온프레미스 방화벽 Management Center 디바이스 구성

이 장에는 다음 섹션이 포함되어 있습니다.

온보딩된 온프레미스 방화벽 Management Center 보기

온보딩된 온프레미스 방화벽 Management Center를 보려면 다음 단계를 수행합니다.

1. 왼쪽 창에서 **Administration(관리)** > **Integration(통합)** > **Firewall Management Center**를 클릭합니다.
2. **FMC** 탭을 클릭합니다.

온프레미스 방화벽 Management Center 고가용성 쌍 보기

고가용성 쌍은 서비스 페이지에 표시됩니다. 쌍을 확장하면 현재 상태와 함께 기본 및 보조 온프레미스 방화벽 Management Center 노드를 볼 수 있습니다.

활성 온프레미스 방화벽 Management Center을 교차 실행하려면 다음 단계를 수행합니다.

1. 서비스 페이지에서 해당 고가용성 쌍을 확인합니다.
2. 오른쪽 창에서 온프레미스 방화벽 Management Center에서 열려는 기능을 클릭합니다.

   FMC 교차 실행 **URL** 확인 창이 표시됩니다. 기본적으로 현재 활성 온프레미스 방화벽 Management Center의 공인 IP 주소 또는 FQDN이 표시되며, 온프레미스 방화벽 Management Center를 여는데 사용됩니다. 필요한 경우 대기 중인 온프레미스 방화벽 Management Center의 URL을 지정하여 교차 실행할 수 있습니다.

각 온프레미스 방화벽 Management Center 노드에 교차 실행 URL을 추가할 수 있습니다. 쌍에서 교차 실행할 때는 활성 노드가 교차 실행되며 현재 어떤 노드가 활성 상태인지 확인할 필요가 없습니다.

활성 온프레미스 방화벽 Management Center 노드를 교차 실행하려면 다음 단계를 수행합니다.

1. 고가용성 쌍을 확장하고 실행하려는 기본 또는 보조 온프레미스 방화벽 Management Center 노드를 클릭합니다.
2. 오른쪽의 외부 링크 창에서 **FMC** 교차 실행 **URL**을 클릭하여 선택한 온프레미스 방화벽 Management Center를 교차 실행합니다.

   온프레미스 방화벽 Management Center의 공인 IP 주소 또는 FQDN과 포트 번호를 업데이트하려면 **FMC** 교차 실행 **URL** 위로 마우스를 가져가서 편집 아이콘을 클릭합니다.

참고 온프레미스 방화벽 Management Center(버전 7.4.x 이하)에서 고가용성을 중단하거나 역할을 전환하는 경우 SecureX 통합을 비활성화했다가 보조 온프레미스 방화벽 Management Center에서 다시 활성화해야 합니다. 이렇게 하려면 보조 온프레미스 방화벽 Management Center로 이동하여 선택합니다.

고가용성 온프레미스 방화벽 Management Center 쌍을 끊으면 참여하는 Management Center가 두 개의 독립 실행형 온프레미스 방화벽 Management Center로 전환됩니다.

온프레미스 Firewall Management Center 네트워크 개체 검색 및 관리

Security Cloud Control를 사용하여 관리하는 온프레미스 방화벽 Management Center가 있고 해당 개체를 공유하고 관리하려면 다음을 수행합니다.

프로시저

단계 **1** 왼쪽 창에서 **Administration(관리)** > **Integration(통합)** > **Firewall Management Center**를 선택하여 **Services(서비스)** 페이지를 확인합니다.

단계 **2** 온프레미스 방화벽 Management Center를 이미 Security Cloud Control에 온보딩한 경우, 이를 선택합니다.

새 온프레미스 방화벽 Management Center를 온보딩하려면 온프레미스 Firewall Management Center 온보딩을 참조하십시오.

단계 **3** 오른쪽의 **Actions(작업)** 창에서 **Settings(설정)**를 선택합니다. 둘 이상의 온프레미스 방화벽 Management Center를 선택하는 경우에는 **Actions(작업)** 창이 표시되지 않습니다.

참고
관리자 또는 최고 관리자여야 **Settings(설정)**를 사용할 수 있습니다.

단계 **4** **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)** 토글 버튼을 활성화합니다.변경 사항을 검토를 위해 스테이징하지 않고 온프레미스 방화벽 Management Center과 자동으로 동기화하려면 네트워크 개체의 자동 동기화 사용 토글을 활성화합니다.

참고

- 선택한 온프레미스 방화벽 Management Center에 하나 이상의 하위 도메인이 있거나 변경 관리 워크플로우가 활성화되어 있는 경우에는 **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)** 토글을 켤 수 없습니다.
- **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)** 토글이 꺼져 있으면 **Enable automatic sync of network objects(**네트워크 개체 자동 동기화 활성화**)** 토글을 켤 수 없습니다.

Security Cloud Control에 온보딩되는 모든 새 온프레미스 방화벽 Management Center에 대해 이 토글 버튼은 수동으로 활성화해야 합니다. 이 옵션을 활성화하면 Security Cloud Control는 온프레미스 방화벽 Management Center에서 개체 검색을 시작합니다. 이러한 개체는 공유, 관리, Security Cloud Control에서 관리하는 다른 플랫폼 전반에서 일관된 개체 정의를 설정하는 데 사용할 수 있습니다.

Security Cloud Control에서 온프레미스 방화벽 Management Center에서 검색된 개체에 재정의를 추가하고 변경 사항을 온프레미스 방화벽 Management Center로 다시 푸시하면 이러한 개체는 이전에는 재정의를 허용하지 않았더라도 온프레미스 방화벽 Management Center에서 재정의를 수락하기 시작합니다. Security Cloud Control에서 재정의가 추가되는 경우 **View Network Object(**네트워크 개체 보기**)** 창의 **Allow Overrides(**재정의 허용**)** 확인란이 자동으로 선택됩니다.

참고
Security Cloud Control의 이미 존재하는 개체를 온프레미스 방화벽 Management Center에 할당하려면 온프레미스 방화벽 Management Center를 선택하고 **Actions(**작업**)** 창에서 **Assign Objects(**개체 할당**)**를 클릭합니다.

관련 정보

- 네트워크 개체
- 온프레미스 Firewall Management Center 구성 미리보기 및 구축
- 온프레미스 방화벽 Management Center에서 충돌 탐지 활성화, 10 페이지

구성 변경 사항 읽기, 삭제, 확인 및 구축

모든 디바이스 구성 읽기

Security Cloud Control 외부의 디바이스에 대한 구성이 변경되면 Security Cloud Control에 저장된 디바이스의 구성과 디바이스의 로컬 구성의 사본은 더 이상 동일하지 않습니다. 구성을 다시 동일하게 만들기 위해 디바이스에 저장된 구성으로 Security Cloud Control의 디바이스 구성 복사본을 덮어쓰려는 경우가 많습니다. **Read All(**모두 읽기**)** 링크를 사용하여 여러 디바이스에서 동시에 이 작업을 수행할 수 있습니다.

Security Cloud Control에서 디바이스 구성의 두 복사본을 관리하는 방법에 대한 자세한 내용은 구성 변경 사항 읽기, 폐기, 확인 및 구축을 참조하십시오.

다음은 **Read All(**모두 읽기**)**을 클릭하면 Security Cloud Control의 디바이스 구성 복사본을 디바이스의 구성 복사본으로 덮어쓰는 세 가지 구성 상태입니다.

- **Conflict Detected(**충돌 탐지**)** -충돌 탐지가 활성화된 경우 Security Cloud Control는 구성 변경 사항에 대해 10분마다 관리하는 디바이스를 폴링합니다. Security Cloud Control는 디바이스의 구성이 변경된 것을 발견하면 Security Cloud Control는 디바이스에 대한 구성 상태를 "충돌 탐지됨"으로 표시합니다.
- **Synced(**동기화됨**)** -디바이스가 동기화된 상태인 경우 **Read All(**모두 읽기**)**을 클릭하면 Security Cloud Control는 즉시 디바이스를 확인하여 구성이 직접 변경되었는지 확인합니다. **Read All(**모두 읽기**)**을 클릭하면 Security Cloud Control는 디바이스 구성의 복사본을 덮어쓸 것임을 확인한 다음 Security Cloud Control는 덮어쓰기를 수행합니다.
- **Not Synced(**동기화되지 않음**)** - 디바이스가 동기화되지 않음 상태인 경우 **Read All(**모두 읽기**)**을 클릭하면 Security Cloud Control는 Security Cloud Control를 사용하는 디바이스의 구성에 대해 보류 중인 변경 사항이 있으며 Read All(모두 읽기) 작업을 진행하면 해당 변경 사항이 삭제되고 디바이스의 구성이 포함된 Security Cloud Control의 구성 복사본입니다. 이 Read All(모두 읽기)은 Discard Changes(변경 사항 취소)와 같은 기능을 합니다.

Procedure

단계 **1** 왼쪽 창에서 보안 디바이스를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** (선택 사항) 변경 로그에서 이 대량 작업의 결과를 쉽게 식별할 수 있도록 변경 요청 레이블을 생성합니다.

단계 **5** Security Cloud Control를 저장할 디바이스를 선택합니다. Security Cloud Control는 선택한 모든 디바이스에 적용할 수 있는 작업에 대해서만 명령 버튼을 제공합니다.

단계 **6** **Read All(**모두 읽기**)**을 클릭합니다.

단계 **7** Security Cloud Control는 Security Cloud Control에 준비된 구성 변경 사항이 있는 경우 선택한 디바이스에 대해 경고하고, 구성 대량 읽기 작업을 계속할 것인지 묻습니다. 계속하려면 **Read All(**모두 읽기**)**을 클릭합니다.

단계 **8** Read All(모두 읽기) 구성 작업의 진행 상황은 알림 탭에서 확인합니다.

단계 **9** 변경 요청 레이블을 생성하고 활성화한 경우 실수로 다른 구성 변경 사항을 이 이벤트와 연결하지 않도록 레이블을 지워야 합니다.

관련 정보

- 구성 변경 사항 읽기, 삭제, 확인 및 구축
- 변경 사항 취소

모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축

Security Cloud Control는 테넌트에서 테넌트의 디바이스에 대한 구성을 변경했지만 해당 변경 사항을 구축하지 않은 경우 구축 아이콘 에 주황색 점을 표시하여 알려줍니다. 이러한 변경의 영향을 받는 디바이스는 **Devices and Services(**디바이스 및 서비스**)** 페이지에서 "Not Synced(동기화되지 않음)" 상태로 표시됩니다. **Deploy(**구축**)**를 클릭하면 보류 중인 변경 사항이 있는 디바이스를 검토하고 해당 디바이스에 변경 사항을 구축할 수 있습니다.

이 구축 방법은 지원되는 모든 디바이스에서 사용할 수 있습니다.

단일 구성 변경 사항에 이 구축 방법을 사용하거나, 기다렸다가 여러 변경 사항을 한 번에 구축할 수 있습니다.

프로시저

단계 **1** Security Cloud Control의 메뉴 모음에서 **Deploy(**구축**)** 버튼 을 클릭합니다.

단계 **2** 구축하려는 변경 사항이 있는 디바이스를 선택합니다. 디바이스에 노란색 주의 삼각형이 있는 경우 해당 디바이스에 변경 사항을 구축할 수 없습니다. 노란색 주의 삼각형 위에 마우스를 올려놓으면 해당 디바이스에 변경 사항을 구축할 수 없는 이유를 확인할 수 있습니다.

단계 **3** (선택 사항) 보류 중인 변경 사항에 대한 자세한 정보를 보려면 **View Detailed Changelog(**자세한 변경 로그 보기**)** 링크를 클릭하여 해당 변경과 관련된 변경 로그를 엽니다. **Deploy(**구축**)** 아이콘을 클릭하여 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지로 돌아갑니다.

단계 **4** 선택한 디바이스에 변경 사항을 즉시 구축하려면 **Deploy Now(**지금 구축**)**를 클릭합니다. 작업 트레이의 활성 작업 표시기에 진행 상황이 표시됩니다.

단계 **5** (선택 사항) 구축이 완료되면 Security Cloud Control 탐색 모음에서 **Jobs(**작업**)**를 클릭합니다. 구축 결과를 보여주는 최근 "Deploy Changes(변경 사항 구축)" 작업이 표시됩니다.

단계 **6** 변경 요청 레이블을 생성했으며 더 이상 연결할 구성 변경 사항이 없는 경우 해당 레이블을 지웁니다.

디바이스 구성 대량 구축

예를 들어 공유 개체를 수정하여 여러 디바이스를 변경한 경우 해당 변경 사항을 영향을 받는 모든 디바이스에 한 번에 적용할 수 있습니다.

Procedure

단계 **1** 왼쪽 창에서 보안 디바이스를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** Security Cloud Control에서 구성을 변경한 모든 디바이스를 선택합니다. 이러한 디바이스는 "동기화되지 않음" 상태로 표시되어야 합니다.

단계 **5** 다음 방법 중 하나를 사용하여 변경 사항을 구축합니다.

- 화면 오른쪽 상단의 버튼을 클릭하여 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 창을 봅니다. 이렇게 하면 구축하기 전에 선택한 디바이스에서 보류 중인 변경 사항을 검토할 수 있습니다. **Deploy Now(**지금 구축**)**를 클릭하여 변경 사항을 구축합니다.

  Note
  Devices with Pending Changes(보류 중인 변경 사항이 있는 디바이스**)** 화면에서 디바이스 옆에 노란색 경고 삼각형이 표시되면 해당 디바이스에 변경 사항을 구축할 수 없습니다. 변경 사항을 해당 디바이스에 구축할 수 없는 이유에 대한 정보를 보려면 경고 삼각형 위에 마우스를 올려놓습니다.

- 세부 정보 창에서 **Deploy All(**모두 구축**)** 을 클릭합니다. 경고를 검토하고 **OK(**확인**)**를 클릭합니다. 대량 구축은 변경 사항을 검토하지 않고 즉시 시작됩니다.

단계 **6** (선택 사항) 탐색 모음에서 Jobs(작업) 아이콘 을 클릭하여 대량 구축의 결과를 확인합니다.

온프레미스 방화벽 **Management Center** 구성 미리보기 및 구축

예를 들어 값을 변경하거나 개체에 재정의를 추가하는 것과 같이 개체의 구성을 변경한 경우, 이러한 모든 변경 사항을 온프레미스 방화벽 Management Center에 한 번에 구축할 수 있습니다.

참고 이 작업은 구성 변경 사항만 온프레미스 방화벽 Management Center에 푸시합니다. 온프레미스 방화벽 Management Center의 Firewall Threat Defense 디바이스에는 이러한 변경 사항을 수동으로 구축해야 합니다. 자세한 내용은 *Cisco Secure Firewall Management Center* 디바이스 구성 가이드의 구성 구축을 참조하십시오.

프로시저

단계 **1** 탐색창에서 **Administration(**관리**)** > **Integration(**통합**)** > **Firewall Management Center**를 클릭하고 변경 사항을 미리 보고 구축하려는 온프레미스 방화벽 Management Center를 선택합니다.

참고
Security Cloud Control는 온프레미스 방화벽 Management Center이 동기화되지 않은 것을 탐지하고 상태를 **Not Synced(**동기화되지 않음**)**로 표시합니다.

단계 **2** 오른쪽의 세부 정보 창에서 **Preview and Deploy(**미리보기 및 구축**)**를 클릭합니다.

단계 **3** 경고를 검토하고 **Deploy Now(**지금 구축**)**를 클릭합니다. 구축은 변경 사항을 검토하지 않고 즉시 시작됩니다. 미리보기 후 구축을 진행하지 않으려면 **Discard All(**모두 취소**)**을 클릭합니다.

단계 **4** 또는 화면 오른쪽 상단의 버튼을 클릭하여 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 창을 볼 수도 있습니다. 원하는 디바이스를 선택하고 디바이스를 구축하기 전에 선택한 디바이스의 보류 중인 변경 사항을 검토합니다.

단계 **5** **Deploy Now(**지금 구축**)**를 클릭하여 변경 사항을 구축합니다.

구성 변경 사항 취소

Security Cloud Control를 사용하여 디바이스의 구성에 적용한 구축 해제된 구성 변경 사항을 모두 "실행 취소"하려면 **Discard Changes(**변경 사항 취소**)**를 클릭합니다. **Discard Changes(**변경 사항 취소**)**를 클릭하면 Security Cloud Control는 디바이스 구성의 로컬 복사본을 디바이스에 저장된 구성으로 완전히 덮어씁니다.

Discard Changes(변경 사항 취소**)**를 클릭하면 디바이스의 구성 상태가 **Not Synced(**동기화되지 않음**)** 상태가 됩니다. 변경 사항을 취소하면 Security Cloud Control의 구성 복사본이 디바이스의 구성 복사본과 동일하게 되며 Security Cloud Control의 구성 상태는 Synced(동기화)로 돌아갑니다.

디바이스에 대해 구축되지 않은 모든 구성 변경 사항을 취소하거나 "실행 취소"하려면 다음을 수행합니다.

Procedure

단계 **1** Security Cloud Control 홈 페이지에서 보안 디바이스를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 구성을 변경한 디바이스를 선택합니다.

단계 **5** 오른쪽의 **Not Synced(**동기화되지 않음**)** 창에서 **Discard Changes(**변경 사항 취소**)**를 클릭합니다.

- FDM 관리 디바이스의 경우 Security Cloud Control는 "Security Cloud Control에서 보류 중인 변경 사항이 취소되고 이 디바이스에 대한 Security Cloud Control 구성이 디바이스에서 현재 실행 중인 구성으로 교체됩니다."라고 경고합니다. 변경 사항을 취소하려면 **Continue(**계속**)**를 클릭합니다.
- Meraki 디바이스의 경우 Security Cloud Control가 변경 사항을 즉시 삭제합니다.
- AWS 디바이스의 경우 Security Cloud Control는 삭제하려는 항목을 표시합니다. **Accept(**수락**)** 또는 **Cancel(**취소**)**을 클릭합니다.

온프레미스 방화벽 **Management Center** 구성 변경 사항 취소

예를 들어, Security Cloud Control와 온프레미스 방화벽 Management Center간에 공유되는 개체에 대해 수행한 모든 Security Cloud Control 변경 구성을 취소하려면 이 절차를 사용합니다. 이렇게 하면

Security Cloud Control가 디바이스에 저장된 구성을 사용하여 구성의 로컬 복사본을 완전히 덮어씁니다.

프로시저

단계 **1** 왼쪽 창에서 **Administration(**관리**)** > **Integration(**통합**)** > **Firewall Management Center**를 클릭합니다.

단계 **2** 변경 사항을 취소하려는 온프레미스 방화벽 Management Center를 선택합니다.

단계 **3** 오른쪽의 **Not Synced(**동기화되지 않음**)** 창에서 **Discard Changes(**변경 사항 취소**)**를 클릭합니다.

Discard Changes(변경 사항 취소**)**를 클릭하면 온프레미스 방화벽 Management Center의 구성 상태가 **Not Synced(**동기화되지 않음**)** 상태가 됩니다. 변경 사항을 취소하면 온프레미스 방화벽 Management Center의 구성 복사본이 Security Cloud Control의 구성 복사본과 동일하게 되며 Security Cloud Control의 구성 상태는 **Synced(**동기화**)**로 돌아갑니다.

디바이스의 대역 외 변경 사항

대역 외 변경 사항은 Security Cloud Control를 사용하지 않고 디바이스에서 직접 변경한 사항을 의미합니다. 이러한 변경은 SSH 연결을 통해 디바이스의 명령줄 인터페이스를 사용하거나 ASA용 ASDM(Adaptive Security Device Manager), FDM 관리디바이스용 또는온프레미스 방화벽 Management Center사용자 인터페이스의 온프레미스 방화벽 Management Center용 FDM과 같은 로컬 관리자를 사용하여 수행할 수 있습니다. 대역 외 변경 사항은 Security Cloud Control에 저장된 디바이스의 구성과 디바이스 자체에 저장된 구성 간에 충돌을 일으킵니다.

디바이스에서 대역외 변경 탐지

ASA 또는 FDM 관리 디바이스, Cisco IOS 디바이스 또는 온프레미스 방화벽 Management Center에 대해 Conflict Detection(충돌 탐지)이 활성화된 경우 Security Cloud Control는 10분마다 디바이스를 확인하여 Security Cloud Control외부에서 디바이스의 구성에 직접 적용된 새로운 변경 사항을 검색합니다.

Security Cloud Control에 저장되지 않은 디바이스 구성 변경 사항이 있음을 발견하면 Security Cloud Control는 해당 디바이스의 구성 상태를 "충돌 탐지됨" 상태로 변경합니다.

Security Cloud Control에서 충돌을 탐지하는 경우 다음 두 가지 조건 중 하나가 발생할 수 있습니다.

- Security Cloud Control의 데이터베이스에 저장되지 않은 디바이스에 직접 적용된 구성 변경 사항이 있습니다.
- FDM 관리 디바이스의 경우 구축되지 않은 FDM 관리 디바이스에 "보류 중인" 구성 변경 사항이 있을 수 있습니다.
- 온프레미스 방화벽 Management Center의 경우, 예를 들어 Security Cloud Control 외부의 개체에 변경 사항이 있어 Security Cloud Control와의 동기화를 위해 보류 중이거나 Security Cloud Control에서 변경 사항이 있어 온프레미스 방화벽 Management Center에 구축하기 위해 보류 중일 수 있습니다.

Security Cloud Control와 디바이스 간 구성 동기화

구성 충돌 정보

Security Devices(보안 디바이스**)** 페이지에서 디바이스 또는 서비스의 상태가 "Synced(동기화됨)", "Not Synced(동기화되지 않음)" 또는 "Conflict Detected(충돌 탐지됨)"인 것을 확인할 수 있습니다. Security Cloud Control를 사용하여 관리하는 온프레미스 방화벽 Management Center의 상태를 확인하려면 **Administration(**관리**)** > **Integration(**통합**)** > **Firewall Management Center**으로 이동합니다.

- 디바이스가 동기화되면 Security Cloud Control의 구성과 디바이스에 로컬로 저장된 구성이 동일합니다.
- 디바이스가 동기화되지 않으면 Security Cloud Control에 저장된 구성이 변경되어 이제 디바이스에 로컬로 저장된 구성과 다릅니다. Security Cloud Control에서 디바이스로 변경 사항을 구축하면 Security Cloud Control의 버전과 일치하도록 디바이스의 구성이 변경됩니다.
- Security Cloud Control 외부에서 디바이스에 적용된 변경 사항을 대역 외 변경 사항이라고 합니다. 대역 외 변경이 수행되면 디바이스에 대해 충돌 탐지가 활성화된 경우 디바이스 상태가 "Conflict Detected(충돌 탐지됨)"로 변경됩니다. 대역 외 변경 사항을 수락하면 는 Security Cloud Control의 구성을 디바이스의 구성과 일치하도록 변경합니다.

충돌 탐지

충돌 탐지가 활성화된 경우 Security Cloud Control는 기본 간격 동안 디바이스를 폴링하여 Security Cloud Control 외부에서 디바이스의 구성이 변경되었는지 확인합니다. Security Cloud Control는 변경 사항을 탐지하면 디바이스의 구성 상태를 **Conflict Detected(**충돌 탐지됨**)**로 변경합니다. Security Cloud Control 외부에서 디바이스에 적용된 변경 사항을 "대역 외" 변경 사항이라고 합니다.

Security Cloud Control에서 관리하는 온프레미스 방화벽 Management Center의 경우, 준비되는 변경 사항이 있고 디바이스가 **Not Synced(**동기화되지 않음**)** 상태이면 Security Cloud Control는 디바이스 폴링을 중지하여 변경 사항을 확인합니다. Security Cloud Control 외부에서 이루어진 변경 사항 중 Security Cloud Control와의 동기화를 위해 보류 중인 변경 사항과 Security Cloud Control에서 수행된 변경 사항 중 온프레미스 방화벽 Management Center에 구축되기 위해 보류 중인 사항이 있는 경우, Security Cloud Control는 온프레미스 방화벽 Management Center이 **Conflict Detected(**충돌 탐지됨**)** 상태임을 선언합니다.

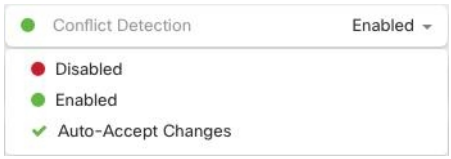
이 옵션이 활성화되면 디바이스별로 충돌 또는 OOB 변경 사항이 탐지되는 빈도를 구성할 수 있습니다. 자세한 내용은 디바이스 변경 사항에 대한 폴링 예약, on page 13를 참조하십시오.

충돌 탐지 활성화

충돌 탐지를 활성화하면 Security Cloud Control 외부에서 디바이스가 변경된 경우 인스턴스에 알림이 표시됩니다.

Procedure

단계 **1** 왼쪽 창에서 보안 디바이스를 클릭합니다.
단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.
단계 **3** 해당 디바이스 탭을 선택합니다.
단계 **4** 충돌 탐지를 활성화할 디바이스를 선택합니다.
단계 **5** 디바이스 테이블 오른쪽에 있는 충돌 감지 상자의 목록에서 **Enabled(**활성화됨**)**을 선택합니다.



온프레미스 방화벽 **Management Center**에서 충돌 탐지 활성화

온프레미스 방화벽 Management Center에 대해 충돌 탐지를 활성화하면 Security Cloud Control 외부에서 이루어진 변경 사항 중 Security Cloud Control와의 동기화를 위해 보류 중인 변경 사항과 Security Cloud Control에서 수행된 변경 사항 중 온프레미스 관리 센터에 구축되기 위해 보류 중인 변경 사항이 있는 경우 알림을 받을 수 있습니다.

프로시저

단계 **1** 내비게이션 바에서 **Administration(**관리**)** > **Integration(**통합**)** > **Firewall Management Center**를 클릭합니다.
단계 **2** 목록에서 충돌 탐지를 활성화할 온프레미스 관리 센터를 선택합니다.
단계 **3** 오른쪽 창에 있는 **Conflict Detection(**충돌 감지**)** 상자의 목록에서 **Enabled(**활성화됨**)**을 선택합니다.

참고
Security Cloud Control에서 관리하는 다른 디바이스와 달리 온프레미스 방화벽 Management Center의 경우 충돌 탐지를 활성화 또는 비활성화할 수 있습니다. 변경 사항 자동 수락을 선택할 수 없습니다.

디바이스에서 대역외 변경 사항 자동 수락

변경 사항 자동 수락을 활성화하여 매니지드 디바이스에 대한 직접 변경 사항을 자동으로 수락하도록 Security Cloud Control를 구성할 수 있습니다. Security Cloud Control를 사용하지 않고 디바이스에 직접 적용된 변경 사항을 대역 외 변경 사항이라고 합니다. 대역 외 변경은 Security Cloud Control에 저장된 디바이스의 구성과 디바이스 자체에 저장된 구성 간에 충돌을 일으킵니다.

자동 수락 변경 기능은 충돌 탐지를 개선한 것입니다. 디바이스에서 변경 사항 자동 수락이 활성화된 경우 Security Cloud Control는 10분마다 변경 사항을 확인하여 디바이스의 구성에 대한 대역 외 변경 사항이 있는지 확인합니다. 구성이 변경된 경우 Security Cloud Control는 사용자에게 확인 상자를 표시하지 않고 디바이스 구성의 로컬 버전을 자동으로 업데이트합니다.

Security Cloud Control에서 아직 디바이스에 구축되지 않은 구성 변경 사항이 있는 경우 Security Cloud Control는 구성 변경을 자동으로 수락하지 않습니다. 화면의 프롬프트에 따라 다음 작업을 결정합니다.

자동 수락 변경 사항을 사용하려면 먼저 테넌트가 **Security Devices(**보안 디바이스**)** 페이지의 Conflict Detection(충돌 탐지) 메뉴에서 자동 수락 옵션을 표시하도록 활성화합니다. 그런 다음 개별 디바이스에 대한 변경 사항 자동 수락을 활성화합니다.온프레미스 방화벽 Management Center의 경우 **Services(**서비스**)** 페이지에서 **Administration(**관리**)** > **Integration(**통합**)** > **Firewall Management Center** 로 이동하고 FMC를 선택하여 이 작업을 수행할 수 있습니다.

Security Cloud Control가 대역 외 변경 사항을 탐지하지만 수동으로 수락하거나 거부할 수 있는 옵션을 제공하도록 하려면 대신 충돌 탐지, on page 9를 활성화합니다.

변경 사항 자동 수락 구성

Procedure

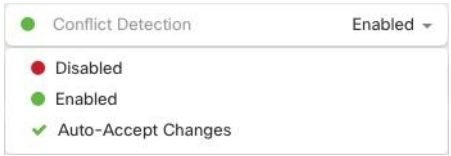
단계 **1** 관리자 또는 슈퍼 관리자 권한이 있는 어카운트를 사용하여 Security Cloud Control에 로그인합니다.

단계 **2** 왼쪽 창에서 **Administration(**관리**)** > **General Settings(**일반 설정**)**를 클릭합니다.

단계 **3** **Tenant Settings(**테넌트 설정**)** 영역에서, 토글을 클릭하여 디바이스 변경 사항을 자동으로 수락하는 옵션 활성화로 전환합니다. 이렇게 하면 변경 사항 자동 수락 메뉴 옵션이 **Security Devices(**보안 디바이스**)** 페이지의 충돌 감지 메뉴에 표시됩니다.

단계 **4** 왼쪽 창에서 보안 디바이스을 클릭하고 대역 외 변경 사항을 자동으로 수락할 디바이스를 선택합니다.

단계 **5** **Conflict Detection(**충돌 감지**)** 메뉴의 드롭다운 메뉴에서 **Auto-Accept Changes(**변경 사항 자동 수락**)**을 선택합니다.



테넌트의 모든 디바이스에 대한 변경 사항 자동 수락 비활성화

Procedure

단계 **1** 관리자 또는 슈퍼 관리자 권한이 있는 어카운트를 사용하여 Security Cloud Control에 로그인합니다.

단계 **2** 왼쪽 창에서 **Administration(**관리**)** > **General Settings(**일반 설정**)**를 클릭합니다.

단계 **3** **Tenant Settings(**테넌트 설정**)** 영역에서 회색 X가 표시되도록 토글을 왼쪽으로 밀어 "디바이스 변경 사항을 자동으로 수락하는 옵션 활성화"를 비활성화합니다. 이렇게 하면 충돌 감지 메뉴에서 변경 사항 자동 수락 옵션이 비활성화되고 테넌트의 모든 디바이스에 대한 기능이 비활성화 됩니다.

Note
"자동 수락"을 비활성화하면 Security Cloud Control에 수락하기 전에 각 디바이스 충돌을 검토해야 합니다. 여기에는 이전에 변경 사항을 자동으로 수락하도록 구성된 디바이스가 포함됩니다.

구성 충돌 해결

이 섹션에서는 디바이스에서 발생하는 구성 충돌을 해결하는 방법에 대한 정보를 제공합니다.

동기화되지 않음 상태 해결

다음 절차를 사용하여 구성 상태가 "동기화되지 않음"인 디바이스를 확인합니다.

Procedure

단계 **1** 탐색 모음에서 보안 디바이스를 클릭합니다.

Note
온프레미스 방화벽 Management Center의 경우, **Administration(**관리**)** > **Integration(**통합**)** > **Firewall Management Center**를 클릭하고 **Not Synced(**동기화되지 않음**)** 상태인 FMC를 선택한 후 5단계부터 계속 진행합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 동기화되지 않은 것으로 보고된 디바이스를 선택합니다.

단계 **5** 오른쪽의 동기화되지 않음 패널에서 다음 중 하나를 선택합니다.

- 미리보기 및 구축**...** - Security Cloud Control에서 디바이스로 구성 변경 사항을 푸시하려면 지금 수행한 변경 사항을 미리 보고 구축하거나 한 번에 여러 변경 사항을 기다렸다가 구축하십시오.
- 변경 사항 취소 - Security Cloud Control에서 디바이스로 구성 변경을 푸시하지 않으려는 경우, 또는 Security Cloud Control에서 시작한 구성 변경을 "취소"하려는 경우. 이 옵션은 Security Cloud Control에 저장된 구성을 디바이스에 저장된 실행 중인 구성으로 덮어씁니다.

충돌 탐지됨 상태 해결

Security Cloud Control를 사용하면 각 라이브 디바이스에서 충돌 탐지를 활성화하거나 비활성화할 수 있습니다. 충돌 탐지, on page 9이 활성화되어 있고 Security Cloud Control를 사용하지 않고 디바이스의 구성을 변경한 경우, 디바이스의 구성 상태는 **Conflict Detected(**충돌 탐지됨**)**로 표시됩니다.

"충돌 탐지됨" 상태를 해결하려면 다음 절차를 수행합니다.

Procedure

단계 **1** 탐색 모음에서 보안 디바이스를 클릭합니다.

Note
온프레미스 방화벽 Management Center의 경우, **Administration(**관리**)** > **Integration(**통합**)** > **Firewall Management Center**를 클릭하고 **Not Synced(**동기화되지 않음**)** 상태인 FMC를 선택한 후 5단계부터 계속 진행합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 충돌을 보고하는 디바이스를 선택하고 오른쪽의 세부 정보 창에서 **Review Conflict(**충돌 검토**)**를 클릭합니다.

단계 **5** **Device Sync(**디바이스 동기화**)** 페이지에서 강조 표시된 차이점을 검토하여 두 구성을 비교합니다.

- "Last Known Device Configuration(마지막으로 알려진 디바이스 구성)" 패널은 Security Cloud Control에 저장된 디바이스 구성입니다.
- "Found on Device(디바이스에서 발견됨)" 패널은 ASA에서 실행 중인 구성에 저장된 구성입니다.

단계 **6** 다음 중 하나를 선택하여 충돌을 해결합니다.

- **Accept Device changes(**디바이스 변경 사항 수락**)**: 구성 및 Security Cloud Control에 저장된 보류 중인 변경 사항을 디바이스의 실행 중인 구성으로 덮어씁니다.

  Note
  Security Cloud Control는 명령줄 인터페이스 외부에서 Cisco IOS 디바이스에 변경 사항을 구축하는 것을 지원하지 않으므로, 충돌을 해결할 때 Cisco IOS 디바이스에 대한 유일한 선택은 **Accept Without Review(**검토 없이 수락**)**를 선택하는 것입니다.

- **Reject Device Changes(**디바이스 변경 거부**)**: 디바이스에 저장된 구성을 Security Cloud Control에 저장된 구성으로 덮어씁니다.

Note
거부되거나 수락된 모든 구성 변경 사항은 변경 로그에 기록됩니다.

디바이스 변경 사항에 대한 폴링 예약

충돌 탐지, on page 9를 활성화했거나 Settings(설정) 페이지에서 **Enable device changes to auto-accept device changes(**디바이스 변경 자동 수락 옵션 활성화**)**를 선택한 경우 Security Cloud Control은 기본 간격 동안 디바이스를 폴링하여 Security Cloud Control 외부에서 디바이스의 구성이 변경되었는지 확인합니다. Security Cloud Control가 디바이스별로 변경 사항을 폴링하는 빈도를 맞춤화할 수 있습니다. 이러한 변경 사항은 둘 이상의 디바이스에 적용할 수 있습니다.

디바이스에 대해 구성된 선택 항목이 없으면 "테넌트 기본값"에 대한 간격이 자동으로 구성됩니다.

Note **Security Devices(**보안 디바이스**)** 페이지에서 디바이스별 간격을 맞춤 설정하면 **General Settings(**일반 설정**)** 페이지에서 Default Conflict Detection Interval(기본 충돌 탐지 간격)로 선택한 폴링 간격이 재정의됩니다.

Security Devices(보안 디바이스**)** 페이지에서 **Conflict Detection(**충돌 탐지**)**을 활성화하거나 Settings(설정) 페이지에서 디바이스 변경 사항을 자동 수락하는 옵션을 활성화한 후 다음 절차를 사용하여 Security Cloud Control가 디바이스를 폴링할 빈도를 예약합니다.

Procedure

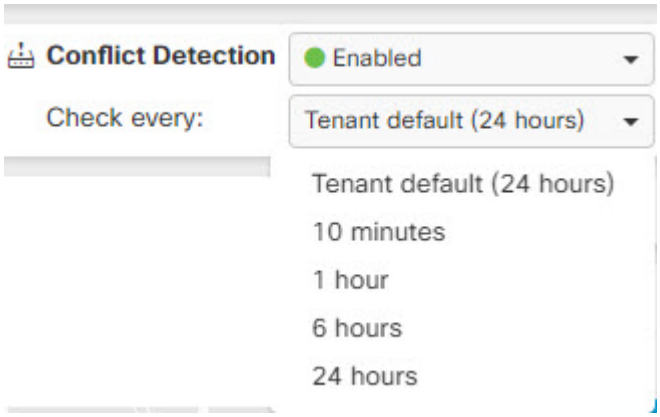
단계 **1** 왼쪽 창에서 보안 디바이스를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 충돌 탐지를 활성화할 디바이스를 선택합니다.

단계 **5** **Conflict Detection(**충돌 탐지**)**과 동일한 영역에서 **Check every(**확인 간격**)**의 드롭다운 메뉴를 클릭하고 원하는 폴링 간격을 선택합니다.



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.