# 변경 로그, 워크플로우 및 작업 모니터링 및 보고

Security Cloud Control는 구성 변경 로그, 대량 디바이스 작업, 디바이스와 통신할 때 실행되는 프로세스를 효과적으로 모니터링합니다. 이를 통해 네트워크의 기존 정책이 보안 상태에 어떤 영향을 미치는지 파악할 수 있습니다.



## Security Cloud Control에서 변경 로그 관리

변경 로그는 Security Cloud Control에서 수행한 구성 변경 사항을 캡처하여, 지원되는 모든 디바이스 및 서비스의 변경 사항을 포함하는 단일 보기를 제공합니다. 다음은 변경 로그의 몇 가지 기능입니다.

- 디바이스 구성에 대한 변경 사항을 나란히 비교하여 제공합니다.
- 모든 변경 로그 항목에 대한 레이블을 제공합니다.
- 디바이스의 온보딩 및 제거를 기록합니다.
- Security Cloud Control 외부에서 발생하는 정책 변경 충돌을 탐지합니다.
- 인시던트 조사 또는 문제 해결 중에 누가, 무엇을, 언제 하는지에 대한 답변을 제공합니다.
- 전체 변경 로그 또는 일부만 CSV 파일로 다운로드할 수 있습니다.

**Note** 클라우드 제공 Firewall Management Center에서 변경한 사항은 변경 로그에 반영되지 않습니다.

### 로그 용량 변경 관리

Security Cloud Control는 변경 로그 정보를 1년 동안 보관하고 1년이 지난 데이터는 삭제합니다.

Security Cloud Control의 데이터베이스에 저장된 변경 로그 정보와 내보낸 변경 로그에 표시되는 변경 로그 정보에는 차이가 있습니다. 자세한 내용은 변경 로그 내보내기, on page 9를 참조하십시오.

### 변경 로그 항목

변경 로그 항목은 단일 디바이스 구성의 변경 사항, 디바이스에서 수행된 작업 또는 Security Cloud Control 외부에서 디바이스에 이루어진 변경 사항을 반영합니다.

- 구성 변경 내용이 포함된 변경 로그 항목의 경우 해당 행의 아무 곳이나 클릭하여 변경 내용에 대한 세부 정보를 볼 수 있습니다.
- Security Cloud Control 외부에서 이루어진 대역 외 변경이 충돌로 감지되는 경우 시스템 사용자가 마지막 사용자로 보고됩니다.
- Security Cloud Control의 디바이스 구성이 디바이스의 구성과 동기화된 후 또는 디바이스가 Security Cloud Control에서 제거되면 Security Cloud Control는 변경 로그 항목을 닫습니다. 구성은 디바이스에서 Security Cloud Control로 구성을 읽거나 Security Cloud Control에서 디바이스로 구성을 구축한 후에 동기화된 것으로 간주됩니다.
- Security Cloud Control는 변경의 성공 여부와 관계없이 기존 항목을 완료한 후 즉시 새 변경 로그 항목을 만듭니다. 새 변경 로그 항목이 열리면 추가 구성 변경 사항이 추가됩니다.
- 디바이스에 대한 읽기, 구축 및 삭제 작업에 대한 이벤트가 표시됩니다. 이러한 작업은 디바이스의 변경 로그를 닫습니다.
- (읽기 또는 구축을 통해) Security Cloud Control가 디바이스의 구성과 동기화된 후에 또는 Security Cloud Control가 더 이상 디바이스를 관리하지 않는 경우 변경 로그가 닫힙니다.
- Security Cloud Control 외부에서 디바이스를 변경하면 변경 로그에 "충돌 감지됨" 항목이 포함됩니다.

### 보류 중 및 완료된 변경 로그 항목

변경 로그의 상태는 보류 중 또는 완료 중 하나입니다. Security Cloud Control를 사용하여 디바이스의 구성을 변경하면 이러한 변경 사항은 보류 중인 변경 로그 항목에 기록됩니다. 다음 활동으로 보류 중인 변경 로그가 완성되고, 그 후에는 향후 변경 사항을 기록하기 위한 새 변경 로그가 만들어집니다.

- 디바이스에서 Security Cloud Control로 구성을 읽기
- Security Cloud Control에서 디바이스로 변경 사항 구축
- Security Cloud Control에서 디바이스 삭제
- 실행 중인 구성 파일을 업데이트하는 CLI 명령 실행

변경 로그 항목 검색 및 필터링

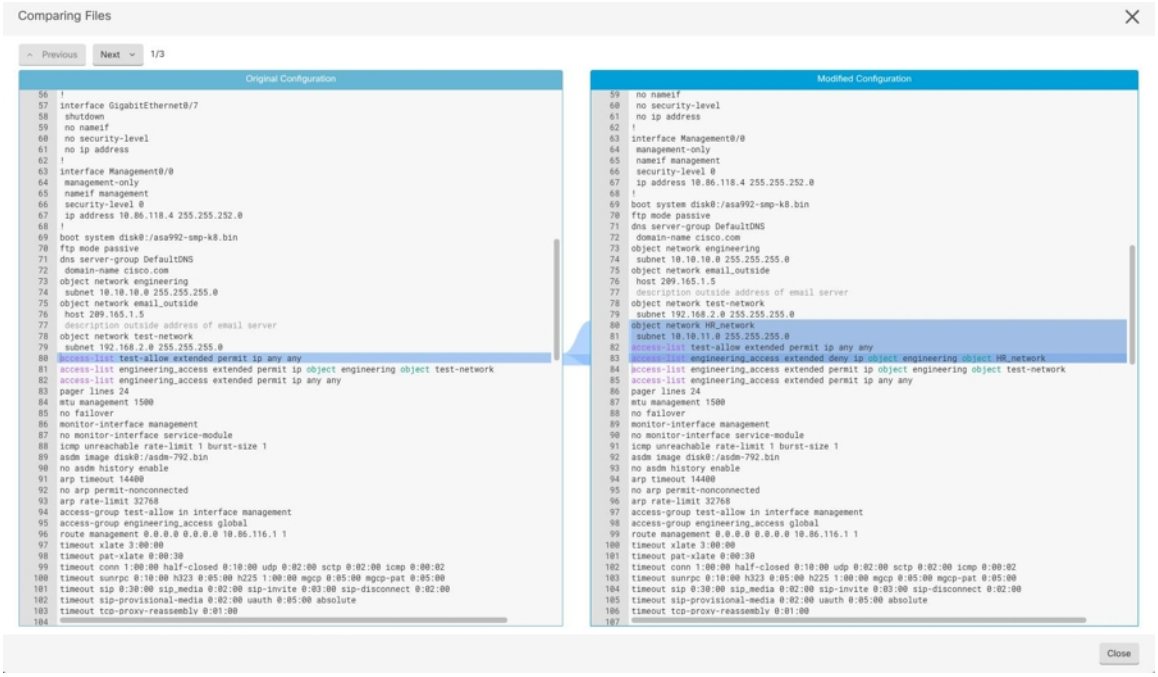
변경 로그 항목을 검색하고 필터링할 수 있습니다. 검색 필드를 사용하여 이벤트를 찾습니다. 필터 ( )를 사용하여 지정한 기준에 맞는 항목을 찾습니다. 변경 로그를 필터링하고 검색 필드에 키워드를 추가하여 필터링된 결과 내에서 항목을 찾는 방식으로 두 작업을 결합할 수도 있습니다.

# 변경 로그 차이점 보기

변경 로그에서 파란색 **Diff**를 클릭하면 디바이스의 실행 중인 구성 파일에서 변경 사항을 나란히 비교할 수 있습니다.

다음 그림에서 **Original Configuration(**원래 구성**)** 열은 ASA 디바이스에 변경 사항을 기록하기 전에 실행 중인 구성 파일입니다. **Modified Configuration(**수정된 구성**)** 열에는 변경 사항이 작성된 후 실행 중인 구성 파일이 표시됩니다. 이 경우 원래 구성 열은 실행 중인 구성 파일의 행을 강조 표시하며, 이 행은 변경되지 않지만 수정된 구성 열에서 참조할 수 있는 지점을 제공합니다.

왼쪽 열에서 오른쪽 열로 가로지르는 선을 따라가면 엔지니어링 네트워크의 주소가 *HR_network* 네트워크의 주소에 도달하지 못하도록 하는 액세스 규칙과 *HR_network* 개체가 추가되는 것을 확인할 수 있습니다. **Previous(**이전**)** 및 **Next(**다음**)**를 클릭하여 파일의 변경 사항으로 이동합니다.




관련 주제

- Security Cloud Control에서 변경 로그 관리, on page 1

# 변경 요청 관리

변경 요청 관리는 변경 요청과 그 비즈니스 정당성을 변경 로그 이벤트에 연결할 수 있습니다. 변경 요청은 서드파티 티켓팅 시스템에서 열립니다.

변경 요청 관리를 사용하여 Security Cloud Control에서 변경 요청을 생성하고 변경 로그 이벤트와 연결합니다. 변경 로그 내에서 이름으로 이 변경 요청을 검색할 수 있습니다.

**Note** Security Cloud Control에서 변경 요청 추적과 변경 요청 관리는 동일한 기능을 의미합니다.

## 변화 요청 관리 활성화

변경 요청 추적을 활성화하면 조직의 모든 사용자에게 영향을 미칩니다.

**Procedure**

단계 **1** 왼쪽 창에서 **Administration(**관리**)** > **General Settings(**일반 설정**)**을 클릭합니다.

단계 **2** **Change Request Tracking(**변경 요청 추적**)** 토글 버튼 활성화


이 기능을 활성화하면 변경 요청 메뉴가 왼쪽 하단에 나타나고 변경 로그 페이지에서 변경 요청 드롭다운 목록을 사용할 수 있습니다.

## 변경 요청 생성

**Procedure**

단계 **1** Security Cloud Control에서 왼쪽 하단의 **Change Request** (변경 요청) 메뉴에서 변경 요청 생성(+ ) 아이콘을 클릭합니다.

단계 **2** **Name(**이름**)** 및 **Description(**설명**)**을 입력합니다.

**Name(**이름**)**이 조직에서 사용하려는 **Change Request(**변경 요청**)** 이름과 일치하는지, **Description(**설명**)**에 변경의 목적이 설명되어 있는지 확인합니다.

**Note**
**Change Request(**변경 요청**)**을 생성한 후에는 이름을 변경할 수 없습니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

**Note**
**Change Request(**변경 요청**)**이 저장되면 Security Cloud Control은 모든 새 변경 사항을 해당 **Change Request(**변경 요청**)** 이름에 연결합니다. 이 연결은 변경 요청을 비활성화하거나 메뉴에서 변경 요청 세부 정보를 지울 때까지 계속됩니다.

# 변경 요청을 변경 로그 이벤트와 연결

**Procedure**

단계 **1** 왼쪽 창에서 를 클릭합니다**Monitor(**모니터링**)** > **Events & Logs(**이벤트 및 로그**)** > **Log(**로그**)** > **Change Log(**변경 로그**)**.

단계 **2** 변경 로그를 확장하여 변경 요청과 연결하려는 이벤트를 확인합니다.

단계 **3** 해당 변경 로그 항목 옆에 있는 드롭다운 목록을 클릭합니다.

**Note**
최신 변경 요청은 변경 요청 목록 상단에 표시됩니다.

단계 **4** 변경 요청을 선택하고 **Select(**선택**)**을 클릭합니다.

# 변경 요청으로 변경 로그 이벤트 검색

**Procedure**

단계 **1** 왼쪽 창에서 를 클릭합니다**Monitor(**모니터링**)** > **Events & Logs(**이벤트 및 로그**)** > **Log(**로그**)** > **Change Log(**변경 로그**)**.

단계 **2** 해당 변경 요청과 연관된 변경 로그 이벤트를 찾기 위해 변경 로그 검색 필드에 변경 요청의 이름을 입력합니다.

Security Cloud Control는 정확히 일치하는 변경 로그 이벤트를 강조 표시합니다.

# 변경 요청 검색

**Procedure**

단계 **1** Security Cloud Control에서 왼쪽 하단의 **Change Request** (변경 요청) 메뉴에서 변경 요청 생성(**+** ) 아이콘을 클릭합니다.

단계 **2** 검색 필드에 **Change Request(**변경 요청**)**의 이름 또는 관련 키워드를 입력합니다. 값을 입력하면 입력한 내용과 부분적으로 일치하는 결과가 이름 및 설명 필드에 모두 표시됩니다.

# 변경 요청 필터링

**Procedure**

단계 **1** 왼쪽 창에서 를 클릭합니다**Monitor(**모니터링**)** > **Events & Logs(**이벤트 및 로그**)** > **Log(**로그**)** > **Change Log(**변경 로그**)**.

단계 **2** 모든 옵션을 보려면 필터 아이콘을 클릭합니다.

단계 **3** 검색 필드에 **Change Request(**변경 요청**)**의 이름을 입력합니다.

값을 입력하면 입력한 값과 부분적으로 일치하는 결과가 표시됩니다.

단계 **4** 해당 체크 박스 을 선택 하여 변경 요청 을 선택합니다.

일치하는 항목은 **Change Log(**변경 로그**)** 테이블에 표시됩니다. Security Cloud Control는 정확히 일치하는 변경 로그 이벤트를 강조 표시합니다.

# 변경 요청 툴바 지우기

변경 로그 이벤트가 기존 변경 요청과 자동으로 연결되지 않도록 하려면 변경 요청 도구 모음에서 정보를 지우십시오.

**Procedure**

단계 **1** 왼쪽 하단의 변경 요청 메뉴에서 변경 요청 생성(**+** ) 아이콘을 클릭합니다.

단계 **2** **Clear(**지우기**)**를 클릭합니다.

이제 변경 요청 메뉴에 **None(**없음**)**이 표시됩니다.

# 변경 로그 이벤트와 관련된 변경 요청 지우기

**Procedure**

단계 **1** 왼쪽 창에서 **Monitor(**모니터링**)** > **Events & Logs(**이벤트 및 로그**)** > **Log(**로그**)** > **Change Log(**변경 로그**)**를 클릭합니다.

단계 **2** 변경 로그를 확장하여 변경 요청에서 연결 해제하려는 이벤트를 표시합니다.

단계 **3** 해당 변경 로그 항목 옆에 있는 드롭다운 목록을 클릭합니다.

단계 **4** **Clear(**지우기**)**를 클릭합니다.

# 변경 요청 삭제

변경 요청을 삭제하면 변경 요청 목록에서는 삭제되지만 변경 로그에서는 삭제되지 않습니다.

**Procedure**

단계 **1** 왼쪽 하단의 변경 요청 메뉴에서 변경 요청 생성(+ ) 아이콘을 클릭합니다.

단계 **2** 변경 요청 을 선택하고 저장소 아이콘을 클릭하여 삭제합니다.

단계 **3** 확인 표시를 클릭하여 확인합니다.

# 변화 요청 관리 비활성화

**Change Request Management(**변경 요청 관리**)**를 비활성화하거나 **Change Request Tracking(**변경 요청 추적**)**을 비활성화하면 어카운트의 모든 사용자에게 영향을 미칩니다.

**Procedure**

단계 **1** 왼쪽 창에서 **Administration(**관리**)** > **General Settings(**일반 설정**)**을 클릭합니다.

단계 **2** **Change Request Tracking(**변경 요청 추적**)** 토글 버튼 비활성화

# 변경 요청 관리 사용 사례

이 사용 사례에서는 변경 요청 관리를 활성화했다고 가정합니다.

### 외부 시스템에서 유지 관리되는 티켓을 해결하기 위해 방화벽 디바이스에 적용된 변경 사항을 추적

이 활용 사례 에서는 외부 시스템에서 유지 관리되는 티켓을 해결하기 위해 방화벽 디바이스를 변경하고 이러한 방화벽 변경에서 발생하는 변경 로그 이벤트를 변경 요청 에 연결하려는 시나리오에 대해 설명합니다. 변경 요청을 생성하고 변경 로그 이벤트를 연결하려면 다음 절차를 따르십시오.

1. 변경 요청 생성, on page 4.
2. 외부 시스템의 티켓 이름이나 번호를 변경 요청의 이름으로 사용하고 설명 필드에 변경의 정당성 및 기타 관련 정보를 추가합니다.
3. 변경 요청 도구 모음에 새 변경 요청이 표시되는지 확인합니다.
4. 방화벽 디바이스를 변경합니다.
5. 탐색창에서 변경 로그를 클릭하고 새 변경 요청과 연결된 변경 로그 이벤트를 찾습니다.
6. 변경 로그 이벤트가 기존 변경 요청과 자동으로 연결되지 않도록 하기 위한 변경 요청 툴바 지우기, on page 6.

### 방화벽 디바이스 변경 후 개별 변경 로그 이벤트 수동 업데이트

이 사용 사례에서는 외부 시스템에서 유지 관리되는 티켓을 해결하기 위해 방화벽 디바이스를 변경했지만 변경 요청 관리 기능을 사용하여 변경 요청을 변경 로그 이벤트와 연결하는 것을 잊어버린 시나리오를 설명합니다. 티켓 번호로 변경 로그 이벤트를 업데이트하려고 합니다. 변경 요청을 변경 로그 이벤트와 연결하려면 다음 절차를 따르십시오.

1. 변경 요청 생성, on page 4. 외부 시스템의 티켓 이름 또는 번호를 변경 요청 이름으로 사용합니다. 설명 필드를 사용하여 변경 및 기타 관련 정보에 대한 근거를 추가합니다.
2. 탐색창에서 **Change Log(**로그 변경**)**를 클릭하고 변경 사항과 관련된 변경 로그 이벤트를 검색합니다.
3. 변경 요청을 변경 로그 이벤트와 연결, on page 5.
4. 변경 로그 이벤트가 기존 변경 요청과 자동으로 연결되지 않도록 하기 위한 변경 요청 툴바 지우기, on page 6.

### 변경 요청과 관련된 변경 로그 이벤트 검색

이 사용 사례에서는 외부 시스템에서 유지 관리되는 티켓을 해결하기 위해 수행한 작업으로 인해 변경 로그에 어떤 변경 로그 이벤트가 기록되었는지 확인하려는 시나리오를 설명합니다. 변경 요청과 관련된 변경 로그 이벤트를 검색하려면 다음 절차를 따르십시오.

1. 탐색창에서 **Change Log(**변경 로그**)**를 클릭합니다**.**
2. 다음 방법 중 하나를 사용하여 변경 요청과 관련된 변경 로그 이벤트를 검색합니다.
   - 해당 변경 요청과 연관된 변경 로그 이벤트를 찾기 위해 변경 로그 검색 필드에 변경 요청의 정확한 이름을 입력합니다. Security Cloud Control는 정확히 일치하는 변경 로그 이벤트를 강조 표시합니다.

- 변경 로그 이벤트를 찾기 위한 변경 요청 필터링, on page 6

3. 관련된 변경 요청을 보여주는 강조 표시된 변경 로그 이벤트를 찾으려면 각 변경 로그를 봅니다.

# 변경 로그 내보내기

Security Cloud Control 변경 로그 전체 또는 하위 집합을 쉼표로 구분된 값(.csv) 파일로 내보내 원하는 대로 정보를 필터링하고 정렬할 수 있습니다.

변경 로그를 .csv 파일로 내보내려면 다음 절차를 수행합니다.

**Procedure**

단계 **1** 왼쪽 창에서 **Monitor(**모니터링**)** > **Events & Logs(**이벤트 및 로그**)** > **Log(**로그**)** > **Change Log(**변경 로그**)**를 클릭합니다.

단계 **2** 다음 작업 중 하나를 수행하여 내보낼 변경 사항을 찾습니다.

- 필터( ) 및 검색 필드를 사용하여 내보낼 항목을 찾습니다. 예를 들어 디바이스를 기준으로 필터링하면 선택한 디바이스에 대한 변경 사항만 표시됩니다.
- 변경 로그에서 모든 필터 및 검색 기준을 지웁니다. 이렇게 하면 전체 변경 로그를 내보낼 수 있습니다.

**Note**
Security Cloud Control는 1년간의 변경 로그 데이터를 보관합니다. 1년 동안의 전체 변경 로그 기록을 다운로드하는 것보다 변경 로그 내용을 필터링하여 그 결과를 .csv 파일로 다운로드하는 것이 좋습니다.

단계 **3** 페이지 오른쪽 상단에 있는 내보내기 아이콘을 클릭합니다.

단계 **4** .csv 파일을 설명이 포함된 이름과 함께 로컬 파일 시스템에 저장합니다.

# Security Cloud Control의 변경 로그 용량과 내보낸 변경 로그 크기의 차이

Security Cloud Control의 변경 로그 페이지에서 내보내는 정보는 Security Cloud Control가 데이터베이스에 저장하는 변경 로그 정보와 다릅니다.

모든 변경 로그에 대해 Security Cloud Control는 두 개의 디바이스 구성 사본을 저장합니다. 하나는 시작 구성이고, 다른 하나는 닫힌 변경 로그의 경우 종료 구성 또는 열린 변경 로그의 경우 현재 구성입니다. 이를 통해 Security Cloud Control는 구성 차이를 나란히 표시할 수 있습니다. 또한 Security Cloud Control는 변경한 사용자 이름, 변경한 시간 및 기타 세부 정보와 함께 모든 단계 (변경 이벤트)를 추적하고 저장합니다.

그러나 변경 로그를 내보낼 때 구성의 전체 사본 두 개가 내보내기에 포함되지 않습니다.두 여기에는 내보내기 파일이 변경 로그 Security Cloud Control가 저장하는 것보다 훨씬 작은 변경 이벤트만 포함됩니다.

Security Cloud Control는 변경 로그 정보를 1년 동안 저장합니다. 여기에는 두 개의 구성 사본이 포함됩니다.

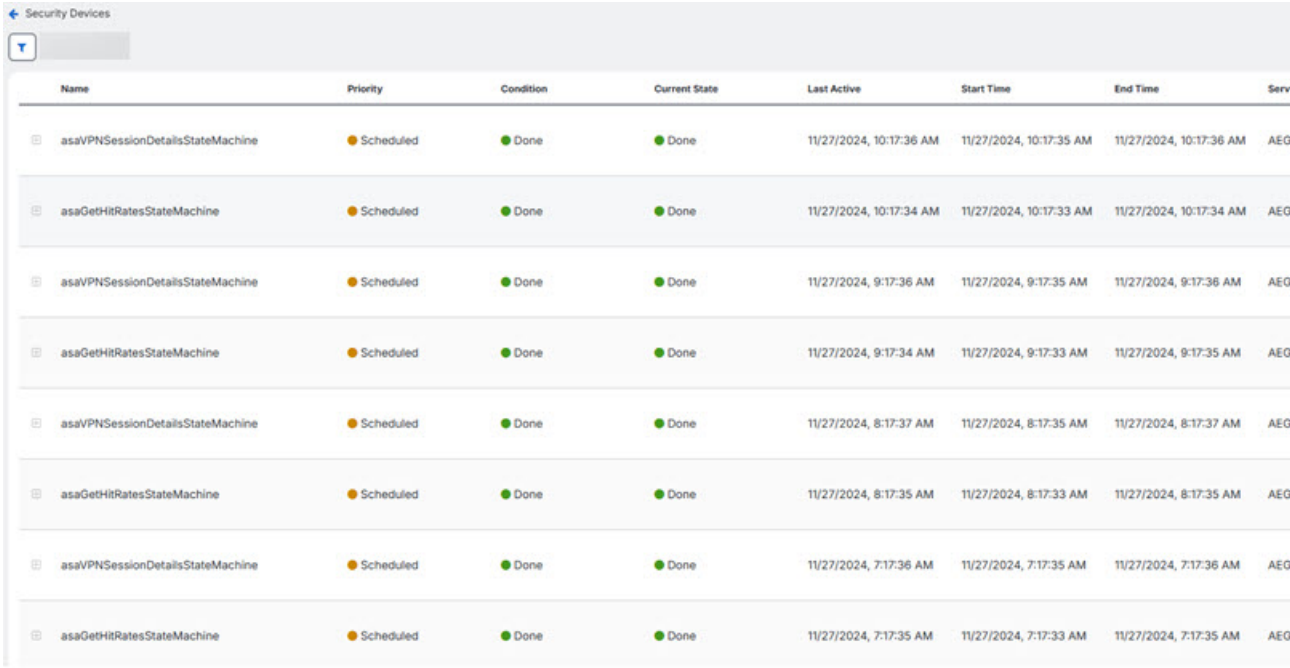
# Security Cloud Control에서 워크플로우 모니터링

워크플로우 페이지에서는 디바이스, SDC(Secure Device Connector) 또는 보안 이벤트 커넥터(SEC)와 통신할 때, 디바이스에 규칙 집합 변경 사항을 적용할 때 Security Cloud Control가 실행하는 모든 프로세스를 모니터링할 수 있습니다. Security Cloud Control은 모든 단계에 대해 워크플로우 테이블에 항목을 만들고 이 페이지에 결과를 표시합니다. 이 항목에는 상호 작용하는 디바이스가 아니라 Security Cloud Control가 수행하는 작업에만 관련된 정보가 포함되어 있습니다.

Security Cloud Control는 디바이스에서 작업을 수행하지 못할 때 오류를 보고합니다. 워크플로우 페이지로 이동하여 오류가 발생한 단계를 확인하여 자세한 내용을 확인하십시오.

또한 이 페이지에서는 오류를 확인 및 해결하거나 필요한 경우 TAC와 정보를 공유할 수 있습니다.

**Workflows(**워크플로우**)** 페이지로 이동하려면, 왼쪽 창의 **Security Devices(**보안 디바이스**)**를 클릭하고, **Devices(**디바이스**)** 탭을 클릭합니다. 적절한 디바이스 유형 탭을 클릭하여 디바이스를 찾고 원하는 디바이스를 선택합니다. 오른쪽 창의 **Devices and Actions(**디바이스 및 작업**)**에서 **Workflows(**워크플로우**)**를 클릭합니다. 다음 그림은 워크플로우 테이블의 항목이 있는 워크플로우 페이지를 보여줍니다.



### 디바이스 워크플로우 내보내기

전체 워크플로우 정보를 JSON 파일로 다운로드하고 TAC 팀에서 추가 분석을 요청할 때 제공할 수 있습니다. 워크플로우 정보를 내보내려면 해당 디바이스를 선택하고 해당 워크플로우 페이지로 이동하여 오른쪽 상단에 나타나는 내보내기( ) 아이콘을 클릭합니다.

### 스택 추적 복사

해결할 수 없는 오류가 발생하여 TAC에 문의하면 스택 추적 사본을 요청할 수 있습니다. 오류에 대한 스택 추적을 수집하려면 **Stack Trace(**스택 추적**)** 링크를 클릭하고 **Copy Stacktrace(**스택 추적 복사**)**를 클릭하여 화면에 나타나는 스택을 클립보드로 복사합니다.

번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.

번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.