

Jira Software 9.13.x 릴리스 노트

이 문서는 2024년 1월 22일 출시된 Jira Software 9.13.x 릴리즈 노트를 공유하기 위해 작성되었습니다.

- [Highlights](#)
- 호환 가능한 응용 프로그램
- 항상 가장 오래된 메모 또는 가장 최근에 표시된 메모를 먼저 봅니다.
- 여러 문제에 대한 설명을 동시에 업데이트
- 이슈를 만드는 동안 Watchers 추가
- 데이터베이스 암호를 HashiCorp Vault에 저장하여 보안
- 해결된 문제
 - 9.13.0에서 해결된 내용
 - 9.13.1에서 해결된 내용



9.13.x부터 Jira의 새 릴리스는 데이터 센터 고객만 사용할 수 있습니다. 서버 라이선스가 있는 경우 [업그레이드 옵션을 확인하십시오](#).

Highlights

- 항상 가장 오래되거나 최신으로 표시된 주석을 먼저 봅니다
- 여러 문제에 대한 설명을 동시에 업데이트합니다
- 이슈를 생성하는 동안 Watchers 추가
- 데이터베이스 암호를 HashiCorp Vault에 저장하여 보안 설정

호환 가능한 응용 프로그램

호환되는 Jira 애플리케이션을 찾고 있다면 더 이상 찾지 마십시오.

- [Jira Service Management 5.13 릴리스 노트](#)

항상 가장 오래된 메모 또는 가장 최근에 표시된 메모를 먼저 봅니다.

이제 Jira는 선호하는 댓글 정렬 순서를 기억합니다. 문제 댓글을 보는 방법(최신 또는 오래된 것부터)을 선택하면 나머지도 같은 방식으로 정렬됩니다.

로그아웃하거나 캐시를 지울 수 있지만 정렬 순서는 변경하지 않는 한 기본 "최신 주석 먼저"로 재설정되지 않습니다.

여러 문제에 대한 설명을 동시에 업데이트

여러 문제에 대한 설명을 조정해야 하는 경우 각 문제를 개별적으로 수정하는 데 시간이 걸릴 수 있습니다. 특히 몇 줄만 변경하면 되는 경우입니다.

시간을 절약하고 이슈 편집 프로세스를 보다 효율적으로 만들기 위해 대량 편집 메뉴에 **새로운** 옵션인 **설명 변경**을 추가했습니다. 여러 가지 방법으로 선택한 문제에 대한 설명을 자동으로 수정할 수 있습니다. [blocked URL](#)

1. 설명 필드를 업데이트하기 위한 옵션:
 - **Replace existing**: 현재 설명을 새 텍스트로 바꿉니다.
 - **Add before existing** (the default option): 현재 설명의 시작 부분에 텍스트를 추가합니다.
 - **Add after existing**: 현재 설명 끝에 텍스트를 추가합니다.
2. 문제 설명에 대한 텍스트 필드

문제 설명을 일괄 편집하려면 선택한 모든 문제에 대한 **문제 수정** 권한이 있어야 합니다. 자세한 내용은 다음 가이드를 확인하세요.

- [Jira에서 프로젝트 권한 관리](#)
- [여러 이슈를 동시에 편집](#)

이슈를 만드는 동안 Watchers 추가

문제를 만들 때 Watchers를 추가하여 팀을 최신 상태로 유지하면서 시간을 절약하세요. 문제를 만든 다음 Watchers를 추가하기 위해 즉시 편집하는 데 시간을 낭비할 필요가 없습니다!



이 기능을 사용하려면 관리자가 기능 플래그 `.com.atlassian.jira.initialwatchers.enabled`를 사용해야 합니다. Jira에서 다크 기능을 활성화하는 방법에 대해 알아보십시오 [Learn how to enable dark features in Jira](#)

새 문제를 만드는 경우:

1. **Create issue(문제 만들기)** 대화 상자에서 **Watchers**로 이동합니다.
2. 입력을 시작하여 이번 이슈를 지켜볼 사람을 찾습니다.
3. Watchers로 추가할 사람을 선택합니다.

문제를 만드는 동안 Watchers를 선택하면 **만들기**를 선택한 후 문제에 추가됩니다. 추가한 사람이 문제에 대한 올바른 프로젝트에 없는 경우 Jira는 사용자에게 알리고 Watchers로 추가하지 않습니다.

[blocked URL](#)

데이터베이스 암호를 HashiCorp Vault에 저장하여 보안

HashiCorp Vault에 암호를 저장하여 암호를 보호하십시오. 이제 관리자는 SecretStore 구현을 활성화하여 Vault 인스턴스에서 데이터베이스 암호를 읽을 수 있습니다. 이 옵션은 데이터베이스 암호를 XML 파일에 일반 텍스트로 저장하기 위한 보다 안전한 대안입니다.

아래 지침에서는 Hashicorp Vault 인스턴스가 이미 실행 중이라고 가정합니다. Hashicorp Vault 인스턴스가 없는 경우 [Hashicorp Vault 설명서를 확인하세요](#).

HashiCorp Vault와 함께 작동하도록 Jira를 구성하려면 다음을 수행합니다.

1. HashiCorp Vault 인스턴스에 비밀을 만듭니다.
2. 보안 암호를 읽을 수 있는 권한이 있는 정책을 생성합니다.
3. Vault를 사용하여 Jira를 인증합니다.
4. `<home-directory>/dbconfig.xml` 구성 파일에 Vault 구성 데이터를 추가합니다.

[HashiCorp Vault에서 데이터베이스 암호 보안에 대해 자세히 알아보기](#)

해결된 문제

[9.13.0에서 해결된 내용](#)

[9.13.1에서 해결된 내용](#)