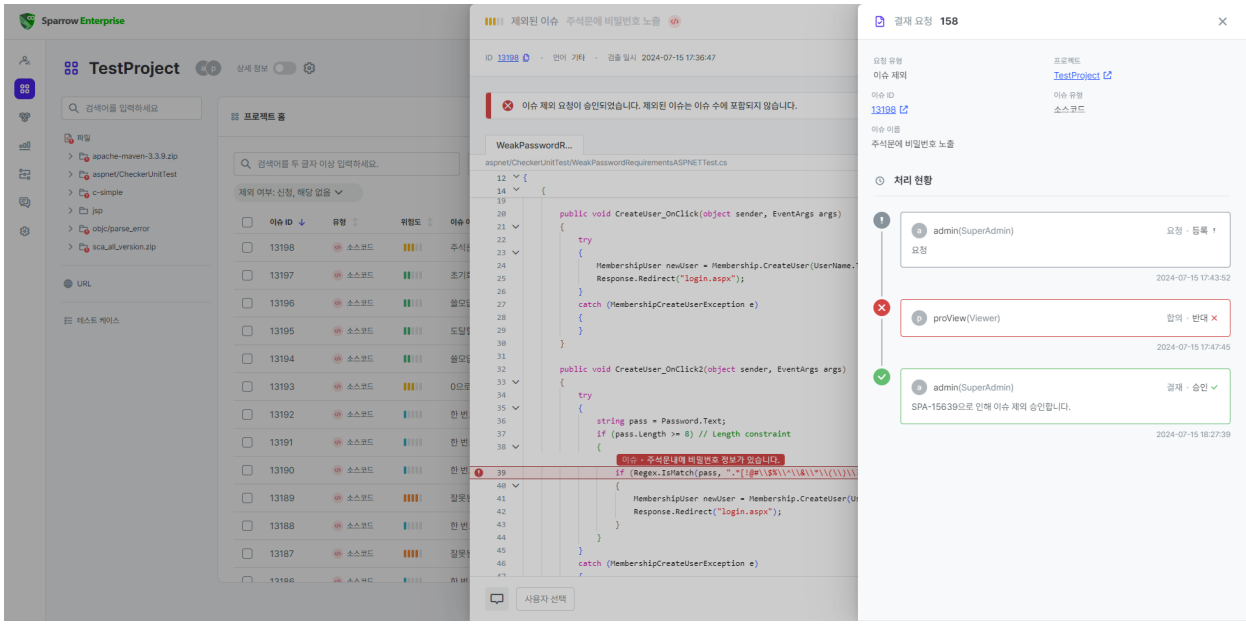
1. 이슈 목록에서 이미 이슈 제외가 신청된 이슈를 클릭하세요.
2. 오른쪽 아래에 있는 **처리 내역** 버튼을 클릭하세요.



3. **결재 단계**를 확인하고 이슈를 제외해야 하는 **처리 의견**을 작성하세요.

> **Tip**: 처리 의견을 입력하지 않아도 결재를 처리할 수 있습니다.

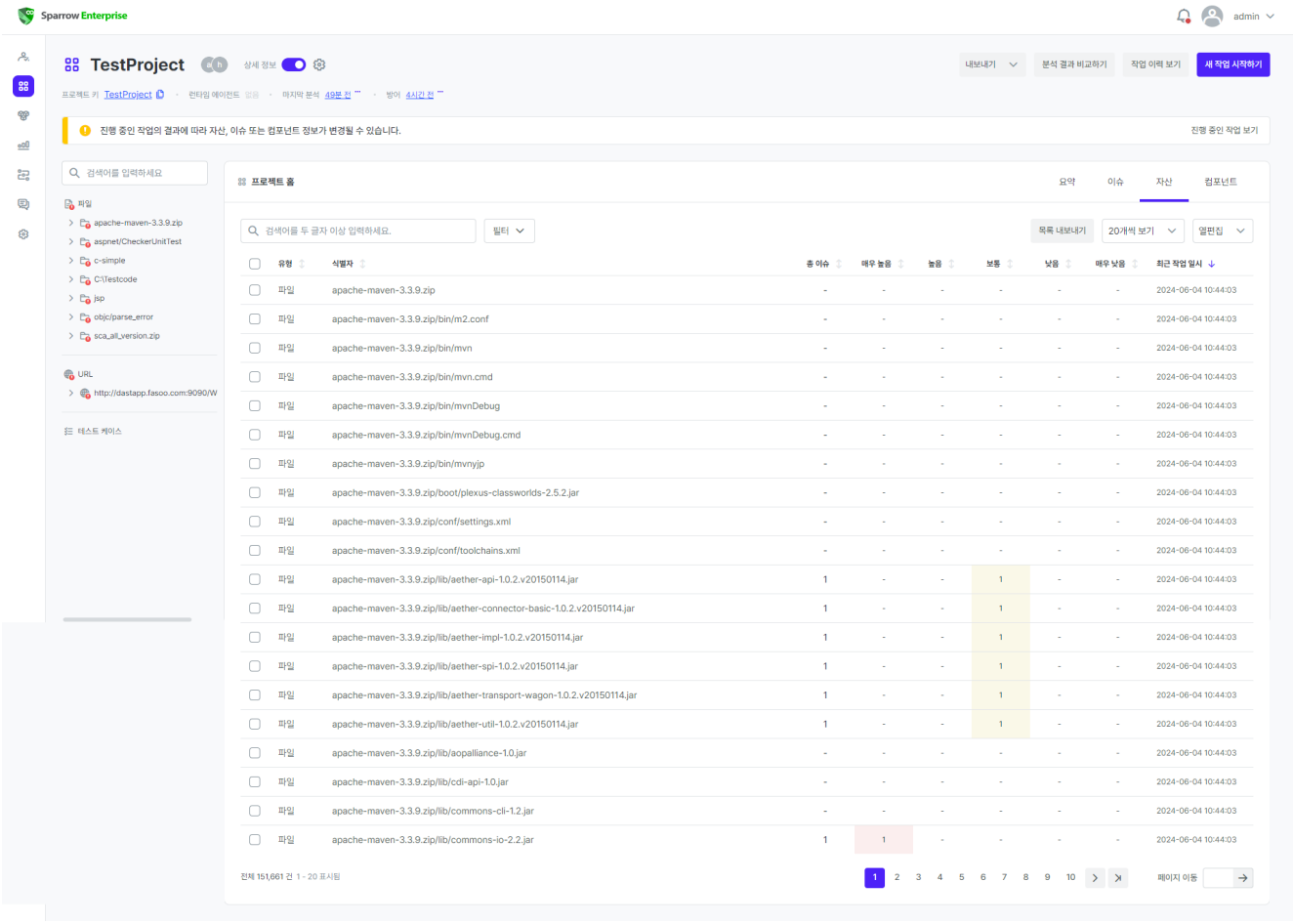
4. **결재** 단계인 경우 이슈 제외를 허락하려면 **승인하기** 버튼을 클릭하고 이슈 제외를 거절하려면 **반려하기** 버튼을 클릭하세요. **합의** 단계인 경우 이슈 제외에 찬성하려면 **동의하기** 버튼을 클릭하고 이슈 제외에 반대하려면 **반대하기** 버튼을 클릭하세요.



5. 결재 단계가 모두 완료되면 이슈가 제외됩니다.

> **Tip**: 단, **합의**의 경우 **반대하기**를 선택한 경우에도 다음 단계로 결재를 계속 진행합니다.

최근 자산 확인하기



자산 목록에는 Sparrow Enterprise에서 마지막으로 시작한 전수 분석 및 해당 전수 분석의 수시 분석에서 검출된 자산이 표시됩니다.

> **Tip**: 전수 분석의 이전에 수행된 분석의 상세 데이터를 확인하는 방법은 작업 이력 확인하기를 참고하세요.

자산 트리 혹은 자산 목록을 확인할 때 주의해야 할 점이 있습니다. 먼저, 자산 목록에는 하나 이상의 작업, 즉, 하나의 전수 분석과 다수의 수시 분석의 결과가 포함될 수 있습니다. 앞서 분석에서 설명한 것처럼 **수시 분석**이 이전에 수행한 **전수 분석**의 결과에 변경된 결과를 업데이트하기 때문입니다.

이전 분석에서 식별한 자산이 새로 시작한 분석의 동일한 경로에서도 발견된다면 하나의 자산으로 표시합니다. 하지만, **이슈**와 달리 한 번 발견한 자산은 목록에서 제거되지 않습니다.

> **Warning**: 단, 웹 분석의 경우에는 자산의 절대 경로를 파악할 수 없기 때문에 이전 분석과 동일한 경로에 있는 자산을 분석하더도 다른 자산으로 식별합니다.

자산을 식별하는 기준인 식별자는 파일인 경우 상대 혹은 절대 경로이고, 웹 사이트인 경우 리소스가 위치한 URL입니다. 따라서, 만약 프로젝트를 진행하는 도중 대상 파일의 이름을 변경하거나 파일을 삭제했다면 전수 분석을 수행하는 것이 정확한 결과를 확인하는데 도움이 됩니다.

유형

이슈가 검출된 분석 대상을 **파일** 또는 **URL** 중에 하나로 구분합니다. 소스코드 분석과 컴포넌트 분석에서는 자산이 파일로 표시되고, 웹 취약점 분석에서는 자산이 URL로 표시됩니다. 자가 방어의 경우 명확한 자산

이 표시되지 않습니다.

식별자

자산을 식별하는데 사용하는 고유한 문자열이며, 보통 자산의 경로 혹은 URL로 표시됩니다. 같은 프로젝트 안에서 식별자가 동일하다면 해당 자산은 동일한 자산입니다.

파일 자산을 표시할 때 **웹 분석**의 경우 자산이 분석 대상으로 선택한 zip 파일 이름을 제외한 상대 경로로 표시되고, **클라이언트 GUI 및 CLI 분석**의 경우 자산이 절대 경로로 표시됩니다.

총 이슈

검출된 자산에 포함된 전체 이슈의 개수입니다.

매우 높음/높음/보통/낮음/매우 낮음

자산에서 검출된 위험도별 이슈의 개수이며 위험도를 **매우 높음**, **높음**, **보통**, **낮음**, **매우 낮음**이라는 5단계로 구분합니다.

마지막 작업 일시

자산이 발견된 마지막 작업의 시작 일시를 표시합니다.

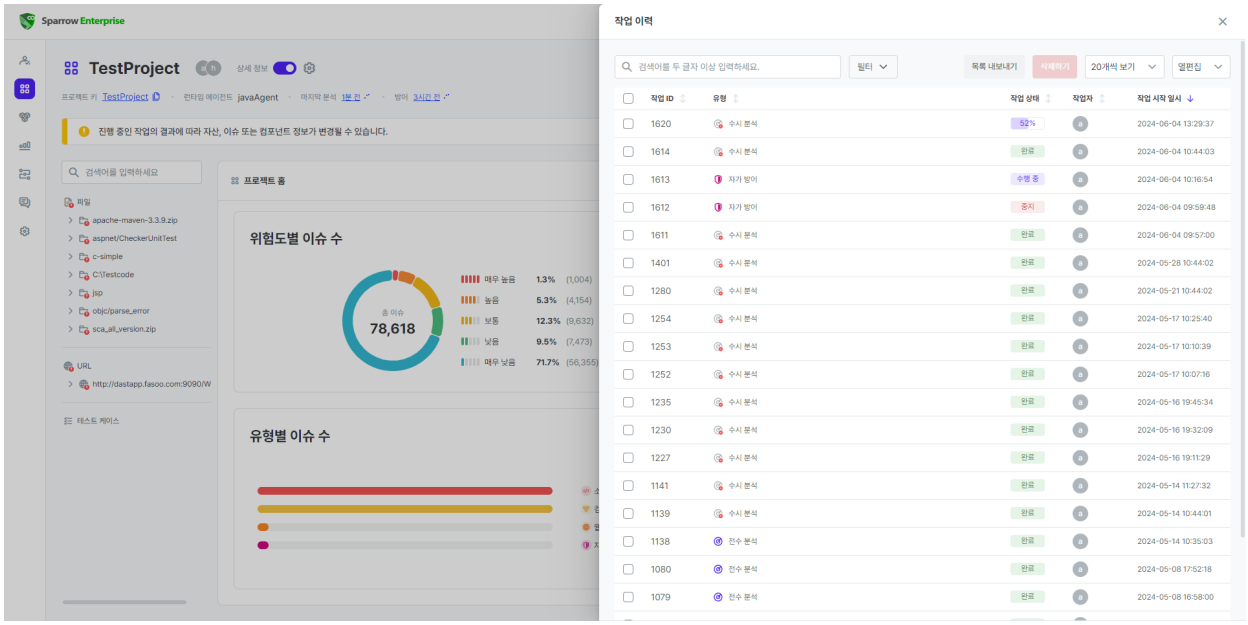
작업 보고서

사용자는 프로젝트에서 수행한 소스코드 분석, 컴포넌트 분석, 웹 취약점 분석, 자가 방어의 결과를 공유하고 검출된 이슈를 처리한 상태를 확인하기 위해서 **작업 보고서**를 출력할 수 있습니다.

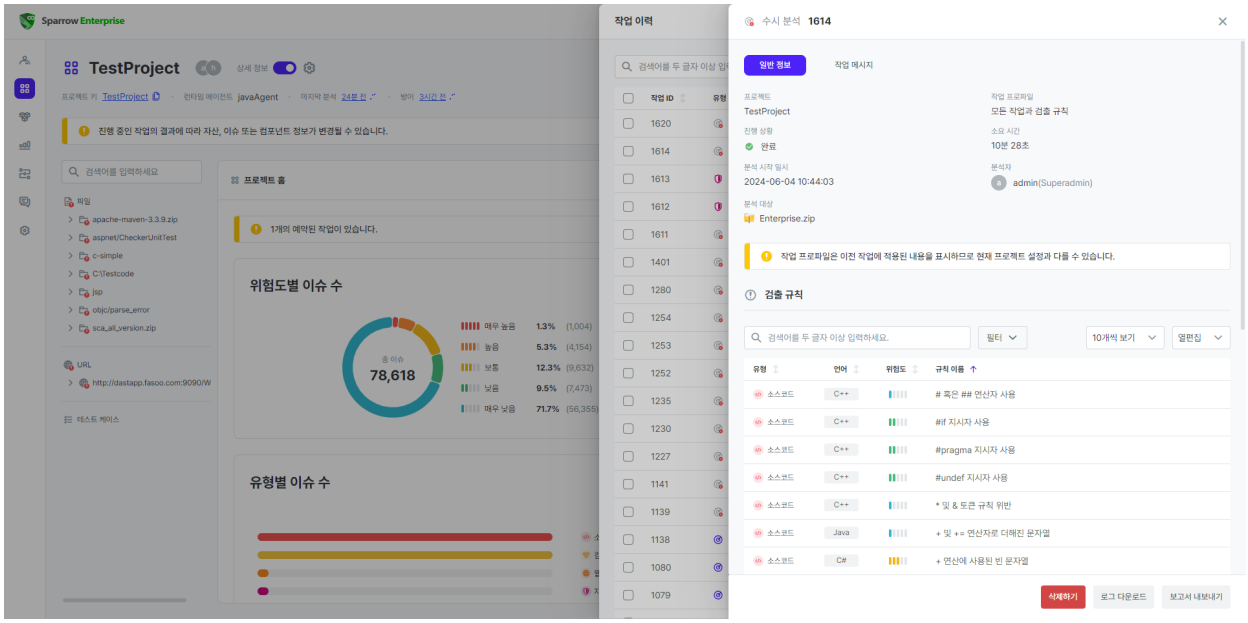
작업 보고서에는 **작업 요약 정보**, **위험도별 이슈 수**, **레퍼런스별 이슈 수**, **검출 결과 상세** 및 **제외된 이슈 목록**이 포함됩니다. 특히, 이슈 목록에서 제외된 이슈는 분석 보고서의 다른 내용에 포함되지 않고 **제외된 이슈 목록**에서만 별도로 확인할 수 있습니다. 보고서 템플릿에 대한 자세한 내용은 보고서 템플릿 관리하기를 참고하세요.

> **Warning**: 작업 보고서는 완료된 분석이나 중지된 자가 방어에서만 출력할 수 있습니다. 분석이 완료되지 않거나 실행 중인 자가 방어에서는 보고서 내보내기를 실행할 수 없습니다.

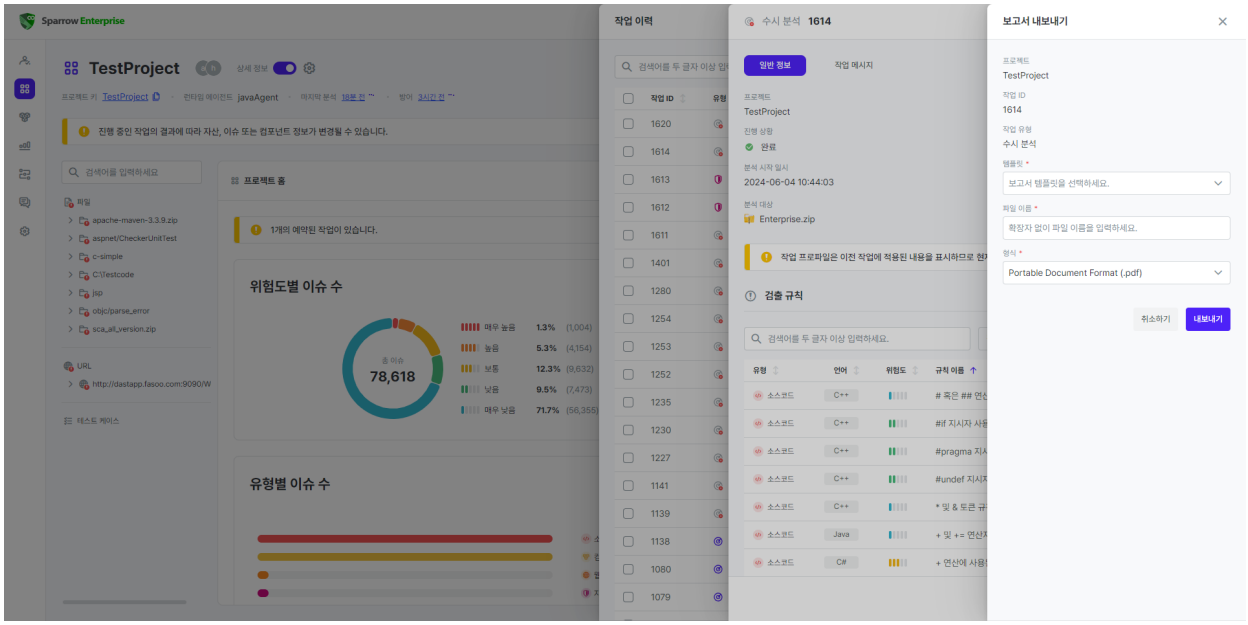
1. 프로젝트의 상세 정보 페이지로 이동하세요.
2. 오른쪽 위에 있는 **작업 이력 보기** 버튼을 클릭하세요.



3. 보고서를 생성할 작업을 선택하세요.



4. 아래쪽에 있는 **보고서 내보내기** 버튼을 클릭하세요.



5. 아래 내용을 참고하여 원하는 **템플릿**, **파일 이름**, **형식**을 선택하세요.

6. **내보내기** 버튼을 클릭하세요.

> **Tip**: 내보낸 작업 보고서는 사용자의 로컬 다운로드 디렉토리에 저장됩니다.

프로젝트

내보낼 작업 보고서가 포함된 작업의 프로젝트입니다.

작업 ID

내보낼 작업 보고서가 포함된 작업의 ID입니다.

작업 유형

내보낼 작업 보고서가 포함된 작업의 유형이며 **전수 분석**, **수시 분석**, **자가 방어** 중 하나로 표시됩니다.

템플릿*

내보낼 작업 보고서의 템플릿을 선택할 수 있습니다. 다른 보고서 템플릿을 추가하려면 보고서 템플릿 추가하기를 참고하세요.

파일 이름*

내보낼 작업 보고서의 파일 이름이며 250자 이하의 한글, 영문, 숫자, 특수 문자를 입력할 수 있습니다.

형식*

내보낼 작업 보고서의 파일 형식입니다. 작업 보고서의 파일 형식은 현재 **Portable Document Format (.pdf)**, **Microsoft Word Open XML (.docx)**, **Microsoft Excel Open XML (.xlsx)**과 **한글 문서 (.hwp)**를 지원합니다.

워크플로

DevSecOps를 구현하기 위해서 사용자는 여러 가지 툴에서 다양한 작업을 수행해야 합니다. 버전 관리 시스템에서 소스코드를 당겨와서, 소스코드 분석을 수행하고, 분석 결과 발견한 이슈가 몇 개인지 확인하고, 다시 이것을 패키징하여 배포하고, 웹 취약점을 다시 확인하는 등 복잡한 과정이 수반됩니다.

워크플로란 이렇게 **복잡한 개발-보안-운영 관리를 하나의 플랫폼에서 수행할 수 있도록 돕는** 기능입니다. 사용자는 워크플로 기능을 통해 이 과정을 평소에 실행해왔던 것보다 더 쉽고 빠르게 진행할 수 있게 됩니다. 또한 워크플로를 Sparrow Enterprise라는 플랫폼에서 수행함으로써 데이터가 쌓이게 됩니다. 따라서 현재 진행 중인 워크플로뿐만 아니라 지금까지 완료된 모든 워크플로의 히스토리를 확인할 수 있다는 장점이 있습니다.

워크플로 만들기

시스템의 **워크플로 관리** 권한이 있는 관리자는 새로운 워크플로를 추가할 수 있습니다. 워크플로에는 태스크라는 주머니와 액션이라는 돌이 있어서 워크플로에서 실제 실행할 작업을 액션에서 설정하고 다수의 작업을 태스크에 저장할 수 있도록 설계되었습니다. 워크플로, 태스크, 액션을 모두 설정해야 워크플로를 실행할 수 있습니다. 먼저 다음과 같이 워크플로의 이름을 정합니다.

1. 전체 워크플로 목록에서 **워크플로 추가하기** 버튼을 클릭하세요.

2. 아래 내용을 참고하여 **워크플로 이름**을 입력하세요.(*는 필수 입력 항목)

3. **추가하기** 버튼을 클릭하세요.

워크플로 이름*

추가할 워크플로의 이름이며 최대 50자까지 입력할 수 있습니다.

설명

추가할 워크플로의 설명이며 최대 500자까지 입력할 수 있습니다.

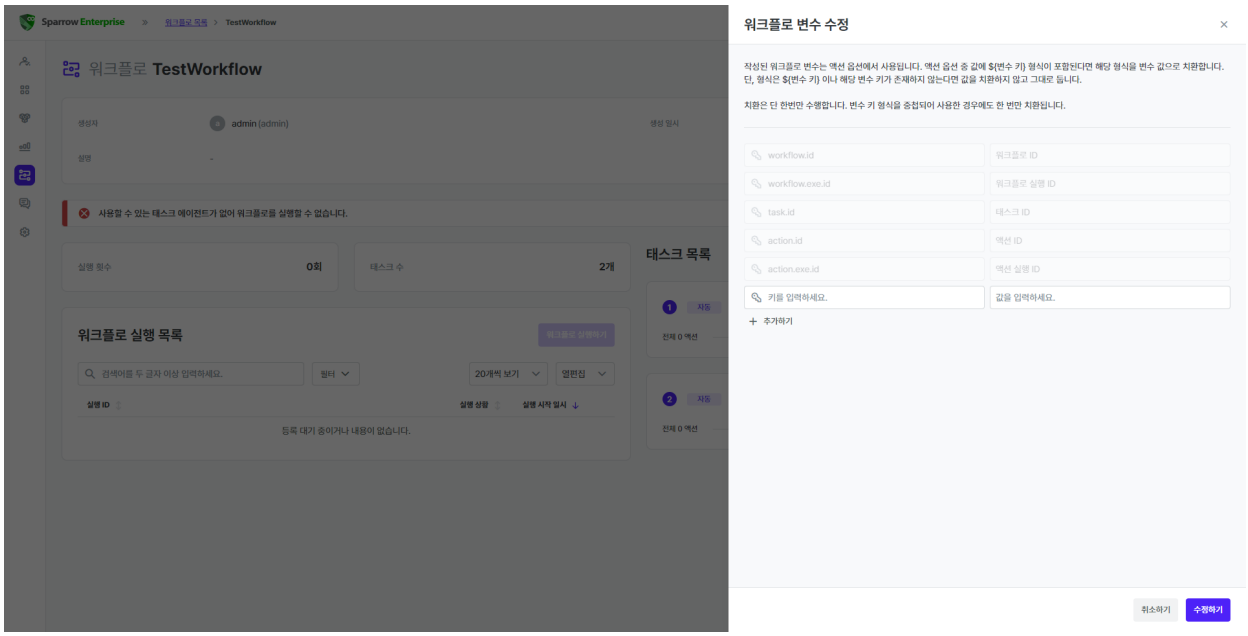
이제 워크플로가 추가되었습니다.

워크플로 변수 추가하기

커맨드라인 명령어를 실행하거나 REST API를 호출하는데 필요한 변수가 있다면 워크플로에서 해당 액션을 수행하기 전에 워크플로에 변수를 미리 저장해두세요. 그러면 액션에 입력한 값에 변수의 `${키}` 형식이 포함되는 경우 해당 형식을 입력한 값으로 바꾸어 줍니다. 하지만 `${키}` 형식이더라도 해당하는 키가 워크플로 변수에 포함되지 않는다면 바꾸지 않고 그대로 둡니다.

다음과 같은 내용을 참고하여 사용하려는 변수를 저장하세요.

1. 워크플로 상세 정보 페이지로 이동하세요.
2. 오른쪽 위에 있는 **변수 수정하기** 버튼을 클릭하세요.



3. 변수에 사용할 **키**와 **값**을 입력하세요.

> **Tip**: 목록의 아래에 있는 **+ 추가하기** 버튼을 클릭하여 키값 쌍을 추가로 입력할 수 있습니다.

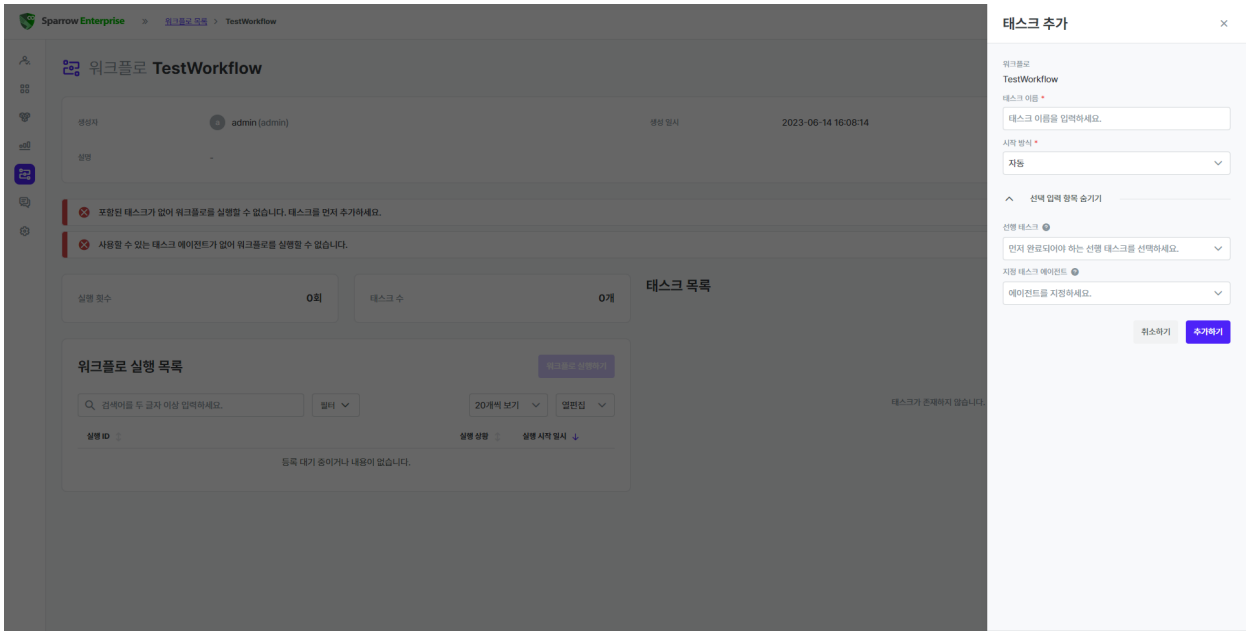
4. 모든 변수를 입력하고 **수정하기** 버튼을 클릭하세요.

워크플로를 실행할 때 여기에 입력한 변수의 키나 값을 변경하거나 추가로 다른 변수를 입력할 수 있습니다. 자세한 내용은 태스크와 액션을 모두 만든 후에 워크플로 실행하기를 참고하세요.

태스크 추가하기

태스크는 워크플로에서 여러 개의 액션을 하나로 모아두는 역할을 하고 있습니다. 여러 개의 액션을 태스크 단위로 구분하여 어떤 것을 먼저 실행할지 우선순위를 결정합니다. 따라서 태스크의 순서에 유의해서 정렬하는 것이 좋습니다.

1. 워크플로 상세 정보 페이지에서 **태스크 추가하기** 버튼을 클릭하세요.



2. **태스크 이름**을 입력하고 **시작 방식**을 선택하세요.
3. 아래 내용을 참고하여 다른 항목을 입력하세요.(*는 필수 입력 항목)
4. **추가하기** 버튼을 클릭하세요.

워크플로

태스크를 추가할 워크플로의 이름이며 변경할 수 없습니다.

태스크 이름*

추가할 태스크의 이름이며 최대 50자까지 입력할 수 있습니다.

시작 방식*

추가할 태스크의 시작 방식이며 자동과 수동 중에 하나를 선택할 수 있습니다. 자동으로 설정된 태스크는 선행 태스크가 없거나 모든 선행 태스크가 완료된 경우 자동으로 실행됩니다. 수동으로 설정된 태스크는 선행 태스크가 없거나 모든 선행 태스크가 완료된 경우 사용자가 **시작하기**를 클릭하여 실행시키게 됩니다.(기본값: 자동)

선행 태스크

추가할 태스크를 실행하기 전에 먼저 완료되어야 하는 태스크입니다. 동일한 워크플로에 포함된 태스크 중에서 하나 이상의 태스크를 선택할 수 있습니다.

> **Tip**: **선행 태스크**가 없는 태스크는 알파벳 순으로 나열됩니다.

지정 태스크 에이전트

추가할 태스크의 액션을 수행하도록 명령을 전달할 태스크 에이전트입니다. 에이전트를 지정하는 경우 태스크에 포함된 모든 액션은 해당 에이전트에서 수행됩니다. 하지만 지정된 에이전트를 사용할 수 없다면 태스크가 실패하게 됩니다. 에이전트를 지정하지 않는 경우 임의의 에이전트에서 태스크에 포함된 액션이 수행됩니다.

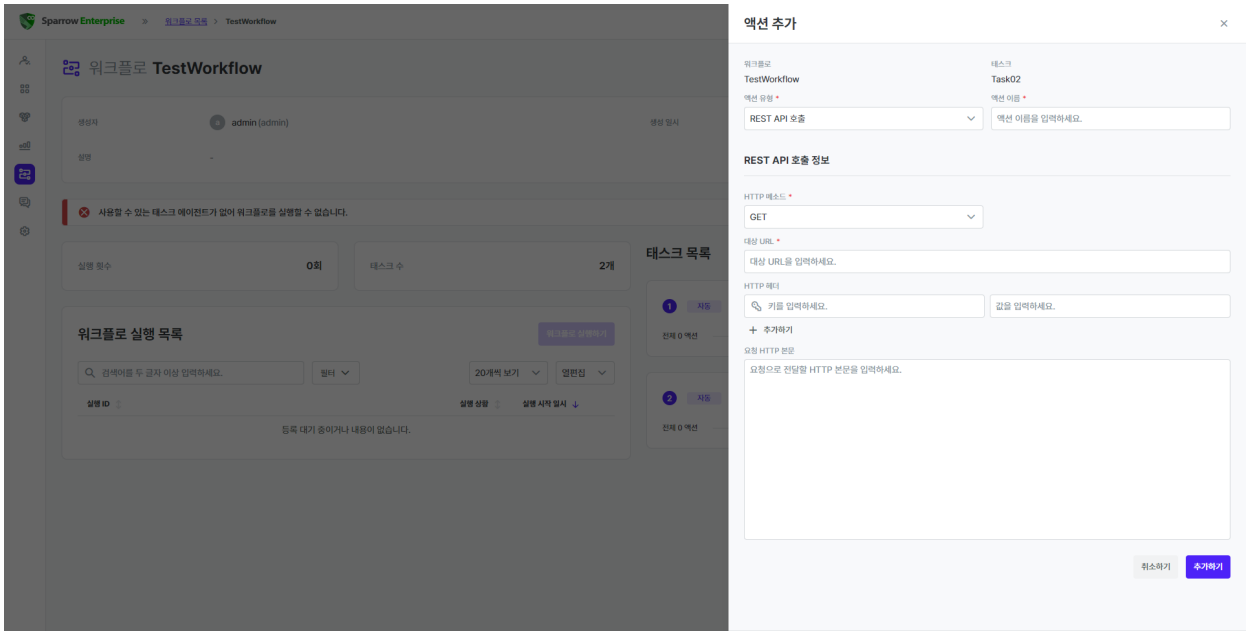
> **Tip**: 태스크 에이전트에 대한 설명이나 설치 방법은 태스크 에이전트 설치하기를 참고하세요.

액션 추가하기

이제 태스크에 액션을 추가하겠습니다. 현재 태스크에서 수행할 수 있는 액션은 **커맨드라인 실행**과 **REST API 호출** 두 가지입니다.

> **Warning**: 하나의 태스크에서는 한 개의 에이전트를 사용하도록 설계되었습니다. 에이전트는 사용자가 설치한 머신에서 동작하며 Sparrow Enterprise 서버와 통신합니다. 따라서 태스크에 **여러 액션을 추가할 때 모두 동일한 IP의 머신에서 수행되도록** 설정해야 합니다.

1. 태스크에서 **액션 추가하기** 버튼을 클릭하세요



> **Tip**: 캡쳐된 화면은 **액션 유형**이 **REST API 호출 정보**인 경우에 입력할 슬라이드입니다.

2. **액션 유형**을 입력하고 **액션 이름**을 입력하세요.
3. 아래 내용을 참고하여 **커맨드라인 실행 정보**나 **REST API 호출 정보**를 입력하세요.(*는 필수 입력 항목)
4. **추가하기** 버튼을 클릭하세요.

워크플로

액션을 추가할 워크플로의 이름이며 변경할 수 없습니다.

태스크

액션을 추가할 태스크의 이름이며 변경할 수 없습니다.

액션 유형*

추가할 액션의 유형이며 **커맨드라인 실행**과 **REST API 호출** 중에 하나를 선택할 수 있습니다.

액션 이름*

추가할 액션의 이름이며 최대 50자까지 입력할 수 있습니다.

✓ 커맨드라인 실행 정보

실행 명령어 내용*

커맨드라인으로 실행할 명령어입니다. 워크플로에서 설정한 변수를 이 옵션에 입력할 수 있습니다.

작업 디렉토리

위 옵션에 입력한 커맨드라인을 실행할 작업 디렉토리 경로입니다.

> **Tip**: **커맨드라인 실행**에는 명령어를 실행할 머신의 IP를 입력하지 않기 때문에 특정 머신을 지정할 수 없다는 사실에 유의하세요. 여러 머신으로부터 사용 가능한 에이전트가 연결된 경우 그중에 **작업 디렉토리가 일치하는 머신에서** 옵션에 입력한 실행 명령어를 실행합니다.
>
> 다만, 태스크를 만들 때 **지정 태스크 에이전트**를 선택하여 태스크 에이전트가 작동 중인 머신에서 커맨드라인을 실행하도록 하는 방법이 있습니다. 태스크 에이전트를 지정하는 방법은 태스크 추가하기 에서 **지정 태스크 에이전트** 옵션을 참고하세요.

✓ REST API 호출 정보

HTTP 메소드*

REST API를 호출하는데 사용할 HTTP 메소드입니다. `GET`, `HEAD`, `POST`, `PUT`, `DELETE`, `CONNECT`, `OPTIONS`, `TRACE`, `PATCH` 중에 하나를 선택할 수 있습니다.(기본값: `GET`)

대상 URL*

REST API 호출을 수행할 대상 URL입니다. 이 옵션은 `https://`로 시작하는 URL 형식으로 입력해야 합니다.

HTTP 헤더

REST API 호출을 수행할 때 대상 URL로 보내는 HTTP 요청에 추가할 헤더의 키와 값 목록입니다. 키와 값의 쌍으로 되어있으며 목록의 아래에 있는 **+ 추가하기** 버튼을 클릭하여 하나 이상의 키값을 입력할 수 있습니다.

요청 HTTP 본문

REST API 호출을 수행할 때 대상 URL에 대한 요청으로 전송할 HTTP 본문입니다. 값이 존재하지 않는 경우 별도의 본문을 전달하지 않습니다. 워크플로에서 설정한 변수를 이 옵션에 입력할 수 있습니다.

> **Tip**: 태스크를 만들 때 **지정 태스크 에이전트**를 선택하지 않은 경우 대상 URL에 해당하는 머신으로부터 사용 가능한 에이전트를 사용합니다. 해당 머신에서 하나 이상의 에이전트가 연결되어 있다면 임의의 에이전트를 사용하게 됩니다.

워크플로 실행하기

이제 워크플로를 실행하겠습니다. 다음과 같은 동작을 수행하세요.

1. 워크플로 상세 정보 페이지로 이동하세요.
2. **워크플로 실행하기** 버튼을 클릭하세요.
3. **워크플로 실행** 슬라이드에서 미리 설정한 **워크플로 변수**의 **키**와 **값**을 변경하거나 새로 입력하세요.

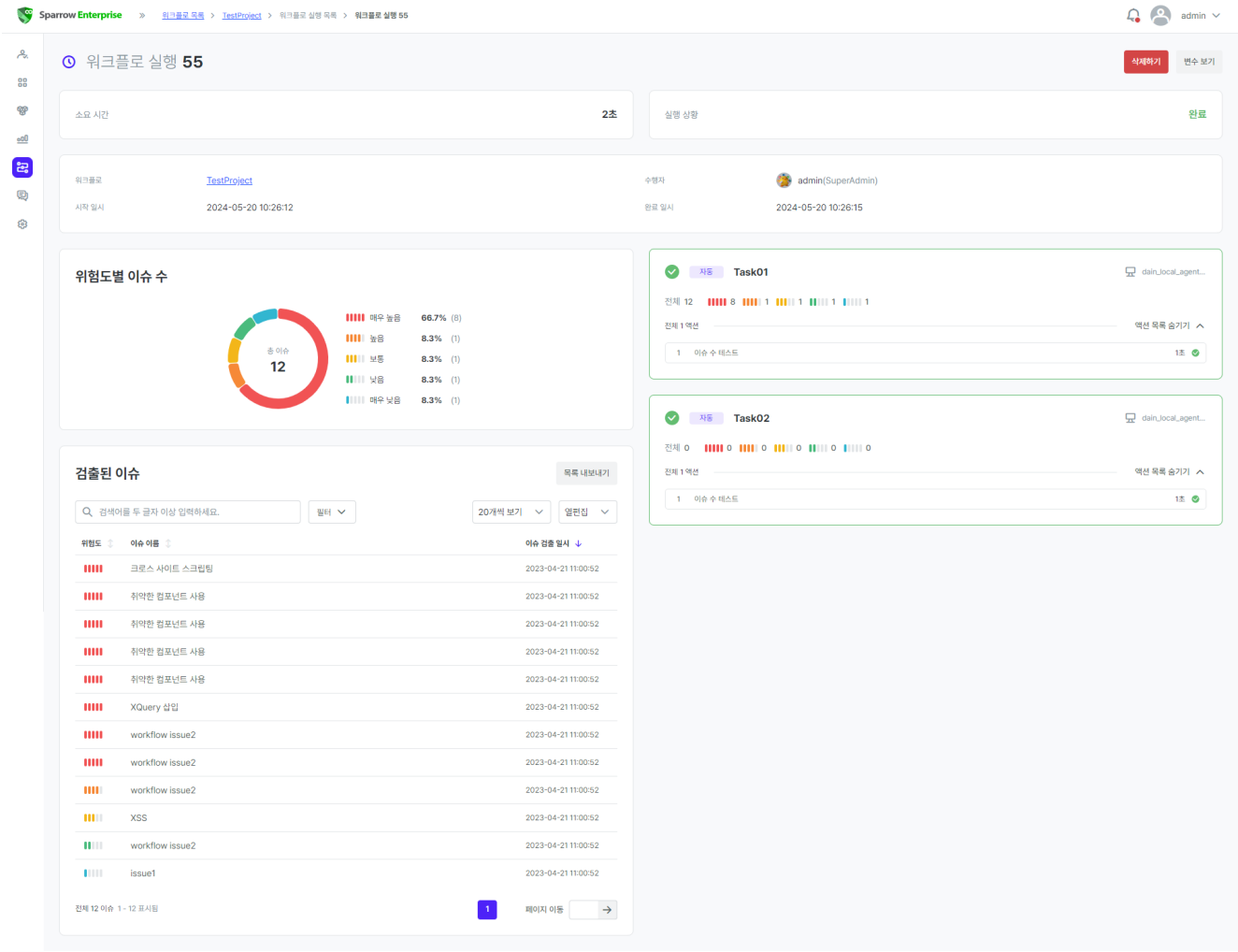
> **Tip**: 워크플로 변수 추가하기에서 입력한 변수가 기본값으로 표시됩니다.

4. **실행하기** 버튼을 클릭하세요.

이제 워크플로가 실행됩니다.

워크플로 실행 확인하기

실행한 워크플로는 워크플로 상세 정보 페이지의 워크플로 실행 목록에 표시됩니다. 목록을 클릭하면 태스크나 액션과 관련된 정보와 실행된 워크플로에서 검출한 이슈를 포함하는 **워크플로 실행 상세 정보** 페이지를 확인할 수 있습니다.



✓ 워크플로 실행 정보

워크플로 실행에 대한 정보입니다. 워크플로 실행 정보에는 워크플로의 **실행 상황**과 **소요 시간**이 표시됩니다.

워크플로 실행을 수행 중인 경우 **중지하기** 버튼을 클릭하여 워크플로를 중지할 수 있습니다. 워크플로 실행이 실패하거나 완료된 경우 **삭제하기** 버튼을 클릭하여 워크플로 실행을 삭제할 수 있습니다. **변수 보기** 버튼을 클릭하면 해당 워크플로 실행에 사용한 변수를 확인할 수 있습니다.

✓ 위험도별 이슈 수

워크플로 실행에서 검출된 이슈의 개수를 **매우 높음**, **높음**, **보통**, **낮음**, **매우 낮음**이라는 위험도에 따라 5단계로 구분하여 그래프로 표시합니다.

✓ 검출된 이슈

워크플로 실행에서 검출한 이슈의 목록입니다. 검출된 이슈 목록에는 검출된 이슈의 **위험도**, **이슈 이름**, **이슈 검출 일시**가 표시됩니다.

여기서 **목록 내보내기**를 클릭하고 **파일 이름**을 입력하여 **.csv**, **.xlsx**, **.cell** 형식의 파일을 다운로드할 수 있습니다. 이 파일에는 검출된 모든 이슈 중에서 목록에 나열된 이슈가 포함됩니다.

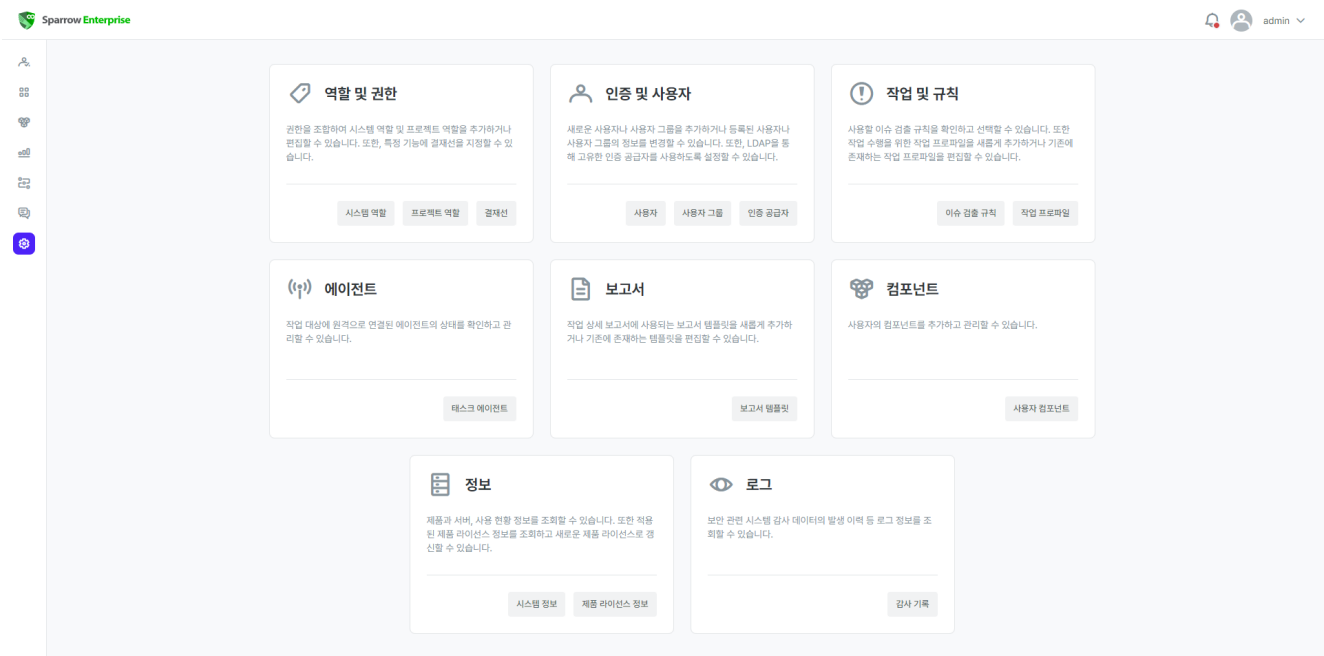
✓ 태스크 실행 목록

페이지의 오른쪽에 있는 태스크 실행 목록은 실제 실행된 태스크와 액션에 대한 정보를 표시합니다. 태스크와 관련된 정보에는 **태스크 상태**, **태스크 시작 방식**, **태스크 이름**, **선행 태스크 목록**, **지정 태스크 에이전트**, 태스크에서 검출된 **이슈 수**가 포함되고, 액션과 관련된 정보에는 **액션 이름**, **액션 실행 소요 시간**, **액션 실행 상황**이 포함됩니다.

액션을 클릭하면 수행된 액션에 대한 좀 더 자세한 내용을 확인할 수 있습니다. 여기에는 **액션 실행 ID**, 액션의 **유형**, **진행 상황**, 액션이 포함된 **워크플로**, **워크플로 실행 ID**, **태스크 이름**이 표시됩니다. 또한 **로그 다운로드하기** 버튼을 클릭하여 실행된 액션의 분석 로그를 다운로드할 수 있습니다.

관리

시스템 권한이 있는 관리자의 경우 기본 메뉴에서 **관리** 아이콘을 클릭하면 다음과 같은 메뉴를 확인할 수 있습니다. 관리 메뉴에서는 Sparrow Enterprise 시스템의 여러 가지 기능을 확인하고 변경할 수 있습니다.



✓ 역할 및 권한

시스템 역할

시스템 역할 탭에서는 시스템 역할 정보를 확인하고 변경할 수 있으며 **역할 및 권한 관리** 권한이 있는 관리자만 해당 탭에 접근할 수 있습니다. 자세한 내용은 시스템 역할 관리하기를 참고하세요.

프로젝트 역할

프로젝트 역할 탭에서는 프로젝트 역할 정보를 확인하고 변경할 수 있으며 **역할 및 권한 관리** 권한이 있는 관리자만 해당 탭에 접근할 수 있습니다. 자세한 내용은 프로젝트 역할 관리하기를 참고하세요.

결재선

결재선 탭에서는 특정 기능에 결재선을 지정할 수 있으며 **역할 및 권한 관리** 권한이 있는 관리자만 해당 탭에 접근할 수 있습니다. 자세한 내용은 결재선 관리하기를 참고하세요.

✓ 인증 및 사용자

사용자

사용자 탭에서는 등록된 사용자 목록 및 사용자 정보를 확인하고 변경할 수 있으며 **인증 및 사용자 관리** 권한이 있는 관리자만 해당 탭에 접근할 수 있습니다. 자세한 내용은 사용자 관리하기를 참고하세요.

사용자 그룹

사용자 그룹 탭에서는 등록된 사용자를 사용자 그룹에 추가하고 변경할 수 있으며 **인증 및 사용자 관리** 권한이 있는 관리자만 해당 탭에 접근할 수 있습니다. 자세한 내용은 사용자 그룹 관리하기를 참고하세요.

인증 공급자

인증 공급자 탭에서는 LDAP을 사용하는 사용자의 외부 인증 공급자 정보를 등록할 수 있습니다. 자세한 내용은 인증 공급자 관리하기를 참고하세요.

✓ 작업 및 규칙

이슈 검출 규칙

이슈 검출 규칙 탭에서는 등록된 이슈 검출 규칙을 확인하고 활성화할 수 있습니다. 자세한 내용은 이슈 검출 규칙 관리하기를 참고하세요.

작업 프로파일

작업 프로파일 탭에서는 이슈 검출 규칙과 작업 옵션과 같이 작업에 필요한 정보를 묶어서 프로젝트의 특정 작업을 수행할 때 사용할 수 있도록 설정할 수 있습니다. 자세한 내용은 작업 프로파일 관리하기를 참고하세요.

✓ 에이전트

태스크 에이전트

태스크 에이전트 탭에서는 워크플로에서 태스크를 실행할 때 사용하는 태스크 에이전트 등록 정보 및 실행 상황을 확인할 수 있습니다. 자세한 내용은 태스크 에이전트 관리하기를 참고하세요.

✓ 보고서

보고서 템플릿

보고서 템플릿 탭에서는 수행한 작업에 대한 보고서를 출력할 때 사용할 보고서의 형식을 새롭게 추가하거나 기존 형식을 수정할 수 있습니다. 자세한 내용은 보고서 템플릿 관리하기를 참고하세요.

✓ **컴포넌트**

사용자 컴포넌트

사용자 컴포넌트 탭에서는 Sparrow 데이터 웨어하우스에서 검출하지 않는 특정 파일을 컴포넌트로 추가함으로써 컴포넌트 분석에서 해당 파일을 컴포넌트로 식별하도록 설정할 수 있습니다. 자세한 내용은 사용자 컴포넌트 관리하기를 참고하세요.

✓ **정보**

시스템 정보

시스템 정보 페이지에서는 시스템 정보를 확인할 수 있으며 **시스템 관리** 권한이 있는 관리자만 해당 페이지에 접근할 수 있습니다. 자세한 내용은 시스템 정보 확인을 참고하세요.

제품 라이선스 정보

제품 라이선스 정보 페이지에서는 Sparrow Enterprise를 사용할 수 있는 권한인 제품 라이선스 정보를 확인하고 변경할 수 있습니다. 이 페이지는 **시스템 관리** 권한이 있는 관리자만 해당 페이지에 접근할 수 있습니다. 자세한 내용은 제품 라이선스 정보 확인을 참고하세요.

✓ **로그**

감사 기록

감사 기록 페이지에서는 Sparrow Enterprise에서 발생한 이벤트를 확인할 수 있으며 **시스템 관리** 권한이 있는 관리자만 해당 페이지에 접근할 수 있습니다. 자세한 내용은 감사 기록 확인을 참고하세요.

역할 및 권한

시스템 역할 관리하기

시스템 역할은 시스템을 사용하기 위해 부여되는 권한을 모은 정보입니다. **시스템 역할** 메뉴에서는 등록된 역할의 목록 및 역할 정보를 확인하고 변경할 수 있습니다.

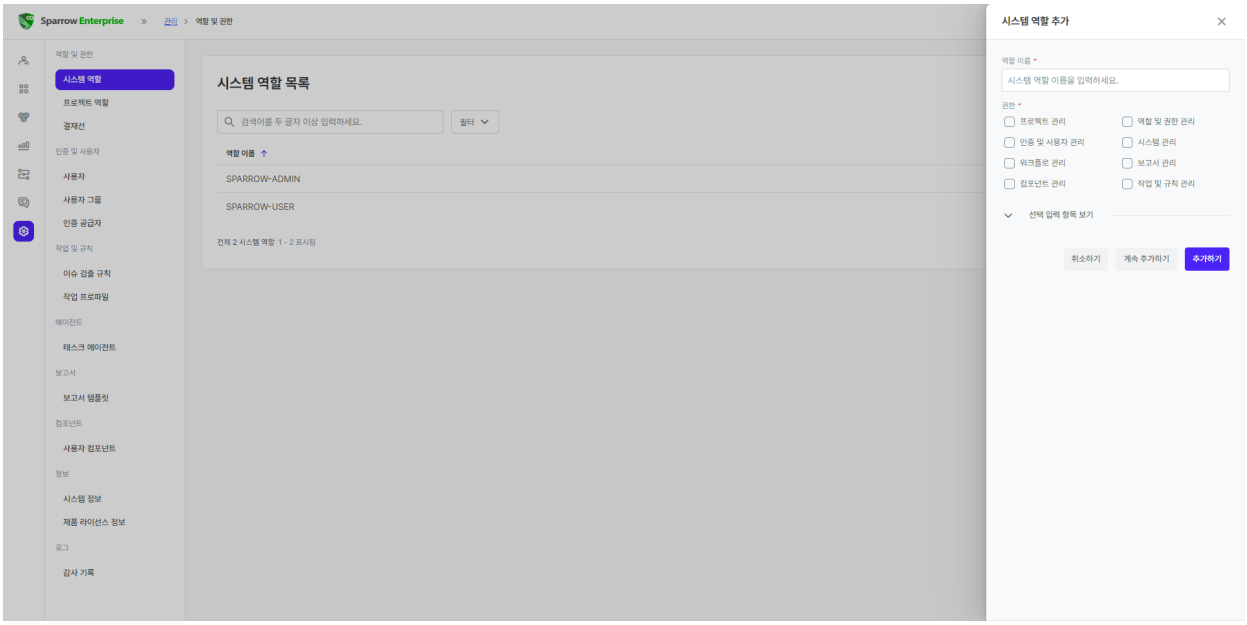
1. 왼쪽 사이드 바에서 **관리**를 클릭하세요.
2. **사용자** 메뉴에서 **시스템 역할**을 클릭하세요.

시스템 역할 추가하기

시스템의 **역할 및 권한 관리** 권한이 있는 관리자는 **관리** 메뉴의 **시스템 역할** 페이지에서 다음과 같은 방법으로 새 시스템 역할을 추가할 수 있습니다.

> **Tip**: 시스템 역할에는 모든 시스템 권한을 가진 `SPARROW-ADMIN`과 아무 시스템 권한이 없는 `SPARROW-USER`라는 역할이 기본적으로 설정되어 있습니다. 기본 설정된 두 역할은 수정하거나 삭제할 수 없습니다. 다른 역할을 추가하여 시스템 역할을 커스터마이징하세요.

1. **시스템 역할** 페이지에서 오른쪽 위에 있는 **시스템 역할 추가하기** 버튼을 클릭하세요.



2. 아래의 내용을 참고하여 역할에 부여할 정보를 입력하세요.(*는 필수 입력 항목)
3. **추가하기** 버튼을 클릭하세요.
4. 역할이 성공적으로 추가되면 왼쪽 아래에 성공 메시지가 출력됩니다.

역할 이름*

시스템 역할의 이름이며 50자 이하의 한글, 영문, 숫자, 특수 문자, 공백을 입력할 수 있습니다.

권한*

역할에 부여할 권한이며 다음 중 하나 이상의 권한을 선택할 수 있습니다.

- 프로젝트 관리 : 프로젝트를 추가하거나, 이미 생성된 프로젝트의 정보를 수정하고 프로젝트를 삭제할 수 있습니다.

> **Tip**: 프로젝트 관리 권한이 있는 시스템 역할의 사용자라도 프로젝트에서 작업을 수행하기 위해서는 작업 수행 권한이 있는 프로젝트 역할이 필요합니다.

- 역할 및 권한 관리 : 시스템 역할과 프로젝트 역할을 생성하거나 수정할 수 있습니다.

> **Tip**: 역할 및 권한 관리는 Sparrow Enterprise의 시스템 전체에서 사용할 역할을 관리합니다. 특정 사용자에게 역할을 부여하려면 아래의 인증 및 사용자 관리 권한이 필요합니다.

- 인증 및 사용자 관리 : 사용자 및 사용자 그룹을 추가하거나 사용자에 관련된 정보, 예를 들어 비밀번호나 사용자 역할을 변경할 수 있습니다. Sparrow Enterprise에 LDAP을 사용하는 인증 방법을 설정하는 권한도 포함되어 있습니다.
- 시스템 관리 : 시스템 정보, 제품 라이선스 정보, 로그를 확인할 수 있습니다. 제품 라이선스를 갱신할 수 있는 권한이기도 합니다.
- 워크플로 관리 : 워크플로를 관리하거나 사용하기 위해 필요합니다.
- 보고서 관리 : 보고서 템플릿을 생성하거나 수정하고 삭제할 수 있습니다.

> **Tip**: 보고서 관리는 보고서 템플릿과 관련된 관리 기능에 접근할 수 있는 권한입니다. 프로젝트에서 작업 보고서를 출력하려면 프로젝트 구성원이어야 합니다. 프로젝트에서 `PROJECT-VIEWER`와 같은 낮은 권한이 있는 사용자도 보고서를 출력할 수 있습니다.

- 컴포넌트 관리 : 컴포넌트 분석에서 사용할 수 있는 사용자 컴포넌트를 추가하고 수정할 수 있습니다.

> **Tip**: 사용자 컴포넌트는 Sparrow 데이터 웨어하우스에서 제공하지 않는 사용자가 지정한 컴포넌트를 의미합니다. 자세한 내용은 사용자 컴포넌트 관리를 참고하세요.

- 작업 및 규칙 관리 : 작업 중 분석 및 자가 방어에 사용할 이슈 검출 규칙 목록을 가져오거나 이슈 검출 규칙을 추가할 수 있습니다. 또한, 작업에 사용할 작업 프로파일을 생성하고 수정할 수도 있습니다.

설명

시스템 역할에 대한 설명을 입력하세요.

시스템 역할 변경하기

이제 앞에서 추가한 역할로 사용자의 시스템 역할을 변경하려는 경우 다음을 참고하세요.

1. 관리 메뉴의 **사용자** 페이지로 이동하세요.
2. 사용자 목록에서 역할을 변경할 사용자의 체크박스를 선택하세요.
3. 오른쪽에 있는 **수정하기** 버튼을 클릭하세요.

> **Tip**: 새로운 사용자에게 역할을 주려는 경우 사용자 목록에서 **사용자 추가하기** 버튼을 클릭하고 새로운 사용자를 추가하세요. 자세한 내용은 사용자 추가하기를 참고하세요.

4. 새로운 **역할**을 선택하세요.
5. **수정하기** 버튼을 클릭하세요.

프로젝트 역할 관리하기

프로젝트 역할은 프로젝트에 대해 부여되는 권한을 모은 정보입니다. **프로젝트 역할** 메뉴에서는 등록된 역할의 목록 및 역할 정보를 확인하고 변경할 수 있습니다.

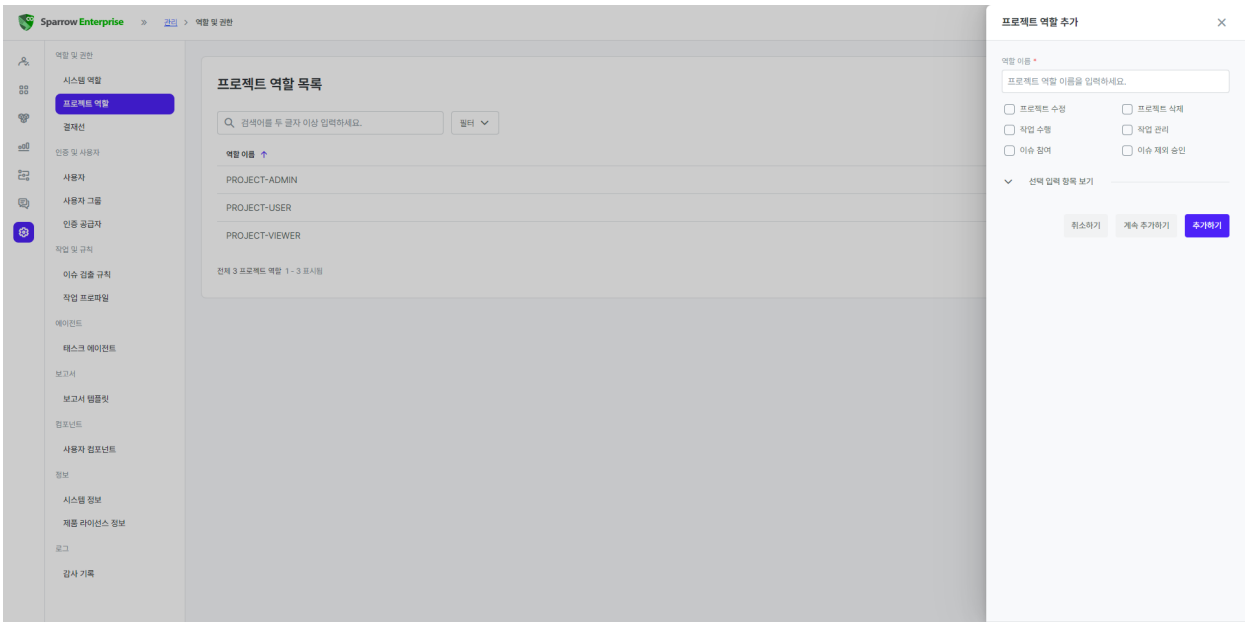
1. 왼쪽 사이드 바에서 **관리**를 클릭하세요.
2. **사용자** 메뉴에서 **프로젝트 역할** 탭을 클릭하세요.

프로젝트 역할 추가하기

시스템의 **역할 및 권한 관리** 권한이 있는 관리자는 **관리** 메뉴의 **프로젝트 역할** 페이지에서 다음과 같은 방법으로 새 프로젝트 역할을 추가할 수 있습니다.

> **Tip**: 프로젝트 역할에는 프로젝트를 마음껏 수정할 수 있는 권한을 가진 `PROJECT-ADMIN`과 프로젝트에서 분석을 수행할 사용할 수 있는 일부 권한이 있는 `PROJECT-USER`, 프로젝트의 구성원으로서 조회 이외에는 다른 권한이 없는 `PROJECT-VIEWER`라는 역할이 기본적으로 설정되어 있습니다. 기본 설정된 세 역할은 수정하거나 삭제할 수 없습니다. 다른 역할을 추가하여 프로젝트 역할을 커스터마이징하세요.

1. **프로젝트 역할** 페이지에서 오른쪽 위에 있는 **프로젝트 역할 추가하기** 버튼을 클릭하세요.



2. 아래의 내용을 참고하여 역할에 부여할 정보를 입력하세요.(*는 필수 입력 항목)

3. **추가하기** 버튼을 클릭하세요.

4. 역할이 성공적으로 추가되면 왼쪽 아래에 성공 메시지가 출력됩니다.

역할 이름*

프로젝트 역할의 이름이며 50자 이하의 한글, 영문, 숫자, 특수 문자, 공백을 입력할 수 있습니다.

권한

역할에 부여할 권한이며 하나 이상의 권한을 선택할 수 있습니다.

- 프로젝트 수정 : 권한이 있는 프로젝트의 기본 정보, 구성원, 작업 프로파일 활성화, 웹훅 등 프로젝트 설정에 포함된 정보를 수정할 수 있습니다.
- 프로젝트 삭제 : 권한이 있는 프로젝트 및 해당 프로젝트에 포함된 모든 정보를 삭제할 수 있습니다.
- 작업 수행 : 권한이 있는 프로젝트에서 작업을 수행할 수 있습니다.
- 작업 관리 : 권한이 있는 프로젝트에서 작업을 중지하거나 삭제할 수 있습니다.
- 이슈 참여 : 권한이 있는 프로젝트에서 이슈의 상태를 변경하거나, 이슈의 담당자 중 한 명으로써 담당자를 지정할 수 있습니다.

> **Tip**: 프로젝트 권한은 모두 독립적이며 다른 권한의 상위 권한으로 동작하지 않습니다. 예를 들어, 작업 관리 권한이 작업 수행 권한을 포함하고 있지 않다는 것에 유의하세요.

설명

프로젝트 역할에 대한 설명을 입력하세요.

프로젝트 역할 변경하기

이제 앞에서 추가한 역할로 사용자의 프로젝트 역할을 변경하려는 경우 다음을 참고하세요.

1. 프로젝트 역할을 변경하려는 프로젝트의 **프로젝트 상세 정보** 페이지로 이동하세요.
2. 오른쪽 위에 있는 **프로젝트 수정하기** 버튼을 클릭하세요.
3. **구성원** 목록에서 역할을 변경할 사용자의 체크박스를 선택하세요.
4. **구성원** 목록에 있는 **수정하기** 버튼을 클릭하세요.

> **Tip**: 다른 사용자를 구성원으로 추가하려는 경우 **구성원** 목록에서 **추가하기** 버튼을 클릭하고 새로운 **구성원**을 선택하세요.

5. 새로운 **역할**을 선택하세요.
6. **수정하기** 버튼을 클릭하세요.

결재선 관리하기

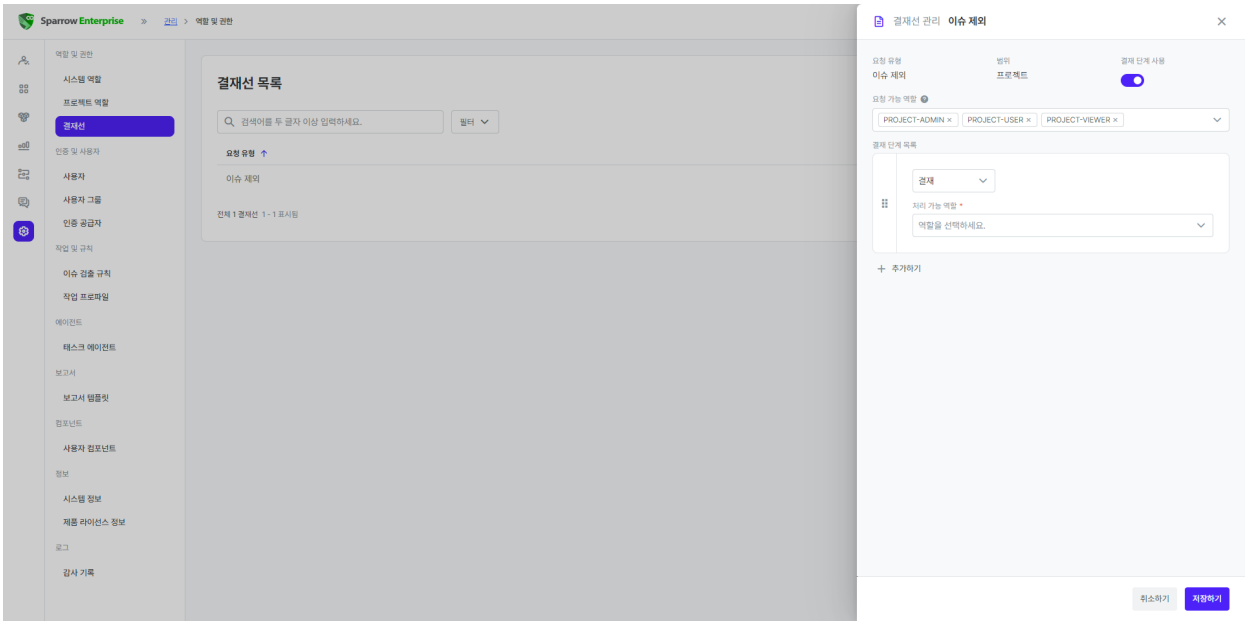
결재선은 특정 동작에 대해 승인을 요청하고 이 요청을 승인하거나 반려하는 절차를 추가하는 기능입니다. **결재선** 메뉴에서는 결재선을 만들 수 있는 동작이 무엇인지 확인할 수 있습니다.

1. 왼쪽 사이드 바에서 **관리**를 클릭하세요.
2. **역할 및 권한** 메뉴에서 **결재선** 탭을 클릭하세요.

결재선 변경하기

시스템의 **역할 및 권한 관리** 권한이 있는 관리자는 **관리** 메뉴의 **결재선** 페이지에서 다음과 같은 방법으로 결재선의 세부 내용을 변경할 수 있습니다.

1. 관리 메뉴의 **결재선** 페이지로 이동하세요.
2. 결재선 목록에서 변경할 항목을 선택하세요.



3. **결재 단계 사용**을 활성화하고 단계를 추가하세요.

4. 아래를 참고하여 옵션을 선택하고 **저장하기** 버튼을 클릭하세요.

요청 유형

결재를 요청하는 목적입니다. 요청 유형은 기본 설정되어 있으며 사용자가 수정할 수 없습니다.

범위

결재가 미치는 영향의 범위를 의미합니다. 범위는 기본 설정되어 있으며 사용자가 수정할 수 없습니다. 이슈 제외 요청은 프로젝트 범위의 결재로 설정되어 있습니다.

결재 단계 사용

결재 단계를 사용하는 경우 이 옵션을 활성화해야 합니다. 이 옵션을 사용하지 않는 경우 결재를 요청하는 즉시 승인하게 됩니다.

요청 가능 역할

결재선 기능에서는 역할에 따라 결재를 요청할 수 있는 사용자를 구분합니다. 따라서 여기에 선택된 역할을 가진 사용자가 결재를 요청할 수 있습니다. 결재의 범위가 시스템인 경우, 시스템 역할 중에서 역할을 선택해야 합니다. 결재의 범위가 프로젝트인 경우, 프로젝트 역할 중에서 역할을 선택해야 합니다.

역할을 선택하지 않는 경우 기본값은 **모든 역할**로 설정됩니다. 기본 설정된 역할 이외에 새로운 역할을 추가하려는 경우 시스템 역할 추가하기 또는 프로젝트 역할 추가하기를 참고하세요.

결재 단계 목록

결재 단계는 결재를 승인 받는 절차이며 결재 유형과 처리 가능 역할을 포함합니다. 결재선에는 최대 5개의 결재 단계를 설정할 수 있습니다. 단, 이 옵션은 결재 단계 사용 옵션을 비활성화하는 경우 표시되지 않습니다.

결재 유형

결재 방법을 결재와 합의로 구분합니다. 결재를 선택하는 경우 결재 요청을 승인하거나 반려하게 됩니다. 합의를 선택하는 경우 결재 요청에 동의하거나 반대하게 됩니다.

결재를 승인하는 경우, 다음 결재 단계가 시작됩니다. 만약 다음 단계가 없다면 결재가 완료됩니다. 결재를 반려하는 경우, 다음 결재 단계가 시작되지 않고 결재 요청 이전으로 돌아갑니다. 합의의 경우, 결재에 동의 혹은 반대가 선택되기만 하면 다음 결재 단계가 시작됩니다.

> **Tip**: 가장 마지막 결재 단계의 유형은 결재여야 합니다.

처리 가능 역할*

결재 단계를 처리할 수 있는 역할을 의미합니다. 여기에 선택된 역할을 가진 사용자가 해당 결재 단계를 처리할 수 있습니다. 결재의 범위가 시스템인 경우, 시스템 역할 중에서 역할을, 결재의 범위가 프로젝트인 경우, 프로젝트 역할 중에서 역할을 선택해야 합니다. 또한, 적어도 하나 이상의 역할을 선택해야 합니다.

> **Tip**: 이슈 제외 결재선의 경우 범위가 프로젝트이므로 프로젝트 역할 중에서 역할을 선택해야 합니다.

인증 및 사용자

사용자 관리하기

시스템의 **인증 및 사용자 관리** 권한이 있는 관리자는 **사용자** 메뉴에서 등록된 사용자 목록 및 사용자 정보를 확인하고 변경할 수 있습니다. 사용자 목록을 확인하는 방법은 다음과 같습니다.

1. 왼쪽 사이드 바에서 **관리**를 클릭하세요.
2. **사용자** 메뉴에서 **사용자**를 클릭하세요.

사용자 목록에 표시되는 각 항목에 대한 설명은 아래의 내용을 참고하세요.

ID

사용자 계정의 ID입니다.

이름

사용자 계정의 이름입니다.

아바타

사용자 계정의 아바타 이미지입니다.

활성화

사용자 계정의 활성화 상태입니다. **활성**이나 **비활성** 중 하나로 표시되며 권한 있는 사용자는 비활성화 상태의 계정을 활성화시킬 수 있습니다.

역할

사용자 계정에 부여된 시스템 역할입니다. 시스템 역할에 대한 자세한 내용은 시스템 역할 관리하기를 참고하세요.

이메일

사용자 계정의 이메일입니다.

인증 공급자

사용자 계정의 인증 공급자입니다.

사용자 그룹

사용자 계정이 포함되어 있는 사용자 그룹입니다.

최근 수정 일시

최근에 사용자 계정을 수정한 일시입니다.

최근 접속 일시

사용자 계정의 권한으로 최근에 접속한 일시입니다.

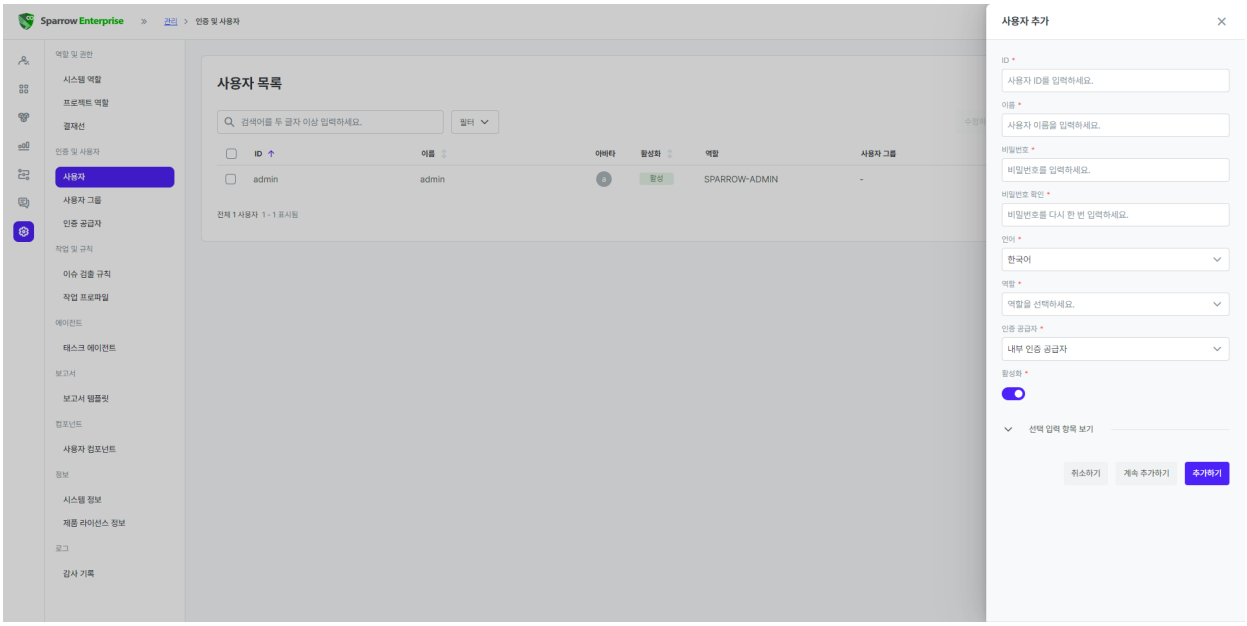
만료 일시

사용자 계정이 만료되는 일시입니다.

사용자 추가하기

시스템의 **인증 및 사용자 관리** 권한이 있는 관리자는 **관리**의 **사용자** 메뉴에서 아래 방법으로 새 사용자를 추가할 수 있습니다.

1. **사용자** 페이지에서 오른쪽 위에 있는 **사용자 추가하기** 버튼을 클릭하세요.



2. 아래의 내용을 참고하여 사용자 정보를 입력하세요.(*는 필수 입력 항목)

3. **추가하기** 버튼을 클릭하세요.

4. 사용자가 성공적으로 추가되면 왼쪽 아래에 성공 메시지가 출력됩니다.

ID*

추가할 사용자 계정의 ID이며 4~32자 사이의 영문, 숫자를 입력할 수 있습니다.

이름*

추가할 사용자 계정의 이름이며 1~50자 사이의 한글, 영문, 공백을 입력할 수 있습니다.

비밀번호*

추가할 사용자 계정의 비밀번호이며 8~32자 사이의 영문, 숫자, 특수 문자의 조합으로 입력해야 합니다. 이 옵션은 **인증 공급자** 옵션에서 **LDAP**을 선택하는 경우 표시되지 않습니다.

> **Tip**: Sparrow Enterprise에서는 Bcrypt, SHA-512를 사용하여 백엔드 데이터에 저장되는 비밀번호를 암호화합니다.

비밀번호 확인*

추가할 사용자 계정의 비밀번호를 다시 입력합니다. 위의 **비밀번호** 항목과 일치해야 합니다. 이 옵션은 **인증 공급자** 옵션에서 **LDAP**을 선택하는 경우 표시되지 않습니다.

언어*

추가할 사용자 계정에 표시할 언어입니다. 한국어, 영어 중에 하나를 선택할 수 있습니다.

> **Tip**: 이미 등록된 사용자의 언어를 변경하려는 경우 목록에서 해당 사용자를 클릭하거나 변경하려는 다수의 사용자를 선택하세요. **수정하기** 버튼을 클릭한 다음 다른 **언어**를 선택하고 **수정하기** 버튼을 클릭하세요.

역할*

추가할 사용자 계정의 시스템 역할이며 적어도 하나 이상의 역할을 선택해야 합니다. 사용자의 역할을 추가하는 방법은 시스템 역할 추가하기를 참고하세요.

인증 공급자

추가할 사용자 계정을 인증할 공급자를 선택하세요. 별도의 외부 인증 공급자를 사용하지 않는 경우 **내부 인증 공급자**를 선택하면 됩니다. **인증 공급자** 탭에서 **LDAP 서버**를 미리 설정한 경우 **LDAP**을 선택하여 인증 정보를 가져올 수 있습니다.

> **Tip**: LDAP 서버를 설정하는 방법은 인증 공급자 관리하기를 참고하세요.

활성화

추가할 사용자 계정의 활성화 상태이며 **활성**이나 **비활성** 중 하나로 표시되며 권한 있는 사용자는 비활성화 상태의 계정을 활성화시킬 수 있습니다.

아바타

추가할 사용자 계정의 아바타를 설정할 수 있습니다. **찾아보기**를 클릭하여 .avif, .gif, .pjp, .jpg, .pjpeg, .jpeg, .pfif, .png, .svgz, .svg, .webp 형식의 이미지 파일을 업로드하세요.

> **Tip**: 이미지 파일의 크기는 5MB 이하여야 합니다.

이메일

추가할 사용자 계정의 이메일 주소를 입력할 수 있습니다.

사용자 그룹

추가할 사용자 계정이 포함될 사용자 그룹을 선택할 수 있습니다.

만료 일시

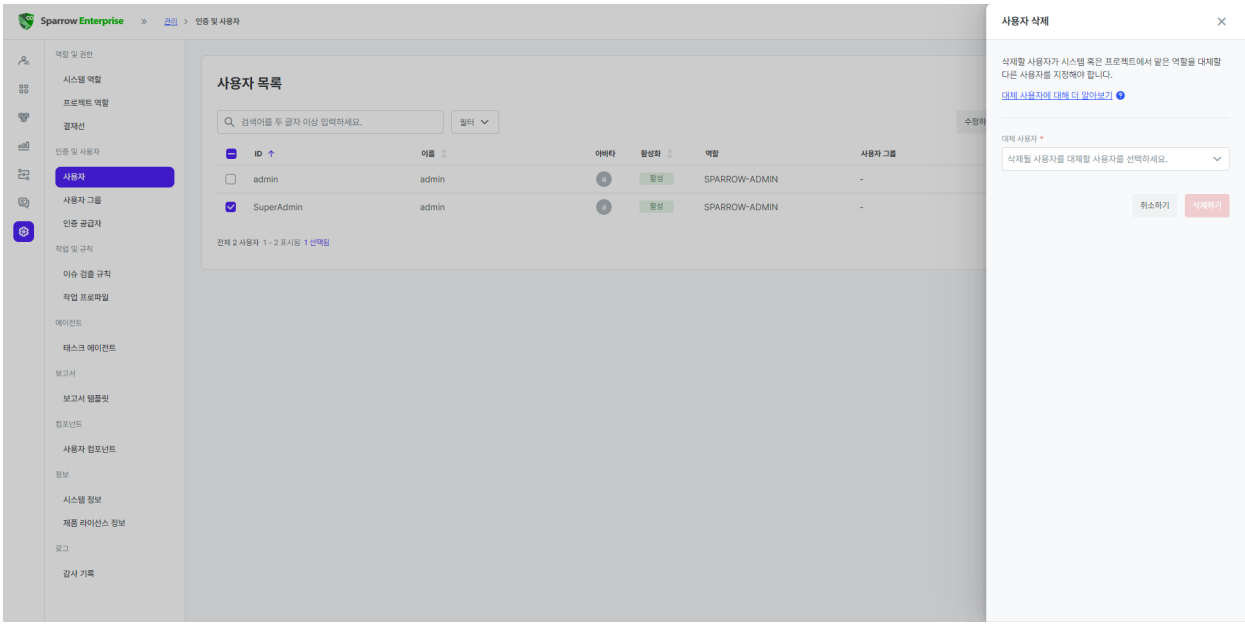
추가할 사용자 계정의 권한을 종료할 일시를 선택할 수 있습니다.

사용자 삭제하기

Sparrow Enterprise에서는 어떤 사용자를 삭제하기 전에 먼저 그 사용자가 시스템 혹은 특정 프로젝트에서 수행하고 있던 역할을 다른 사용자에게 넘겨주도록 강제하고 있습니다. 만약 해당 사용자가 `PROJECT-VIEWER`와 같은 낮은 권한의 역할을 가지고 있더라도 해당 역할을 다른 사용자로 대체해야만 합니다.

1. 사용자 목록에서 삭제할 사용자의 체크박스를 선택하세요.

2. 오른쪽 위에 있는 **삭제하기** 버튼을 클릭하세요.



> **Warning**: 기본 설정된 최고 관리자 계정의 ID인 **admin**은 삭제할 수 없습니다.

3. 아래를 참고하여 **대체 사용자**를 지정하세요.

4. **삭제하기** 버튼을 클릭하세요.

대체 사용자*

삭제할 사용자가 시스템 혹은 프로젝트에서 맡은 역할을 넘겨 받을 다른 사용자입니다. 사용자 목록에 미리 추가된 사용자 중에 하나의 사용자를 선택할 수 있습니다.

대체 사용자는 삭제되는 사용자의 1) 시스템 역할, 2) 프로젝트 역할, 3) 이슈 담당자로 지정된 이슈를 넘겨 받게 됩니다. 그 외에 삭제되는 사용자가 생성한 프로젝트나 수행한 작업 등에는 해당 시점의 데이터가 그대로 저장됩니다.

사용자 그룹 관리하기

시스템의 **인증 및 사용자 관리** 권한이 있는 관리자는 **사용자 그룹** 메뉴에서 등록된 사용자 그룹 목록 및 사용자 그룹 정보를 확인하고 변경할 수 있습니다. 사용자 그룹 목록을 확인하는 방법은 다음과 같습니다.

1. 왼쪽 사이드 바에서 **관리**를 클릭하세요.

2. **사용자** 메뉴에서 **사용자 그룹**을 클릭하세요.

사용자 그룹 목록에 표시되는 각 항목에 대한 설명은 아래의 내용을 참고하세요.

이름

사용자 그룹의 이름입니다.

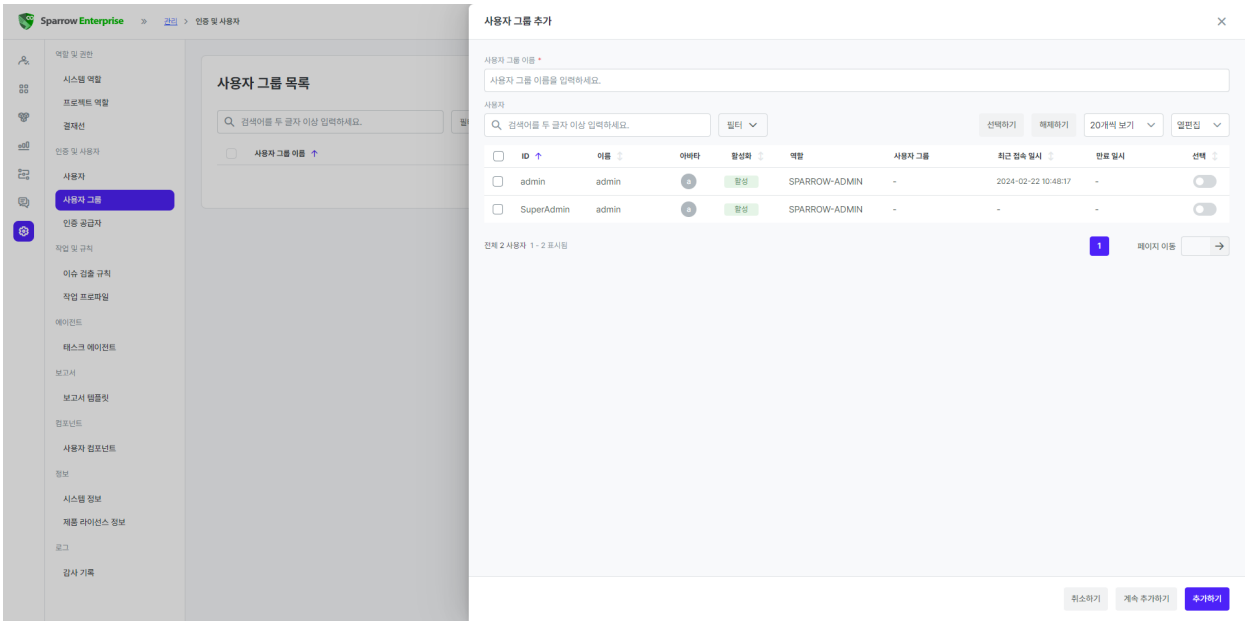
사용자 수

사용자 그룹에 포함된 사용자 계정의 개수입니다.

사용자 그룹 추가하기

시스템의 **인증 및 사용자 관리** 권한이 있는 관리자는 **관리**의 **사용자 그룹**에서 아래 방법으로 새 사용자 그룹을 추가할 수 있습니다.

1. **사용자 그룹** 페이지에서 오른쪽 위에 있는 **사용자 그룹 추가하기** 버튼을 클릭하세요.



2. 아래의 내용을 참고하여 사용자 그룹 정보를 입력하세요.(*는 필수 입력 항목)

3. **추가하기** 버튼을 클릭하세요.

4. 사용자 그룹이 성공적으로 추가되면 왼쪽 아래에 성공 메시지가 출력됩니다.

사용자 그룹 이름*

사용자 그룹의 이름이며 50자 이하의 한글, 영문, 숫자, 특수 문자, 공백을 입력할 수 있습니다.

사용자

새 사용자 그룹에 포함할 사용자의 목록으로 사용자 관리하기에서 확인할 수 있는 사용자가 표시됩니다. 목록의 오른쪽에 있는 **선택** 항목을 활성화하여 사용자를 사용자 그룹에 추가할 수 있습니다. 하나 이상의 사용자를 변경하려는 경우 목록에서 추가할 사용자의 체크박스를 선택하고 **선택하기** 혹은 **해제하기** 버튼을 클릭하여 사용자를 사용자 그룹에 포함하거나 제외할 수 있습니다.

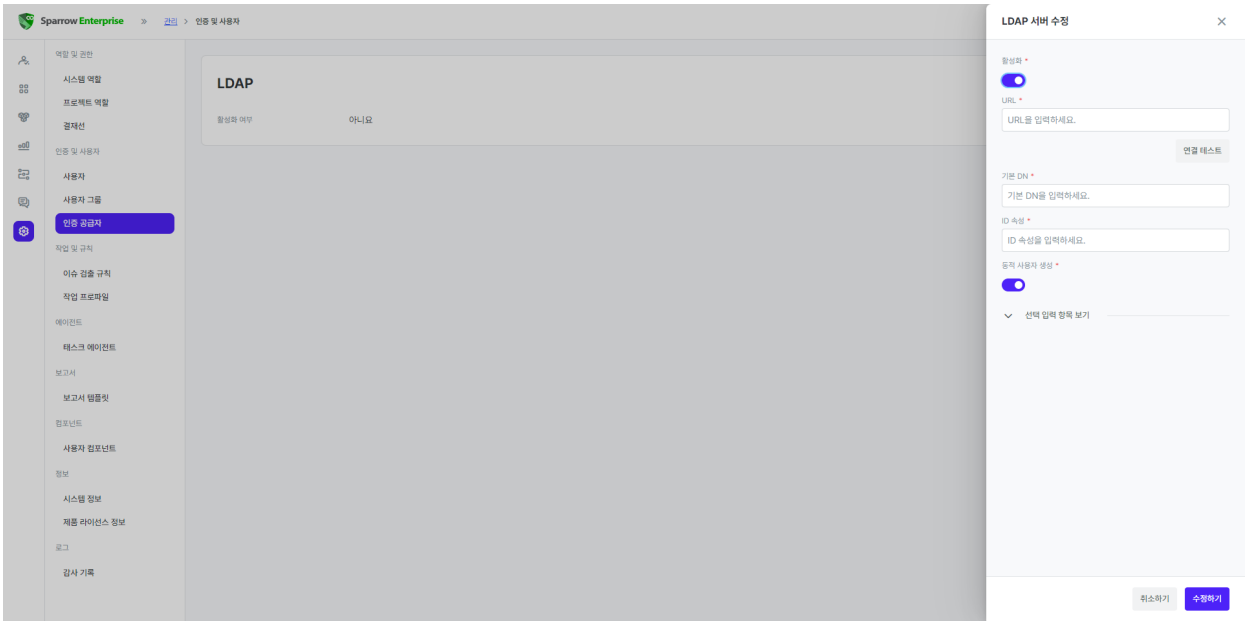
> **Tip**: 사용자를 사용자 그룹에 추가하는 동작으로 인해 선택된 사용자의 다른 정보가 변경되지 않습니다.

인증 공급자 관리하기

기존의 인증 정보를 사용하여 다수의 사용자를 추가하려는 경우 시스템의 **인증 및 사용자 관리** 권한이 있는 관리자는 **인증 공급자** 메뉴에서 등록한 LDAP 서버의 정보를 사용할 수 있습니다. 다음과 같이 LDAP 서버를 등록하세요.

1. **인증 공급자** 페이지에서 오른쪽 위에 있는 **수정하기** 버튼을 클릭하세요.

2. **활성화** 버튼을 토글하여 활성화세요.



3. 아래의 내용을 참고하여 인증 공급자 정보를 입력하세요.(*는 필수 입력 항목)

4. **수정하기** 버튼을 클릭하세요.

5. 인증 공급자가 성공적으로 추가되면 왼쪽 아래에 성공 메시지가 출력됩니다.

활성화*

LDAP 서버 정보의 사용 여부를 의미합니다. 이 정보를 사용자 인증에 사용하려면 이 옵션의 토글 버튼을 활성화해야 합니다.(기본값: 비활성)

> **Tip**: LDAP 서버를 설정한 후 활성화 버튼을 비활성화한 경우에도 이미 저장된 정보는 사라지지 않습니다.

URL*

LDAP 서버의 URL이며 URL 형식으로 입력해야 합니다. URL을 입력한 후 **연결 테스트** 버튼을 클릭하여 LDAP 서버에 정상적으로 연결되는지 확인하세요.

기본 DN*

LDAP 서버의 기본 DN이며 최대 200자까지 입력할 수 있습니다.

ID 속성*

LDAP 인증 공급자를 사용할 때 사용자 ID로 사용할 속성이며 최대 500자까지 입력할 수 있습니다.

동적 사용자 생성*

활성화하는 경우 인증 공급자에 등록된 사용자 정보를 사용하여 Sparrow Enterprise 서버에 등록되지 않은 사용자를 자동으로 추가합니다. 비활성화하는 경우 동적 사용자를 생성하지 않으므로 서버에 등록되지 않은 사용자를 자동으로 추가하지 않습니다.(기본값: 활성)

사용자 DN

LDAP 서버 인증에 사용할 사용자 DN이며 최대 200자까지 입력할 수 있습니다.

비밀번호

사용자 DN과 함께 LDAP 서버 인증에 사용할 비밀번호입니다.

타임아웃

LDAP 서버에 연결을 시도하는 경우 사용하는 제한 시간이며 최대 600을 입력할 수 있습니다.(단위: 초)

이름 속성

사용자 계정의 이름으로 사용될 속성 이름이며 최대 500자까지 입력할 수 있습니다. 값이 존재하지 않는 경우 사용자 계정의 이름을 입력하지 않습니다.

이메일 속성

사용자 계정의 이메일로 사용될 속성 이름이며 최대 500자까지 입력할 수 있습니다. 값이 존재하지 않는 경우 사용자 계정의 메일을 입력하지 않습니다.

작업 및 규칙

이슈 검출 규칙 관리하기

시스템의 **작업 및 규칙 관리** 권한이 있는 관리자는 **이슈 검출 규칙** 메뉴에서 등록된 이슈 검출 규칙을 확인하고 사용 여부를 결정할 수 있습니다. 이슈 검출 규칙 목록을 확인하는 방법은 다음과 같습니다.

1. 왼쪽 사이드 바에서 **관리**를 클릭하세요.
2. **이슈** 메뉴에서 **이슈 검출 규칙**을 클릭하세요.

> **Tip**: 이슈 검출 규칙 목록의 위에 표시되는 알림 메시지에서 이슈 검출 규칙이 업데이트된 시각을 확인할 수 있습니다.

이슈 검출 규칙 목록에 표시되는 각 항목에 대한 설명은 아래의 내용을 참고하세요.

유형

이슈 검출 규칙을 적용하는 작업을 기준으로 이슈 검출 규칙의 유형을 구분합니다. 이 옵션은 작업에 따라 **소스코드**, **웹 취약점**, **컴포넌트**, **자가 방어**로 나눠집니다.

이슈 검출 규칙 제공자

이슈 검출 규칙을 생성한 주체를 표시합니다. **기본**으로 표시된 경우 Sparrow Enterprise에서 기본으로 제공하는 이슈 검출 규칙을 의미합니다. 사용자가 직접 이슈 검출 규칙을 추가한 경우 **사용자 정의**로 표시됩니다. 사용자 지정 이슈 검출 규칙을 추가하는 방법은 사용자 지정 이슈 검출 규칙 추가하기를 참고하세요.

언어

이슈 검출 규칙이 지원하는 언어를 표시합니다.

> **Tip**: 웹 취약점 및 컴포넌트 관련 이슈 검출 규칙의 경우 언어가 **공통**으로 표시됩니다.

위험도

이슈 검출 규칙의 위험도이며 **매우 높음**, **높음**, **보통**, **낮음**, **매우 낮음**이라는 5단계로 구분합니다.

규칙 이름

이슈 검출 규칙의 이름입니다.

레퍼런스

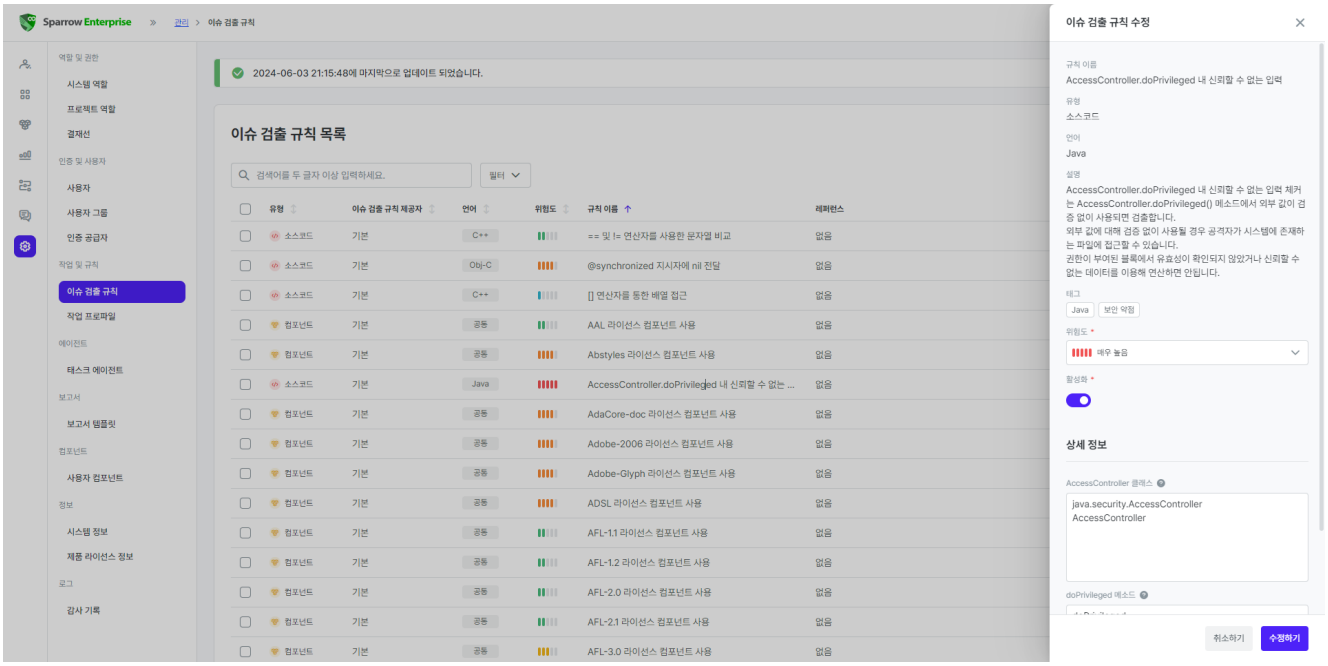
이슈 검출 규칙이 포함되어 있는 국내외 소스코드 취약점 혹은 품질 관련 기준입니다. 레퍼런스에 해당하는 이슈 검출 규칙의 경우 다음과 같은 레퍼런스 중 하나 이상이 표시될 수 있습니다. **.NET framework design guideline**, **Code conventions for the Java Programming Language(Oracle)**, **CWE 658 4.14**, **CWE 658 4.7**, **CWE 659 4.14**, **CWE 659 4.7**, **CWE 660 4.14**, **CWE 660 4.7**, **JavaScript 시큐어코딩 가이드 2022**, **MISRA-C 2004**, **MISRA-C 2012**, **MISRA-C 2012 Amendment 2**, **MISRA-C 2012 Amendment 3**, **MISRA-C++ 2008**, **OWASP 2017**, **OWASP 2021**, **Python 시큐어코딩 가이드 2022**, **Rust ANSSI guide v1.0**, **무기체계 소프트웨어 보안약점 점검 목록**, **방위사업청 코딩규칙**, **소프트웨어 보안약점 진단가이드 2021**, **주요정보통신기반시설 취약점 분석·평가 기준**.

활성화

이슈 검출 규칙의 활성화 상태이며 **활성**, **비활성** 중 하나로 표시됩니다.

이슈 검출 규칙 수정하기

이슈 검출 규칙은 이미 정해진 보안 또는 품질 관련 지침이므로 주요 사항을 변경할 수는 없습니다. 하지만 이슈 검출 규칙의 **상세 정보**가 포함되어 있는 경우 허용하는 범위 안에서 세부적인 규칙을 조정할 수 있습니다. 자세한 내용은 다음을 참고하세요.



1. **이슈 검출 규칙** 목록에서 항목을 클릭하세요.

2. 슬라이드에서 아래를 참고하여 수정할 내용을 선택하거나 입력하세요.

3. **수정하기** 버튼을 클릭하세요.

위험도

이슈 검출 규칙의 **위험도**입니다. 드롭다운 버튼을 클릭하여 **매우 높음**, **높음**, **보통**, **낮음**, **매우 낮음** 중에서 변경하려는 위험도를 선택할 수 있습니다.

> **Warning**: 기본적으로 **위험도**는 국내외 레퍼런스를 기준으로 구분되어 있습니다. 위험도를 조정하면 검출된 이슈가 얼마나 위험한지에 대해 정확한 판단이 어려울 수 있다는 점에 주의하세요.

활성화

규칙을 분석 작업에 적용할 것인지 결정합니다. **활성화** 버튼을 비활성화하면 해당 규칙을 모든 분석에 사용하지 않게 됩니다. 버튼을 활성화하면 다시 해당 규칙을 적용하여 작업을 실행합니다.

> **Tip**: 특정 프로젝트에서 특정 이슈 검출 규칙을 적용하여 작업을 시작하려는 경우 작업 프로파일 관리하기를 참고하세요.

상세 정보

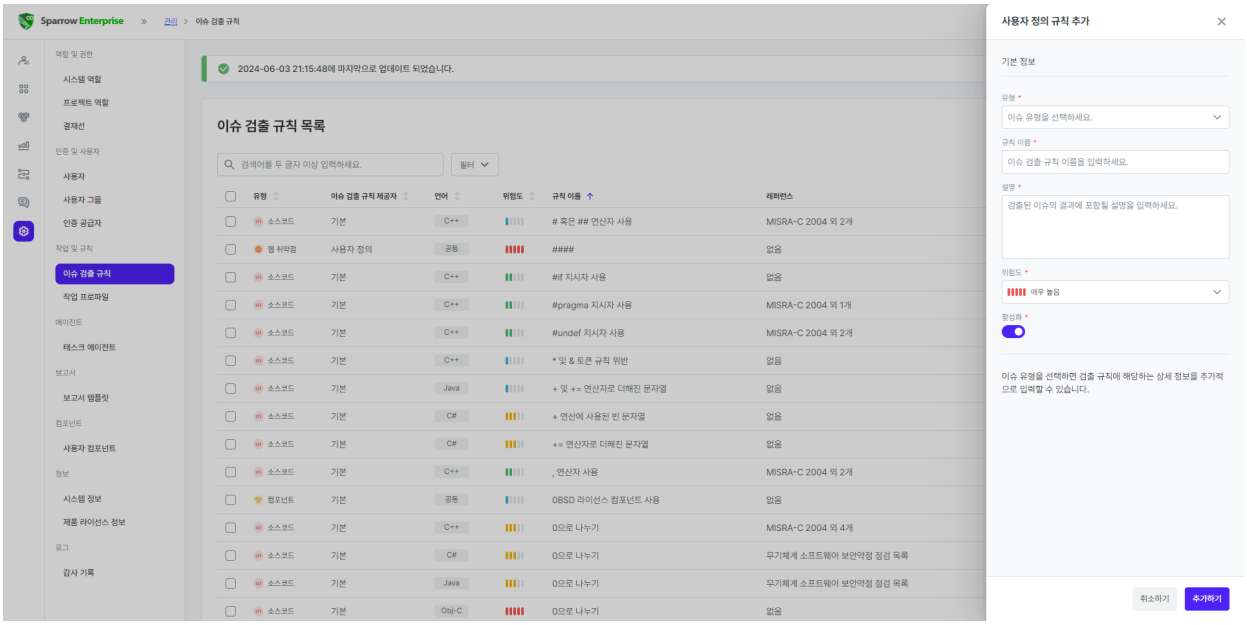
세부적인 **검출 규칙**이나 **제외 규칙**을 표시합니다. 검출 규칙마다 여기에 표시되는 옵션의 내용이 다릅니다. 권한이 있는 사용자는 이 옵션을 조정하여 규칙이 허용하는 조건 안에서 검출 규칙이나 제외 규칙을 수정할 수 있습니다.

사용자 지정 이슈 검출 규칙 추가하기

시스템의 **작업 및 규칙 관리** 권한이 있는 관리자는 **사용자 지정 이슈 검출 규칙**을 추가할 수 있습니다. 자세한 내용은 다음을 참고하세요.

> **Tip**: 현재 **웹 취약점**에 대한 이슈 검출 규칙만 사용자가 추가할 수 있습니다.

1. **이슈 검출 규칙** 페이지에서 오른쪽 위에 있는 **사용자 정의 규칙 추가하기** 버튼을 클릭하세요.



2. 아래의 내용을 참고하여 이슈 검출 규칙의 정보를 입력하세요.(*는 필수 입력 항목)

3. **추가하기** 버튼을 클릭하세요.

4. 사용자 정의 이슈 검출 규칙이 성공적으로 추가되면 왼쪽 아래에 성공 메시지가 출력됩니다.

✓ 기본 정보

유형*

추가할 이슈 검출 규칙이 Sparrow Enterprise가 지원하는 분석 중 어디에 해당하는지를 구분합니다. 현재 **웹 취약점**만 선택할 수 있습니다.

규칙 이름*

추가할 이슈 검출 규칙의 이름이며 최대 50자까지 입력할 수 있습니다.

설명*

추가할 이슈 검출 규칙에 대한 설명이며 최대 2000자까지 입력할 수 있습니다. 여기에 입력한 내용은 이 규칙으로 검출된 이슈의 결과인 이슈 상세 정보 페이지에 표시됩니다.

위험도*

추가할 이슈 검출 규칙의 위험도이며 **매우 높음**, **높음**, **보통**, **낮음**, **매우 낮음**이라는 5단계로 구분합니다.(기본값: 매우 높음)

활성화 여부*

추가할 이슈 검출 규칙의 사용 여부를 의미합니다. 이 규칙을 분석에 사용하려면 이 옵션의 토글 버튼을 활성화해야 합니다.(기본값: 활성)

✓ 상세 정보

침투 공격 대상

웹 취약점 분석 과정에서 공격 문자열을 배치할 위치입니다. **쿼리 문자열**, **폼 데이터**, **쿠키**, **HTTP 헤더**, **URL 경로** 중에서 하나 이상의 대상을 선택할 수 있습니다.

RPC 공격 대상

웹 취약점 공격 문자열을 삽입할 데이터 형식입니다. **multipart/form-data**, **XML**, **JSON**, **구글 웹 툴킷**, **DWR** 중에서 하나 이상의 대상을 선택할 수 있습니다.

공격 문자열

웹 취약점 공격 수행 도중 서버로 전송하는 HTTP 요청 내부에 포함시킬 수 있는 문자열입니다. 하나 이상의 문자열을 엔터와 쉼표(,)로 구분하여 입력할 수 있습니다.

검출 정규식

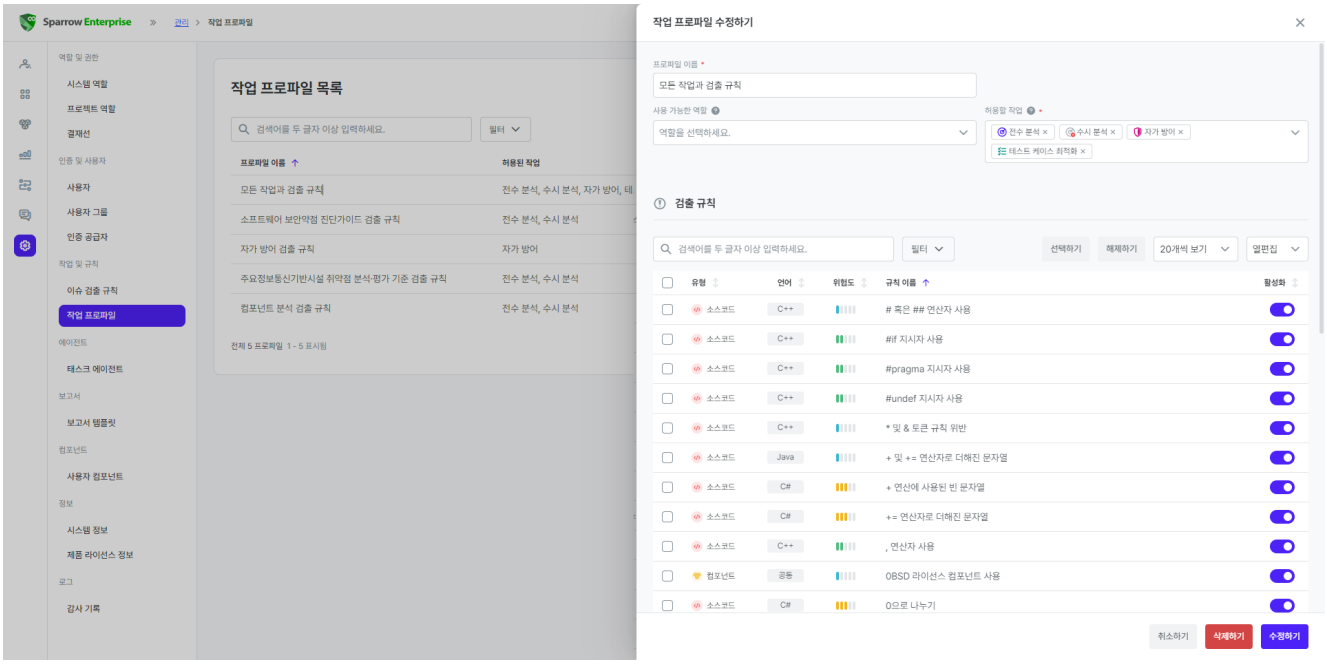
웹 취약점 공격에 대한 서버의 HTTP 응답에서 취약점을 검출하기 위해 사용하는 정규식입니다. 하나 이상의 정규식을 엔터와 쉼표(,)로 구분하여 입력할 수 있습니다.

제외 정규식

웹 취약점 검출에서 제외할 대상을 정의하기 위해 사용하는 정규식입니다. 하나 이상의 정규식을 엔터와 쉼표(,)로 구분하여 입력할 수 있습니다.

작업 프로파일 관리하기

프로젝트에서 **분석**, **자가 방어**, **테스트 케이스 최적화** 작업을 수행하는 경우 **작업 프로파일**을 선택해야 합니다. 선택한 **작업 프로파일**을 통해 작업에 사용할 이슈 검출 규칙 및 작업 옵션을 결정합니다.



만약 특정 레퍼런스에 해당하는 이슈만을 검출하려면 1) 먼저 작업 프로파일 추가하기를 참고하여 해당 레퍼런스의 작업 프로파일을 생성하세요. 여기서 추가한 작업 프로파일은 모든 프로젝트에 공통적으로 적용되지만 작업 유형 및 프로젝트 역할을 통해 사용할 수 있는 작업과 사용자를 조정할 수 있습니다. 그런 다음,

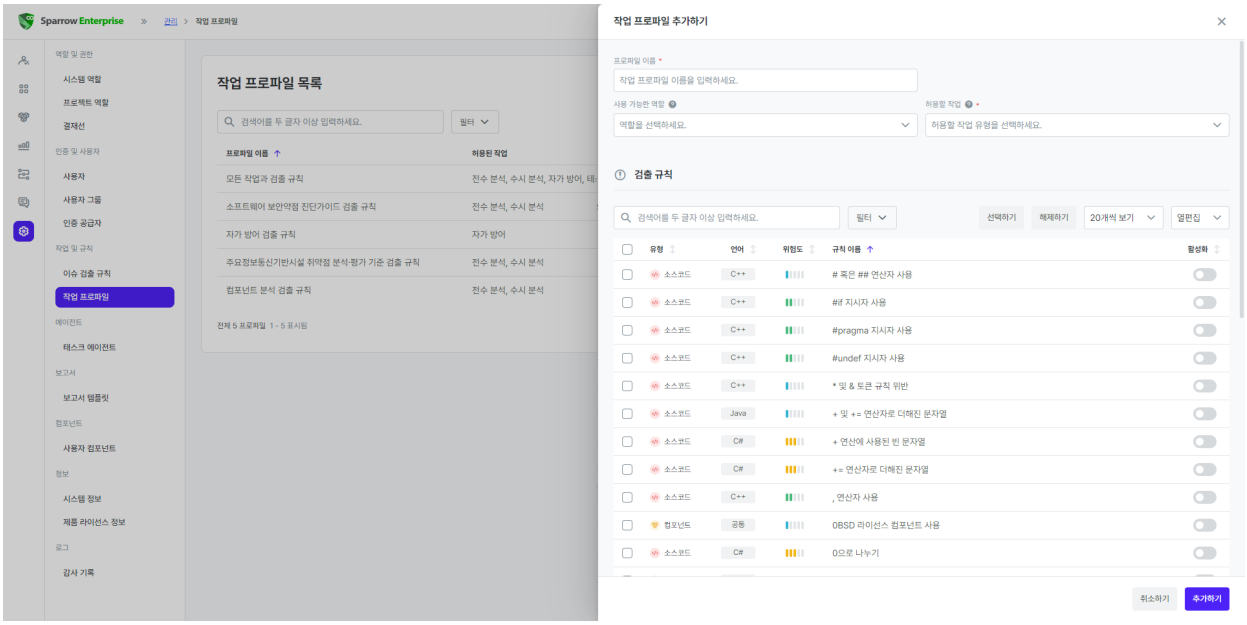
2) **새 작업 시작하기** 슬라이드에서 작업 프로파일을 선택하세요. 앞서 언급한 대로 작업 유형 및 프로젝트 역할에 따라 사용할 수 있는 작업 프로파일이 표시됩니다. 또한 작업 프로파일에 특정 레퍼런스로 매핑된 규칙이 모두 포함되어 있는 경우, 해당 레퍼런스의 이름을 작업 프로파일에서 바로 확인하실 수 있습니다.

특히, **전수 분석**과 **수시 분석**에서 사용할 수 있는 작업 프로파일을 구분할 수 있도록 설계되었습니다. 따라서, 관리자가 전수 분석인 경우 특정 작업 프로파일만 사용해서 분석하도록 설정함으로써 전수 분석의 분석 결과를 정확하게 관리할 수 있습니다.

작업 프로파일 추가하기

시스템의 **작업 및 규칙 관리** 권한이 있는 관리자는 **작업 프로파일** 페이지에서 작업 프로파일을 추가할 수 있습니다. 작업 프로파일을 만드는 방법은 다음과 같습니다.

1. **작업 프로파일** 페이지에서 오른쪽 위에 있는 **프로파일 추가하기** 버튼을 클릭하세요.



2. **작업 프로파일 이름**을 입력하세요.
3. 아래의 내용을 참고하여 **사용 가능한 역할**과 **허용할 작업**을 선택하세요.(*는 필수 입력 항목)
4. 검색이나 필터를 사용하여 작업 프로파일에서 **사용할 이슈 검출 규칙**을 선택하세요.

> **Tip**: 작업 프로파일에서 선택하지 않은 이슈 검출 규칙은 작업에 사용되지 않습니다. 즉, 규칙을 선택하지 않으면 해당 규칙은 분석, 방어, 최적화에 적용되지 않습니다.

5. **추가하기** 버튼을 클릭하세요.
6. 작업 프로파일이 성공적으로 추가되면 왼쪽 아래에 성공 메시지가 출력됩니다.

✓ 기본 정보

작업 프로파일 이름*

추가할 작업 프로파일의 이름이며 50자 이하의 한글, 영문, 숫자, 특수 문자, 공백을 입력할 수 있습니다.

사용 가능한 역할

추가할 작업 프로파일을 사용할 수 있는 프로젝트 역할을 지정합니다. 프로젝트 역할 관리하기에서 설정한 역할 중 하나 이상을 선택할 수 있습니다. 이 옵션을 입력하면 선택한 프로젝트 역할의 구성원만 추가할 작업 프로파일을 사용하게 됩니다. 이 옵션을 입력하지 않으면 모든 프로젝트 구성원이 해당 작업 프로파일을 사용할 수 있습니다.

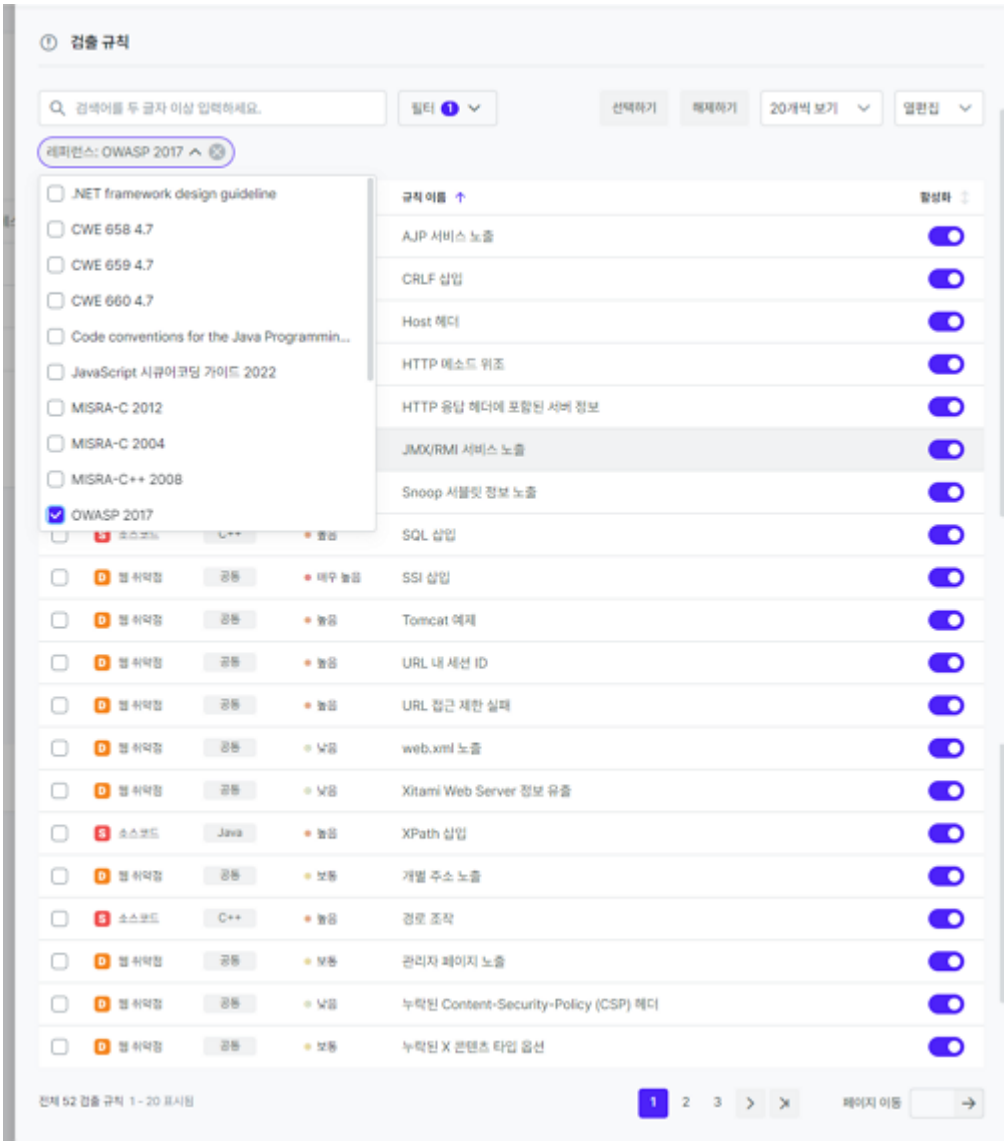
허용할 작업*

추가할 작업 프로파일을 사용할 수 있는 작업 유형을 의미합니다. 이 옵션에서 선택한 작업에만 해당 작업 프로파일을 적용할 수 있습니다. 라이선스에 따라 **전수 분석**, **수시 분석**, **자가 방어**, **테스트 케이스 최적화** 중 하나 이상을 선택할 수 있습니다.

✓ 검출 규칙*

추가할 작업 프로파일에서 사용할 이슈 검출 규칙의 목록입니다. 목록에서 작업 프로파일에 추가할 규칙의 **선택** 항목을 활성화하세요. 목록에 표시된 정보에 대한 자세한 내용은 이슈 검출 규칙 관리하기를 참고하세요.

특정 레퍼런스에 해당하는 이슈 검출 규칙만을 작업 프로파일에서 활성화하려면 **레퍼런스**로 목록을 필터링하고 표시된 목록을 전체 선택한 다음, 목록의 오른쪽 위에 있는 **선택하기** 버튼을 클릭하세요.



✓ 작업 옵션

소스코드 분석

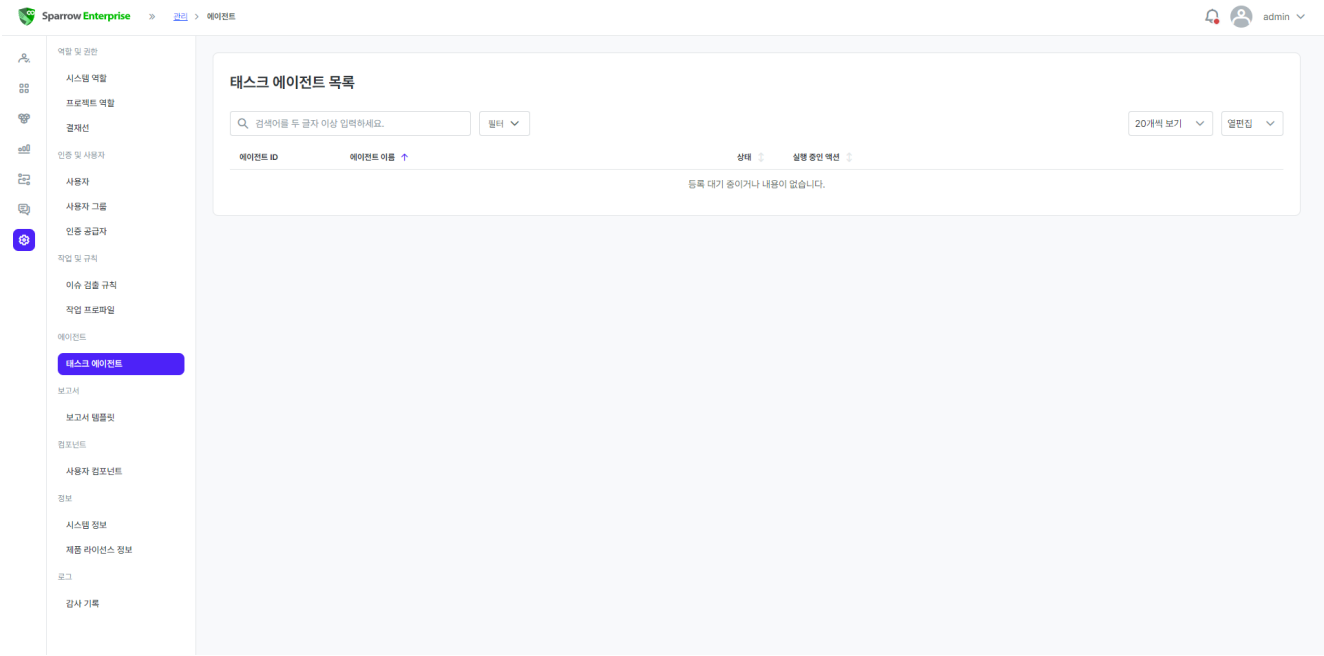
분석 제외 경로

분석 제외 경로는 분석에 포함하지 않을 폴더나 파일의 경로를 의미합니다. 즉, 이 옵션에 값을 입력하면 추가할 작업 프로파일로 분석을 수행할 때 특정 경로를 분석하지 않도록 설정할 수 있습니다. 필요한 경우 하나 이상의 경로를 입력하고 엔터로 구분할 수 있습니다.

분석 제외 경로에 입력한 경로는 **소스코드 분석**에만 적용된다는 점에 주의하세요. 즉, 이 경로에 해당하는 **컴포넌트 분석**의 자산과 이슈는 분석 결과에 그대로 표시됩니다.

에이전트

태스크 에이전트 관리하기



다음과 같은 방법으로 등록된 Sparrow Enterprise의 태스크 에이전트 정보를 확인할 수 있습니다.

> **Tip**: 태스크 에이전트를 설치하는 방법은 태스크 에이전트 설치하기를 참고하세요.

1. 왼쪽 사이드 바에서 **관리**를 클릭하세요.
2. **에이전트** 메뉴에서 **태스크 에이전트**를 클릭하세요.

태스크 에이전트 목록에 표시된 항목에 대한 설명은 아래의 내용을 참고하세요.

에이전트 ID

태스크 에이전트의 ID입니다. 고유한 번호로 부여되며 변경할 수 없습니다.

에이전트 이름

태스크 에이전트의 이름이며 64자까지 표시됩니다. 에이전트를 설치할 때 설정할 수 있으며 변경할 수 없습니다.

상태

현재 에이전트의 상태이며 **사용 가능**과 **사용 중** 중 하나로 표시됩니다. **사용 가능**은 태스크 에이전트가 정상적으로 연결되었으며 액션을 실행하고 있지 않은 상태입니다. **사용 중**은 태스크 에이전트가 정상적으로 연결되었지만 다른 액션을 실행하기 위해 특정 태스크에 할당되었기 때문에 추가로 액션을 실행할 수 없는 상태를 의미합니다.

실행 중인 액션

사용 중인 에이전트가 현재 액션을 실행하고 있는 경우 해당 액션을 표시합니다. 액션이 빠르게 실행되고 종료된 경우 표시되지 않을 수 있습니다.

보고서

보고서 템플릿 관리하기

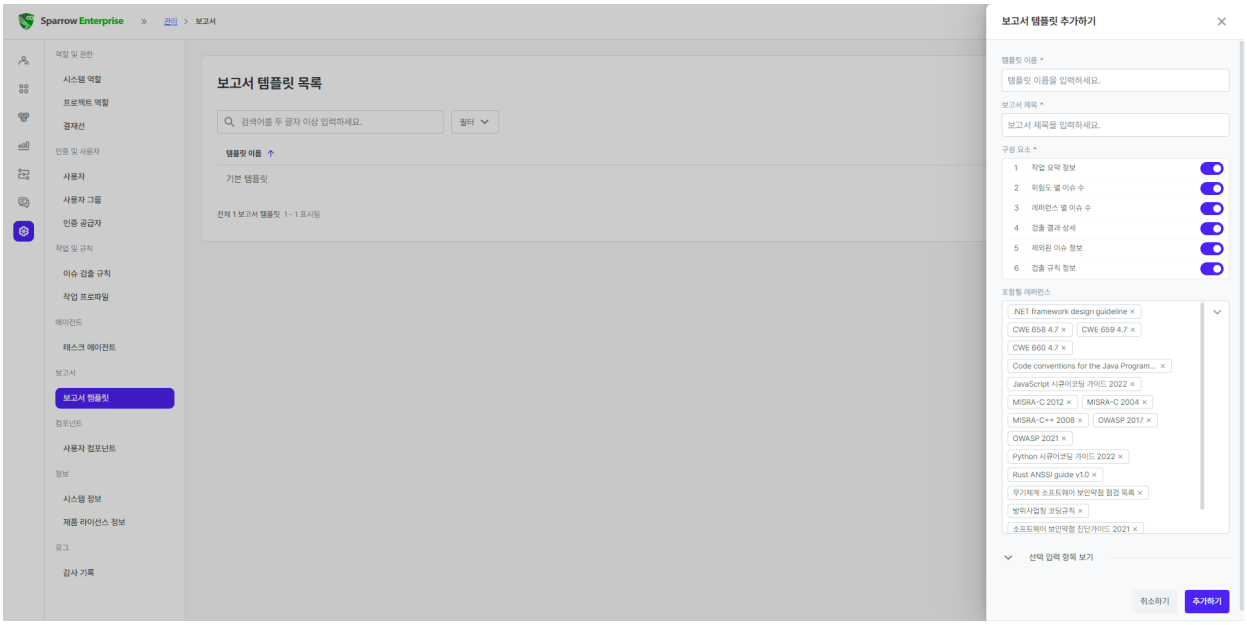
보고서 템플릿 메뉴에서는 프로젝트에서 수행한 소스코드 분석, 컴포넌트 분석, 웹 취약점 분석, 자가 방어에 대한 작업 보고서를 출력할 때 사용할 템플릿을 만들 수 있습니다. 또한 추가한 템플릿을 수정할 수도 있습니다. 단, 보고서 템플릿 목록에 있는 **기본 템플릿**은 사용자가 수정하거나 삭제할 수 없습니다. 보고서 템플릿을 확인하기 위해서는 다음과 같은 방법을 참고하세요.

1. 왼쪽 사이드 바에서 **관리**를 클릭하세요.
2. **정보** 메뉴에서 **보고서 템플릿**을 클릭하세요.

보고서 템플릿 추가하기

시스템의 **보고서 관리** 권한이 있는 관리자는 **관리** 메뉴의 **보고서 템플릿**에서 이런 방법으로 새 보고서 템플릿을 추가할 수 있습니다.

1. **보고서 템플릿** 페이지에서 오른쪽 위에 있는 **보고서 템플릿 추가하기** 버튼을 클릭하세요.



2. 아래의 내용을 참고하여 보고서 템플릿 정보를 입력하세요.(*는 필수 입력 항목)
3. **추가하기** 버튼을 클릭하세요.
4. 보고서 템플릿이 성공적으로 추가되면 왼쪽 아래에 성공 메시지가 출력됩니다.

템플릿 이름*

보고서 템플릿의 이름이며 50자 이하의 한글, 영문, 숫자, 특수 문자, 공백을 입력할 수 있습니다.

보고서 제목*

보고서 템플릿으로 출력할 보고서의 제목이며 50자 이하의 모든 문자를 입력할 수 있습니다.(기본값: `Sparrow 보고서`)

> **Tip**: 보고서 제목은 출력할 보고서의 첫 페이지 및 페이지 헤더에 표시됩니다.

구성 요소

보고서 템플릿에 포함될 요소입니다. **작업 요약 정보**, **위험도별 이슈 수**, **레퍼런스별 이슈 수**, **검출 결과 상세**, **제외된 이슈 정보**, **검출 규칙 정보**로 구성되어 있습니다.(기본값: 모두 선택)

구성 요소 목록의 오른쪽에 있는 토글 버튼을 선택하여 해당 항목을 보고서 템플릿에 포함하거나 템플릿에서 제외할 수 있습니다. 또한 구성 요소 목록의 왼쪽에 있는 선택 버튼을 클릭한 채로 드래그하여 항목의 순서를 변경할 수 있습니다.

포함될 레퍼런스

보고서에 출력할 레퍼런스의 목록이며 **구성 요소** 중 **레퍼런스별 이슈 수**에 표시할 레퍼런스를 선택할 수 있습니다. 그러면 작업에서 검출된 이슈를 해당 레퍼런스에 비교하여 레퍼런스 기준에서 벗어나는 이슈의 개수를 확인할 수 있습니다.(기본값: 모두 선택)

만약 선택한 레퍼런스에 해당하는 이슈가 작업에서 검출되지 않은 경우 해당 레퍼런스는 작업 보고서에 표시되지 않습니다.

보고서 로고

보고서의 첫 페이지에 표시할 로고 파일을 선택할 수 있습니다. 이미지 파일은 5MB 이하의 .jpg, .jpeg, .png 형식이어야 합니다.(기본값: Sparrow Enterprise 로고)

정보

시스템 정보 확인하기

시스템의 **시스템 관리** 권한이 있는 관리자는 다음과 같은 방법으로 등록된 Sparrow Enterprise의 시스템 정보를 확인할 수 있습니다.

1. 왼쪽 사이드 바에서 **관리**를 클릭하세요.
2. **정보** 메뉴에서 **시스템 정보**를 클릭하세요.

시스템 정보의 각 항목에 대한 설명은 아래의 내용을 참고하세요.

✓ 제품 정보

제품 정보에는 **제품명**을 비롯하여 **버전**과 **설치 정보**가 표시됩니다. **버전**에서는 **제품 버전**, **모듈별 버전**, **빌드 일시**, **빌드 ID**에 대한 정보를 확인할 수 있습니다. **설치 정보**에는 **프로그램 경로**, **DB 경로**, **DB 드라이버**, **DB 버전**, **DB URL**이 포함됩니다.

✓ 서버 정보

서버 정보에는 **운영 체제**, **CPU**, **총 메모리**, **사용 가능한 메모리**, **총 디스크**, **사용 가능한 디스크** 정보가 표시됩니다.

✓ 사용 현황

사용 현황에는 Sparrow Enterprise를 사용하는 **사용자 수**, **전체 프로젝트 수**, **전체 분석 수**, **전체 테스트 수**, **전체 이슈 검출 규칙 수**가 표시됩니다.

제품 라이선스 정보 확인하기

시스템의 **시스템 관리** 권한이 있는 관리자는 다음과 같은 방법으로 Sparrow Enterprise에 등록된 제품 라이선스 정보를 확인할 수 있습니다.

1. 왼쪽 사이드 바에서 **관리**를 클릭하세요.
2. **정보** 메뉴에서 **제품 라이선스**를 클릭하세요.

제품 라이선스 정보의 각 항목에 대한 설명은 아래의 내용을 참고하세요.

✓ 제품 라이선스 정보

시스템 ID

시스템을 구분하기 위한 고유의 ID이며 Sparrow Enterprise의 제품 라이선스를 발급하기 위해 사용됩니다.

> **Tip**: 제품 라이선스를 갱신하려면 **시스템 ID**를 복사하여 스패로우 엔지니어에게 전달하세요. 엔지니어에게서 제품 라이선스를 받은 다음, 오른쪽 위에 있는 **갱신하기** 버튼을 클릭하여 제품 라이선스를 입력하고 **갱신하기**를 클릭하면 Sparrow Enterprise의 제품 라이선스가 변경됩니다.

시작일

Sparrow Enterprise의 제품 라이선스가 시작된 날짜입니다.

사용 만료일

Sparrow Enterprise의 제품 라이선스가 만료되는 날짜입니다.

남은 사용일

Sparrow Enterprise의 제품 라이선스를 사용할 수 있는 기간을 일로 표시합니다.

최대 등록 사용자 수

Sparrow Enterprise에 등록할 수 있는 전체 사용자 계정의 개수입니다.

남은 사용자 수

Sparrow Enterprise에 앞으로 등록할 수 있는 사용자 계정의 개수입니다.

활성화된 도구

Sparrow Enterprise에 설치된 제품을 표시합니다. **sast**,**saqt**,**dast**,**rasp**,**sca**,**tso**와 같이 총 6개의 제품이 표시될 수 있습니다.

✓ SAST

최대 라인 수

Sparrow SAST/SAQT에서 분석할 수 있는 소스코드 라인의 개수를 표시합니다.

✓ SCA

최대 누적 분석 크기

Sparrow SCA에서는 제품 라이선스를 통해 분석할 수 있는 대상 파일의 누적 크기를 제한하며 여기에 지정된 용량을 표시합니다.

현재 누적 분석 크기

Sparrow SCA에서 현재까지 분석한 대상 파일의 누적 크기를 표시합니다.

남은 누적 분석 크기

Sparrow SCA에서 앞으로 분석할 수 있는 대상 파일의 크기를 표시합니다.

✓ DAST

최대 동시 분석 수

Sparrow DAST에서는 제품 라이선스를 통해 같은 시각에 분석할 수 있는 대상 웹 애플리케이션의 개수를 제한하며 여기에 지정된 개수를 표시합니다.

현재 동시 분석 수

Sparrow DAST에서 현재 분석하고 있는 웹 애플리케이션의 개수를 표시합니다.

남은 동시 분석 수

Sparrow DAST에서 현재 추가로 분석할 수 있는 웹 애플리케이션의 개수를 표시합니다.

✓ RASP

최대 동시 방어 수

Sparrow RASP에서는 제품 라이선스를 통해 같은 시각에 방어할 수 있는 대상 웹 애플리케이션의 개수를 제한하며 여기에 지정된 개수를 표시합니다.

현재 동시 방어 수

Sparrow RASP에서 현재 방어하고 있는 웹 애플리케이션의 개수를 표시합니다.

남은 동시 방어 수

Sparrow RASP에서 현재 추가로 방어할 수 있는 웹 애플리케이션의 개수를 표시합니다.

로그

감사 기록 확인하기

시스템의 **시스템 관리** 권한이 있는 관리자는 다음과 같은 방법으로 등록된 Sparrow Enterprise의 감사 기록을 확인할 수 있습니다.

1. 왼쪽 사이드 바에서 **관리**를 클릭하세요.
2. **로그** 메뉴에서 **감사 기록**을 클릭하세요.

감사 기록의 각 항목에 대한 설명은 아래의 내용을 참고하세요.

사건 유형

Sparrow Enterprise에서 발생한 이벤트의 유형을 **감사 시작**, **감사 종료**, **서비스 시작**, **서비스 종료**, **로그인**, **로그아웃**, **설정 변경**, **보안 기능 수행**, **분석 시작**, **분석 종료**로 분류합니다.

사건 결과

Sparrow Enterprise에서 발생한 이벤트의 결과를 **성공** 혹은 **실패**로 분류합니다.

주체

Sparrow Enterprise에서 발생한 이벤트의 주체를 사용자 정보의 **아바타**로 표시합니다.

발생 IP

Sparrow Enterprise에서 이벤트가 발생한 IP를 표시합니다.

발생 일시

Sparrow Enterprise에서 이벤트가 발생한 일시를 표시합니다.

사건 내역

Sparrow Enterprise에서 이벤트가 발생할 때 서비스가 수행한 구체적인 내용을 문장으로 설명하거나 해당하는 HTTP 요청을 표시합니다.

로그아웃

Sparrow Enterprise에서 로그아웃하려면 Sparrow Enterprise 웹 페이지의 오른쪽 위에 있는 **사용자 이름**을 클릭하고 **로그아웃** 버튼을 클릭하세요.

1. 기본 메뉴의 오른쪽 끝에서 **사용자 이름**을 클릭하세요.

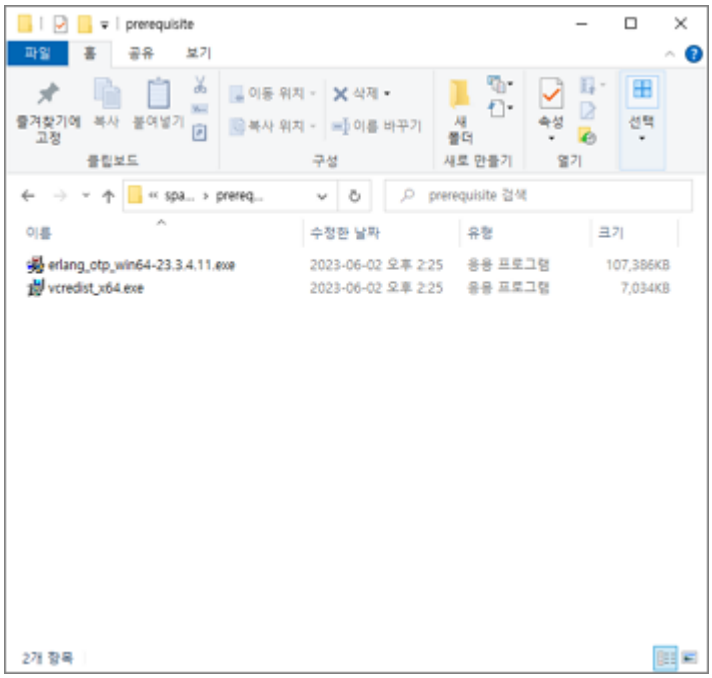
2. **로그아웃** 버튼을 클릭하세요.

FAQ

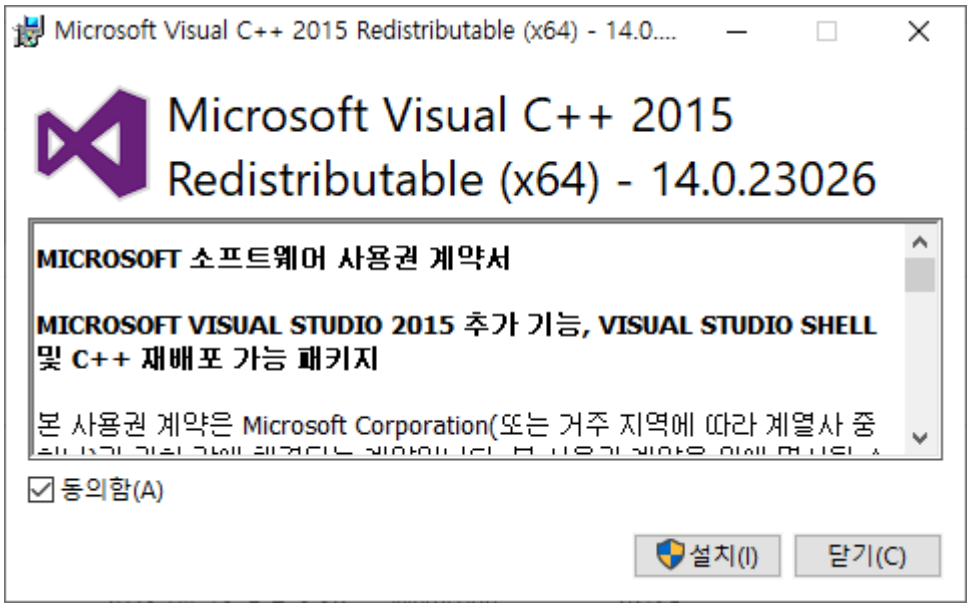
❓ Windows 환경에서 데이터베이스가 정상적으로 초기화되지 않거나 구동되지 않습니다.

Sparrow Enterprise에 포함된 PostgreSQL Windows 버전의 경우 **Microsoft Visual C++ 2015 Redistributable**을 설치해야 합니다. Sparrow Enterprise 서버를 구동하기 전에 아래의 방법을 참고하여 패키지에 포함된 Microsoft Visual C++ 2015 Redistributable을 사전에 설치해주세요.

1. **{Sparrow Enterprise 서버 설치 디렉토리}**에 있는 **prerequisite** 디렉토리로 이동하세요.



2. vcredist_x64.exe(64비트 환경) 혹은 vcredist_x86.exe(32비트 환경)를 실행하여 **Microsoft Visual C++ 2015 Redistributable**을 설치하세요.



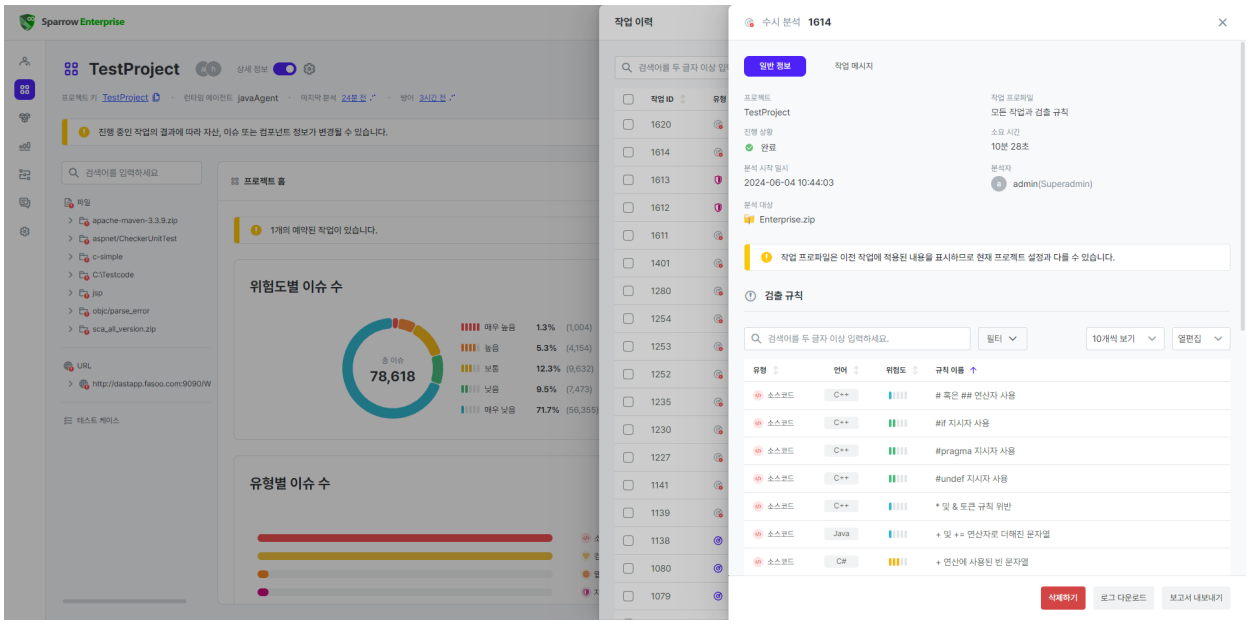
3. 설치가 완료된 이후 Sparrow Enterprise 서버를 다시 시작하세요.

❓ 분석을 실행한 후에 분석이 제대로 시작되었는지 확인하고 싶습니다.

분석이 정상적으로 수행 중인지를 확인하는 방법은 로그를 확인하는 것이 가장 정확합니다. 로그를 가장 간단히 확인할 수 있는 방법은 다음과 같습니다.

웹 서버에서 분석 로그 다운로드하기

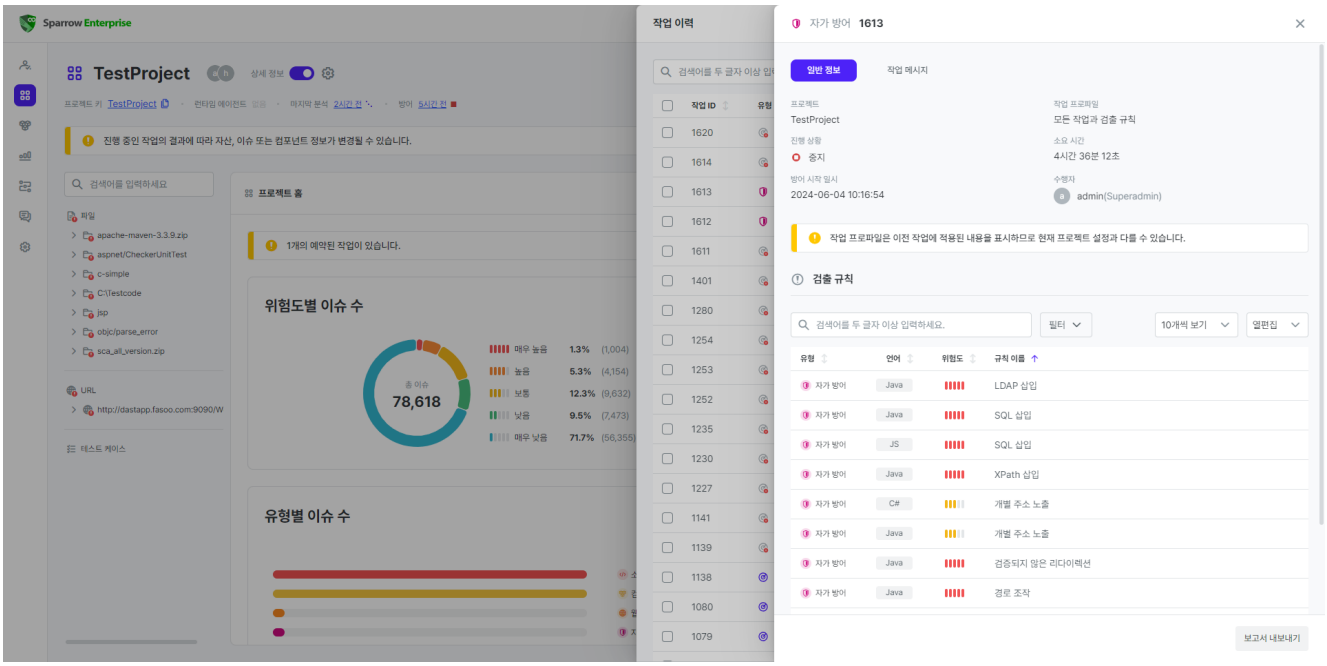
1. 프로젝트의 **작업 이력**에서 확인하려는 분석을 클릭하세요.
2. 그러면 해당 분석 슬라이드로 이동합니다.



3. 아래쪽에 있는 **로그 다운로드** 버튼을 클릭하세요.

다운로드한 **analysis-{분석ID}.log** 파일을 열면 분석이 진행된 시간이 표시됩니다. 수행한 분석을 더 상세히 확인하시려면 해당 파일을 스패로우 엔지니어에게 전달해주세요.

> **Tip**: 단, 자가 방어의 경우 분석 로그 다운로드 기능이 없습니다.



클라이언트 CLI에서 분석 로그 다운로드하기

Sparrow Enterprise 클라이언트 CLI에서 분석 로그를 다운로드하려면 다음을 수행하세요.

1. 명령 프롬프트를 실행하세요.
2. {Sparrow Enterprise 클라이언트 설치 디렉토리}로 이동하세요.
3. Linux 환경에서는 **sparrow-cli** 파일과 `log analysis` 명령어 및 **옵션**을 입력하세요.

```
./sparrow-cli log analysis -i 45 -o filename -s https://localhost:10880 -u
admin -p /home/user/workspace/password.txt
```

4. Windows 환경에서는 **sparrow-cli.cmd** 파일과 `log analysis` 명령어 및 **옵션**을 입력하세요.

```
sparrow-cli.cmd log analysis -i 45 -o filename -s https://localhost:10880 -u
admin -p C:\workspace\password.txt
```

5. 아래 내용을 참고하여 **옵션**을 입력하고 실행하세요.(*는 필수 입력 항목)

-i 또는 --id*

로그를 다운로드할 작업의 고유한 ID입니다.(예시: `-i {작업 ID}`)

-o 또는 --out*

다운로드할 로그의 파일 이름입니다.(예시: `-o {파일 이름}`)

-s 또는 --server*

연결하려는 Sparrow Enterprise 서버의 IP 주소 및 포트 번호입니다.(예시: `-s {Sparrow Enterprise 서버 IP 주소}:{포트 번호}`)

-u 또는 -–user*

분석 로그를 다운로드하려는 사용자 계정의 ID입니다.(예시: `-u {사용자 ID}`)

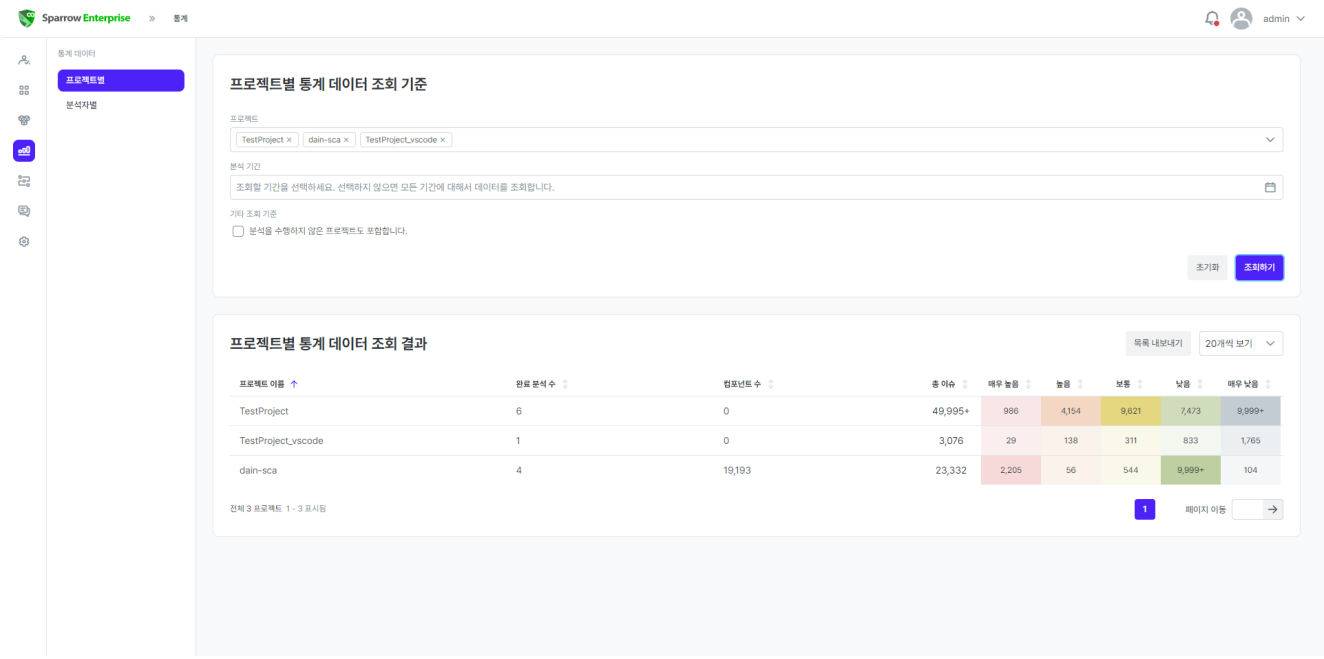
-p 또는 -–password

분석을 수행하려는 사용자 계정의 비밀번호를 저장한 txt 파일의 위치입니다. 이 옵션에 값을 입력하지 않은 경우 사용자 계정의 비밀번호를 입력하라는 메시지가 추가로 표시되며 해당 메시지에 비밀번호를 입력하면 됩니다.(예시: `-p {txt 파일 경로}`)

❓ 사이드 바에 있는 네 번째 아이콘은 어떤 용도인지 궁금합니다.

사이드 바에 있는 네 번째 아이콘은 **통계** 아이콘입니다. 여기서는 Sparrow Enterprise에서 분석한 데이터를 **프로젝트별** 혹은 **분석자별**로 나누어 확인할 수 있습니다.

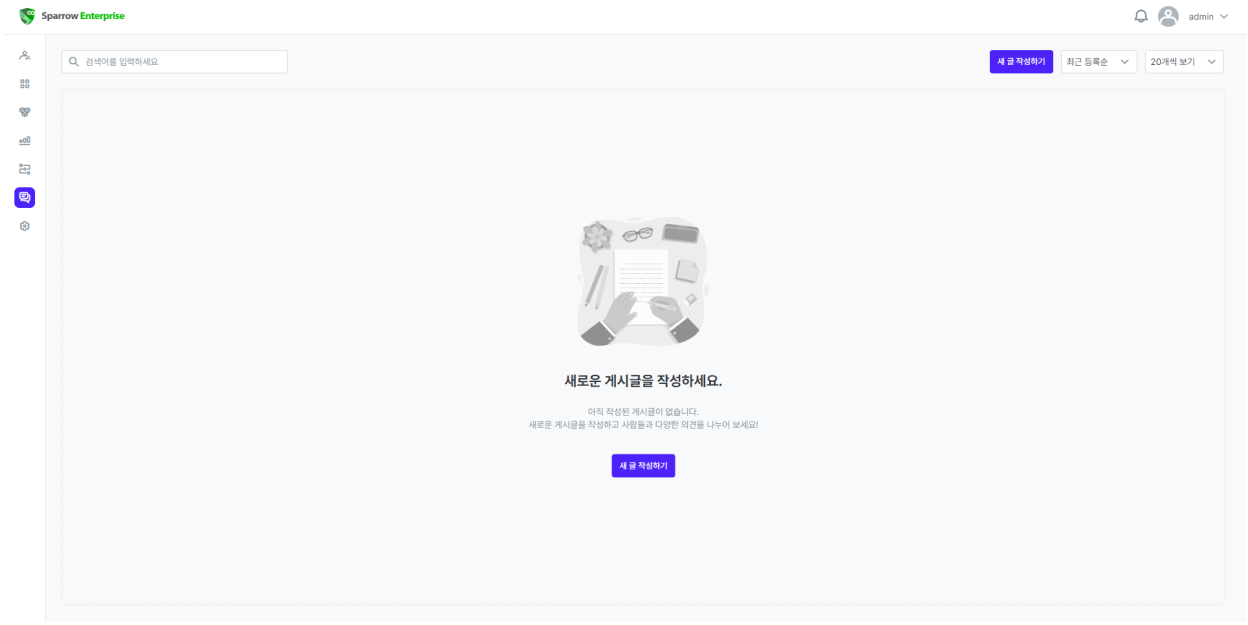
각각의 화면에서 **프로젝트 혹은 분석자**, **분석 완료 기간**, **포함할 분석** 및 **기타 조회 기준**을 선택한 다음 **조회하기** 버튼을 클릭하면 해당하는 데이터가 테이블로 표시됩니다.



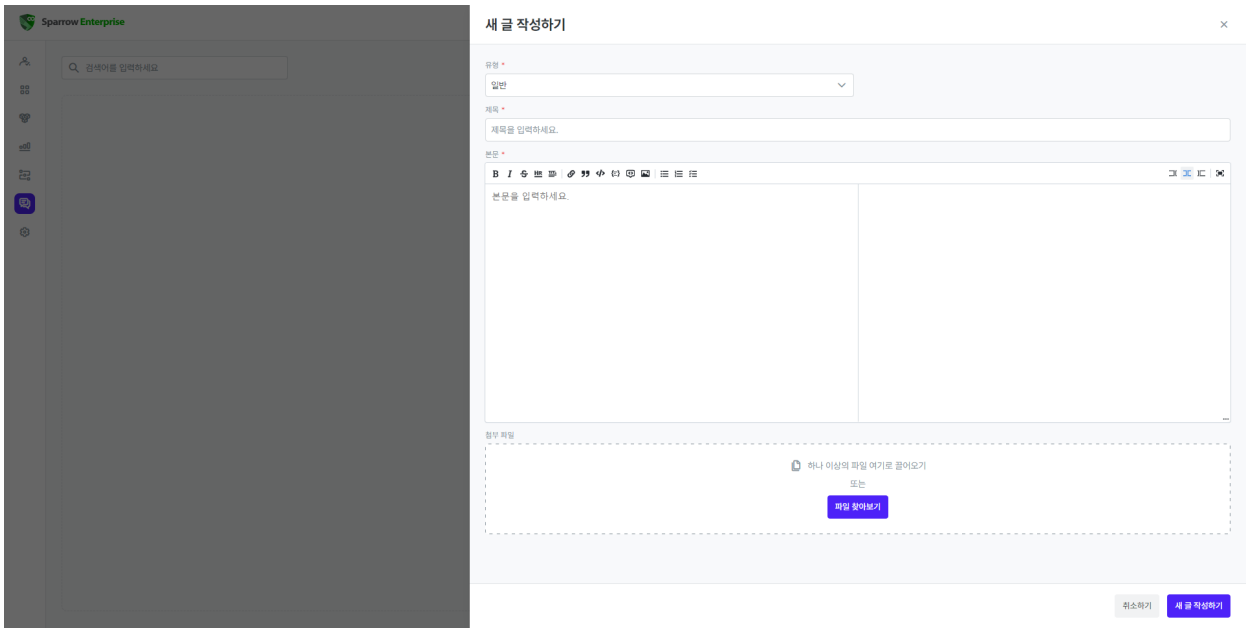
❓ Sparrow Enterprise에는 게시판 기능이 있는지 궁금합니다.

사이드 바에 있는 여섯 번째 아이콘을 클릭하면 게시판을 사용할 수 있습니다. 자세한 방법은 다음과 같습니다.

1. 사이드 바에서 **게시판** 아이콘을 클릭하세요.



2. **새 글 작성하기** 버튼을 클릭하세요.



3. 아래를 참고하여 글의 **유형**, **제목**, **본문**을 입력하세요. (*는 필수 입력 항목)

4. **새 글 작성하기** 버튼을 클릭하세요.

작성한 글을 클릭하여 글 본문 아래에 답글을 올릴 수 있습니다.

유형*

작성할 글의 유형이며 시스템의 **시스템 관리** 권한이 있는 관리자는 일반, 공지사항 중에 하나를 선택할 수 있습니다. 공지사항으로 작성된 글은 게시글의 첫 페이지에 표시됩니다.(기본값: 일반)

제목*

작성할 글의 제목이며 100자 이하의 모든 문자를 입력할 수 있습니다.

본문*

작성할 글의 본문이며 마크다운 형식으로 5,000자까지 입력할 수 있습니다.

첨부 파일

작성할 글에 첨부하려는 파일이며 최대 5개의 파일을 업로드할 수 있습니다. 파일의 크기는 개당 1,000MB 이하여야 합니다.

고객센터

추가적으로 Sparrow Enterprise에 대해 궁금하신 점이나 필요한 정보가 있으신 경우 **스패로우 고객센터**로 문의해주세요.

법적 고지

본 문서는 ㈜스패로우에서 제공하는 Sparrow Enterprise 사용 방법 및 서비스 사용과 관련된 제반 사항을 설명한 문서입니다. 본 문서의 내용과 프로그램은 저작권법의 보호를 받습니다. 본 문서와 본 문서에 설명된 프로그램은 ㈜스패로우와의 사용권 계약 하에서만 사용할 수 있습니다. ㈜스패로우의 사전 서면 동의 없이 본 문서의 전체 또는 일부분을 전자, 기계, 녹음 등의 수단을 사용하여 전송, 복제, 배포하거나 2차적 저작물을 작성할 수 없습니다. 본 문서에 포함된 내용은 추후 제품의 기능 개선 등에 따라 사전 예고 없이 변경될 수 있습니다. 본 제품은 설치 CD와 가이드로 구성됩니다. 본 제품의 품질보증기간은 제품 구입일로부터 1년이며 이후 별도 계약을 통해 품질을 유지 보수할 수 있습니다.

Microsoft, MS, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10은 Microsoft의 등록 상표입니다.

주식회사 스패로우

대표 전화 02-6263-7400

팩스 02-6263-7410

이메일 sales@sparrow.im

홈페이지 https://sparrow.im

주소 서울시 마포구 월드컵북로 396 누리꿈스퀘어 비즈니스타워 13층