문제 해결

이 장에는 다음 섹션이 포함되어 있습니다.

문제 해결 **Security Cloud Control**

로그인 실패 문제 해결

실수로 잘못된 **Security Cloud Control** 지역에 로그인했기 때문에 로그인에 실패함

적절한 Security Cloud Control 지역에 로그인했는지 확인합니다. https://sign-on.security.cisco.com에 로그인하면 액세스할 지역을 선택할 수 있습니다.https://sign-on.security.cisco.com

로그인해야 하는 지역에 대한 자세한 내용은 다른 지역에서 Security Cloud Control 로그인을 참조하십시오.

마이그레이션 후 로그인 실패 문제 해결

잘못된 사용자 이름 또는 암호로 인해 **Security Cloud Control**에 로그인하지 못함

해결 방법 Security Cloud Control에 로그인하려고 할 때 사용자 이름 및 비밀번호가 올바른 데도 로그인이 실패하는 것을 알고 있거나, "비밀번호를 잊음"를 시도하여 사용 가능한 비밀번호를 복원할 수 없는 경우, 새 Cisco Secure Cloud Sign-On 어카운트을 사용하려면 의 지침에 따라 새 Cisco Secure Cloud Sign-On 어카운트에 등록해야 합니다. 새 Cisco Security Cloud Sign On 어카운트을 등록해야 합니다.

해결 방법 참조: 새 Cisco Secure Cloud Sign On 어카운트 생성 및 Duo 다단계 인증 구성.

Cisco Secure Cloud Sign-On 대시보드 로그인에 성공했지만 **Security Cloud Control**를 실행할 수 없음

해결 방법 Security Cloud Control 테넌트와 다른 사용자 이름으로 Cisco Secure Cloud Sign-On 어카운트를 만들었을 수 있습니다. Security Cloud Control와 Cisco Secure Sign-On 간의 사용자 정보를 표준화하려면 Cisco TAC(Technical Assistance Center)에 문의하십시오.

저장된 북마크를 사용한 로그인 실패

해결 방법 브라우저에 저장한 이전 북마크를 사용하여 로그인을 시도했을 수 있습니다. 북마크는 https://cdo.onelogin.com을 가리킬 수 있습니다.

해결 방법 https://sign-on.security.cisco.com에 로그인합니다.

- 해결 방법 아직 Cisco Secure Sign-On 어카운트을 생성하지 않은 경우 어카운트을 생성합니다.
- 해결 방법 새 Secure Sign-On 어카운트를 만든 경우 대시보드에서 테넌트가 만들어진 지역에 해당하는 Security Cloud Control 타일을 클릭합니다.
  - 해결 방법 Security Cloud Control APJ
  - 해결 방법 Security Cloud Control 호주
  - 해결 방법 Security Cloud Control EU
  - 해결 방법 Security Cloud Control 인도
  - 해결 방법 Security Cloud Control US
- 해결 방법 https://sign-on.security.cisco.com를 가리키도록 즐겨찾기를 업데이트합니다.

액세스 및 인증서 문제 해결

새 핑거프린트 탐지 상태 확인

Procedure

단계 **1** 왼쪽 창에서 보안 디바이스를 클릭합니다.

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

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 새 핑거프린트 감지됨 상태에서 디바이스를 선택합니다.

단계 **5** 새 핑거프린트 감지됨 창에서 핑거프린트 검토를 클릭합니다.

단계 **6** 핑거프린트를 검토하고 수락하라는 메시지가 표시되면

a. **Download Fingerprint(**핑거프린트 다운로드**)**를 클릭하고 검토합니다.

b. 핑거프린트에 만족하면 **Accept(**수락**)**를 클릭합니다. 그렇지 않은 경우 **Cancel(**취소**)**를 클릭합니다.

단계 **7** 새 핑거프린트 문제를 해결한 후 디바이스의 연결 상태가 온라인으로 표시되고 구성 상태가 "동기화되지 않음" 또는 "충돌 감지됨"으로 표시될 수 있습니다. 구성 충돌 해결을 검토하여 Security Cloud Control와 디바이스 간의 구성 차이를 검토하고 해결합니다.

보안 및 분석 로깅 이벤트를 사용하여 네트워크 문제 해결

다음은 이벤트 뷰어를 사용하여 네트워크 문제를 문제 해결하는 데 사용할 수 있는 기본 프레임워크입니다.

이 시나리오에서는 네트워크 운영 팀에서 사용자가 네트워크의 리소스에 액세스할 수 없다는 보고를 받은 것으로 가정합니다. 문제를 보고하는 사용자와 해당 위치를 기반으로, 네트워크 운영 팀은 어떤 방화벽이 리소스에 대한 액세스를 제어하는지를 합리적으로 파악합니다.

Note 또한 이 시나리오에서는 FDM 관리 디바이스가 네트워크 트래픽을 관리하는 방화벽이라고 가정합니다. Security Analytics and Logging(보안 분석 및 로깅)은 다른 디바이스 유형에서 로깅 정보를 수집하지 않습니다.

Procedure

단계 **1** 왼쪽 창에서 **Events & Logs(**이벤트 및 로그**)** > **Events(**이벤트**)** > **Event Logging(**이벤트 로깅**)**를 클릭합니다.

단계 **2** 기록 탭을 클릭합니다.

단계 **3** 시간 범위를 기준으로 이벤트 필터링을 시작합니다. 기본적으로 Historical(기록) 탭에는 이벤트의 마지막 시간이 표시됩니다. 올바른 시간 범위인 경우 현재 날짜와 시간을 **End(**종료**)** 시간으로 입력합니다. 올바른 시간 범위가 아닌 경우 보고된 문제의 시간을 포함하는 시작 및 종료 시간을 입력합니다.

단계 **4** **Sensor ID(**센서 **ID)** 필드에 사용자의 액세스를 제어하는 것으로 의심되는 방화벽의 IP 주소를 입력합니다. 방화벽이 두 개 이상인 경우 검색 창에서 속성**:**값 쌍을 사용하여 이벤트를 필터링합니다. 두 항목을 만들고 OR 문으로 결합합니다. 예: `SensorID:192.168.10.2 OR SensorID:192.168.20.2`.

단계 **5** Events(이벤트) 필터 표시줄의 **Source IP(**소스 **IP)** 필드에 사용자의 IP 주소를 입력합니다.

단계 **6** 사용자가 리소스에 액세스할 수 없는 경우 **Destination IP(**대상 **IP)** 필드에 해당 리소스의 IP 주소를 입력해 보십시오.

단계 **7** 결과에서 이벤트를 확장하고 세부 정보를 확인합니다. 다음은 몇 가지 세부 사항입니다.

- **AC_RuleAction** - 규칙이 트리거될 때 수행된 작업(허용, 신뢰, 차단).
- **FirewallPolicy** - 이벤트를 트리거한 규칙이 상주하는 정책입니다.
- **FirewallRule** - 이벤트를 트리거한 규칙의 이름입니다. 값이 Default Action(기본 작업)인 경우 정책의 규칙 중 하나가 아니라 이벤트를 트리거한 것은 정책의 기본 작업입니다.
- **UserName** - 이니시에이터 IP 주소와 연결된 사용자입니다. 이니시에이터 IP 주소는 소스 IP 주소와 동일합니다.

단계 **8** 규칙 작업이 액세스를 차단하는 경우 FirewallRule 및 FirewallPolicy 필드를 확인하여 액세스를 차단하는 정책의 규칙을 식별합니다.

SSL 암호 해독 문제 해결

재서명 암호 해독이 브라우저에서는 작동하지만 앱에서는 작동하지 않는 웹 사이트 처리**(SSL** 또는 인증 기관 피닝**)**

스마트폰 및 기타 디바이스용 일부 앱은 SSL(또는 인증 기관) 피닝이라는 기술을 사용합니다. SSL 피닝 기술은 원래 서버 인증서의 해시를 앱 자체에 포함합니다. 따라서 앱이 Firepower Threat Defense 디바이스에서 재서명된 인증서를 받으면 해시 검증에 실패하고 연결이 중단됩니다.

이때 기본적인 증상은 사용자가 사이트 앱을 사용해서는 웹 사이트에 연결할 수 없지만 웹 브라우저를 사용하면 연결할 수 있다는 것입니다(앱으로 연결에 실패한 디바이스에서 브라우저를 사용할 때도 연결 가능). 예를 들어 사용자는 Facebook iOS 또는 Android 앱을 사용할 수 없지만 Safari 또는 Chrome을 https://www.facebook.com으로 지정하고 성공적으로 연결할 수 있습니다.

SSL 피닝은 특별히 메시지 가로채기(man-in-the-middle) 공격을 차단하는 데 사용되므로 이러한 현상을 해결하는 방법은 없습니다. 다음 옵션 중에서 선택해야 합니다.

기타 세부정보

특정 사이트가 브라우저에서는 작동하는데 동일 디바이스의 앱에서는 작동하지 않는 경우 SSL 피닝 인스턴스를 살펴봐야 합니다. 하지만 심층적으로 확인하려면 연결 이벤트를 사용해 브라우저 테스트와 더불어 SSL 피닝을 확인할 수 있습니다.

앱은 두 가지 방식으로 해시 검증 장애를 처리할 수 있습니다.

- Facebook 등의 그룹 1 앱은 서버에서 SH, CERT, SHD 메시지를 받는 즉시 SSL ALERT 메시지를 보냅니다. Alert는 보통 SSL 피닝을 나타내는 "Unknown CA (48)(알 수 없는 CA(48))" 알림입니다. 알림 메시지 후에는 TCP Reset(TCP 재설정)이 전송됩니다. 이벤트 세부사항에는 다음 증상이 표시됩니다.
  - SSL Flow Flag(SSL 플로우 플래그)에는 ALERT_SEEN이 포함되어 있습니다.
  - SSL Flow Flag(SSL 플로우 플래그)에는 APP_DATA_C2S 또는 APP_DATA_S2C가 포함되어 있지 않습니다.
  - SSL Flow Message(SSL 플로우 메시지)는 보통 CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE입니다.
- Dropbox 등의 그룹 2 앱은 알림을 보내지 않습니다. 대신 핸드셰이크가 완료될 때까지 기다렸다가 TCP Reset(TCP 재설정)을 전송합니다. 이벤트에는 다음 증상이 표시됩니다.
  - SSL Flow Flag(SSL 플로우 플래그)에는 ALERT_SEEN, APP_DATA_C2S 또는 APP_DATA_S2C가 포함되어 있지 않습니다.
  - SSL Flow Message(SSL 플로우 메시지)는 보통 CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE, CLIENT_KEY_EXCHANGE, CLIENT_CHANGE_CIPHER_SPEC, CLIENT_FINISHED, SERVER_CHANGE_CIPHER_SPEC, SERVER_FINISHED입니다.

마이그레이션 후 로그인 실패 문제 해결

잘못된 사용자 이름 또는 암호로 인해 **Security Cloud Control**에 로그인하지 못함

해결 방법 Security Cloud Control에 로그인하려고 할 때 사용자 이름 및 비밀번호가 올바른 데도 로그인이 실패하는 것을 알고 있거나, "비밀번호를 잊음"를 시도하여 사용 가능한 비밀번호를 복원할 수 없는 경우, 새 Cisco Secure Cloud Sign-On 어카운트을 사용하려면 의 지침에 따라 새 Cisco Secure Cloud Sign-On 어카운트에 등록해야 합니다. 새 Cisco Security Cloud Sign On 어카운트을 등록해야 합니다.

해결 방법 참조: 새 Cisco Secure Cloud Sign On 어카운트 생성 및 Duo 다단계 인증 구성.

Cisco Secure Cloud Sign-On 대시보드 로그인에 성공했지만 **Security Cloud Control**를 실행할 수 없음

해결 방법 Security Cloud Control 테넌트와 다른 사용자 이름으로 Cisco Secure Cloud Sign-On 어카운트를 만들었을 수 있습니다. Security Cloud Control와 Cisco Secure Sign-On 간의 사용자 정보를 표준화하려면 Cisco TAC(Technical Assistance Center)에 문의하십시오.

저장된 북마크를 사용한 로그인 실패

해결 방법 브라우저에 저장한 이전 북마크를 사용하여 로그인을 시도했을 수 있습니다. 북마크는 https://cdo.onelogin.com을 가리킬 수 있습니다.

해결 방법 https://sign-on.security.cisco.com에 로그인합니다.

- 해결 방법 아직 Cisco Secure Sign-On 어카운트을 생성하지 않은 경우 어카운트을 생성합니다.
- 해결 방법 새 Secure Sign-On 어카운트를 만든 경우 대시보드에서 테넌트가 만들어진 지역에 해당하는 Security Cloud Control 타일을 클릭합니다.
  - 해결 방법 Security Cloud Control APJ
  - 해결 방법 Security Cloud Control 호주
  - 해결 방법 Security Cloud Control EU
  - 해결 방법 Security Cloud Control 인도
  - 해결 방법 Security Cloud Control US
- 해결 방법 https://sign-on.security.cisco.com를 가리키도록 즐겨찾기를 업데이트합니다.

개체 문제 해결

중복 개체 문제 해결

중복 개체 ⧉는 이름은 다르지만 값은 동일한 디바이스에 있는 두 개 이상의 개체입니다. 이러한 개체는 대개 실수로 생성되고 유사한 용도로 사용되며 다른 정책에서 사용됩니다. 중복 개체 문제를 해결한 후 Security Cloud Control는 유지된 개체 이름으로 영향을 받는 모든 개체 참조를 업데이트합니다.

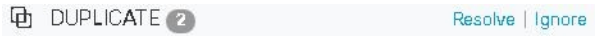
중복 개체 문제를 해결하려면 다음을 수행합니다.

Procedure

단계 **1** 왼쪽 창에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 그런 다음 개체를 필터링하여 중복 개체 문제를 찾습니다.

단계 **3** 결과 중 하나를 선택합니다. 개체 세부 정보 패널에 영향을 받는 중복 수가 포함된 DUPLICATE 필드가 표시됩니다.



단계 **4** **Resolve(**확인**)**를 클릭합니다. Security Cloud Control는 비교할 중복 개체를 표시합니다.

단계 **5** 비교할 두 개체를 선택합니다.

단계 **6** 이제 다음과 같은 옵션이 제공됩니다.

- 개체 중 하나를 다른 개체로 교체하려면 유지할 개체에 대해 **Pick(**선택**)**을 클릭하고 **Resolve(**확인**)**를 클릭하여 영향을 받을 디바이스 및 네트워크 정책을 확인한 다음, 변경 사항이 마음에 들면 **Confirm(**확인**)**를 클릭합니다. Security Cloud Control는 대체물로 선택한 개체를 유지하고 중복을 삭제합니다.
- 목록에 무시할 개체가 있는 경우 **Ignore(**무시**)**를 클릭합니다. 개체를 무시하면 Security Cloud Control에 표시되는 중복 개체 목록에서 제거됩니다.
- 개체는 유지하지만 Security Cloud Control가 중복 개체를 검색할 때 찾지 않도록 하려면 **Ignore All(**모두 무시**)**를 클릭합니다.

단계 **7** 중복 개체 문제가 해결되면 지금 변경 사항을 검토하고 구축하거나, 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

사용되지 않는 개체 문제 해결

사용되지 않는 개체는 디바이스 구성에 존재하지만 다른 개체, 액세스 목록 또는 NAT 규칙에서 참조하지 않는 개체입니다.

관련 정보**:**

- 디바이스 및 서비스 목록 내보내기
- Security Cloud Control에 디바이스 대량 재연결

사용되지 않는 개체 문제 해결

Procedure

단계 **1** 왼쪽 창에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 그런 다음 개체를 필터링하여 사용하지 않는 개체 문제를 찾습니다.

단계 **3** 하나 이상의 사용되지 않는 개체를 선택합니다.

단계 **4** 이제 다음과 같은 옵션이 제공됩니다.

- Actions(작업) 창에서 **Remove(**제거**)** 를 클릭하여 Security Cloud Control에서 사용되지 않는 개체를 제거합니다.
- Issues(문제) 창에서 **Ignore(**무시**)**를 클릭합니다. 개체를 무시하면 Security Cloud Control는 사용되지 않는 개체의 결과에 해당 개체를 표시하지 않습니다.

단계 **5** 사용되지 않는 개체를 제거한 경우, 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축지금 변경한 사항을 수행하거나 대기하고 여러 변경 사항을 한 번에 구축합니다.

Note
사용되지 않는 개체 문제를 벌크로 해결하려면 개체 문제 벌크로 해결을 참조하십시오.

사용되지 않는 개체 대량 제거

Procedure

단계 **1** 왼쪽 창에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 그런 다음 개체를 필터링하여 사용하지 않는 개체 문제를 찾습니다.

단계 **3** 삭제하려는 사용되지 않는 개체를 선택합니다.

- 개체 테이블 헤더 행의 확인란을 클릭하여 페이지의 모든 개체를 선택합니다.
- 개체 테이블에서 사용하지 않는 개별 개체를 선택합니다.

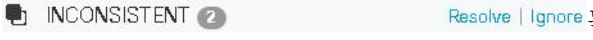
단계 **4** 오른쪽의 작업 창에서 **Remove(**제거**)** 를 클릭하여 Security Cloud Control에서 선택한 사용되지 않는 개체를 모두 제거합니다. 한 번에 99개의 개체를 제거할 수 있습니다.

단계 **5** **OK(**확인**)**을 클릭하여 사용하지 않는 개체를 삭제할 것인지 확인합니다.

단계 **6** 이러한 변경 사항을 구축하기 위한 두 가지 선택 사항이 있습니다.

- 지금 변경한 내용을 검토 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.
- 보안 디바이스 페이지를 열고 변경의 영향을 받은 디바이스를 찾습니다. 변경의 영향을 받는 모든 디바이스를 선택하고 관리 창에서 **Deploy All(**모두 구축**)** 를 클릭합니다. 경고를 읽고 적절한 조치를 취합니다.

불일치 개체 문제 해결

불일치 개체 

는 두 개 이상의 디바이스에서 이름은 같지만 값이 다른 개체입니다. 사용자가 동일한 이름 및 콘텐츠를 사용하여 서로 다른 구성에서 개체를 생성하지만 시간이 지남에 따라 이러한 개체의 값이 달라지므로 불일치가 발생하는 경우가 있습니다.

참고: 일관되지 않은 개체 문제를 벌크로 해결하려면 개체 문제 벌크로 해결을 참조하십시오.

일치하지 않는 개체에 대해 다음을 수행할 수 있습니다.

- **Ignore(**무시**)**: Security Cloud Control가 개체 간의 불일치를 무시하고 해당 값을 유지합니다. 개체가 더 이상 불일치 범주에 나열되지 않습니다.
- **Merge(**병합**)**: Security Cloud Control가 선택한 모든 개체와 해당 값을 단일 개체 그룹으로 결합합니다.
- **Rename(**이름 변경**):** Security Cloud Control를 사용하면 일치하지 않는 개체 중 하나의 이름을 바꾸고 새 이름을 지정할 수 있습니다.
- **Convert Shared Network Objects to Overrides(**공유 네트워크 개체를 재정의로 변환**)**: Security Cloud Control를 사용하면 일관성이 없는 공유 개체(재정의가 있거나 없는)를 재정의가 있는 단일 공유 개체로 결합할 수 있습니다. 일치하지 않는 개체의 가장 일반적인 기본값은 새로 형성된 개체의 기본값으로 설정됩니다.

Note 공통 기본값이 여러 개인 경우 그 중 하나가 기본값으로 선택됩니다. 나머지 기본값 및 재정의 값은 해당 개체의 재정의로 설정됩니다.

- **Convert Shared Network Group to Additional Values(**공유 네트워크 그룹을 추가 값으로 변환**):** - Security Cloud Control를 사용하면 일치하지 않는 공유 네트워크 그룹을 추가 값이 있는 단일 공유 네트워크 그룹으로 결합할 수 있습니다. 이 기능의 기준은 변환할 일관되지 않은 네트워크 그룹에 동일한 값을 가진 공통 개체가 하나 이상 있어야 한다는 것입니다. 이 기준과 일치하는 모든 기본값은 기본값이 되며, 나머지 개체는 새로 형성된 네트워크 그룹의 추가 값으로 할당됩니다.

  예를 들어, 일치하지 않는 두 개의 공유 네트워크 그룹을 고려하십시오. 첫 번째 네트워크 그룹 'shared_network_group'은 'object_1'(192.0.2.x) 및 'object_2'(192.0.2.y)로 구성됩니다. 여기에는 추가 값 'object_3'(192.0.2.a)도 포함됩니다. 두 번째 네트워크 그룹 'shared_network_group'은 'object_1'(192.0.2.x) 및 추가 값 'object_4'(192.0.2.b)로 구성됩니다. 공유 네트워크 그룹을 추가 값으로 변환할 때 새로 형성된 그룹 'shared_network_group'에는 'object_1'(192.0.2.x) 및 'object_2'(192.0.2.y)'가 포함되며, 'object_3'(192.0. 2.a) 및 'object_4'(192.0.2.b)를 추가 값으로 사용합니다.

Note 새 네트워크 개체를 생성하면 Security Cloud Control는 자동으로 해당 값을 동일한 이름의 기존 공유 네트워크 개체에 재정의로 할당합니다. 이는 새 디바이스가 Security Cloud Control에 온보딩된 경우에도 적용됩니다.

자동 할당은 다음 기준을 충족하는 경우에만 발생합니다.

1. 새 네트워크 개체를 디바이스에 할당해야 합니다.
2. 이름과 유형이 같은 공유 개체는 테넌트에 하나만 있어야 합니다.
3. 공유 개체에 이미 재정의가 포함되어 있어야 합니다.

일관성 없는 개체 문제를 해결하려면 다음을 수행합니다.

Procedure

단계 **1** 왼쪽의 Security Cloud Control 탐색 모음에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 그런 다음 개체를 필터링하여 일관성 없는 개체 문제를 찾습니다.

단계 **3** 일치하지 않는 개체를 선택합니다. 개체 세부 정보 패널에 영향을 받는 개체의 수가 포함된 INCONSISTENT 필드가 표시됩니다.

단계 **4** **Resolve(**확인**)**를 클릭합니다. Security Cloud Control는 비교할 중복 개체를 표시합니다.

단계 **5** 이제 다음과 같은 옵션이 제공됩니다.

- 모두 무시**:**
  a. 표시된 개체를 비교하고 개체 중 하나에서 **Ignore(**무시**)**를 클릭합니다. 또는 모든 개체를 무시하려면 **Ignore All(**모두 무시**)**을 클릭합니다.
  b. **OK(**확인**)**를 클릭하여 확인합니다.
- 개체를 병합하여 해결합니다**.**
  a. **Resolve by Merging X Objects(X**개 개체를 병합하여 해결**)**를 클릭합니다.
  b. **OK(**확인**)**를 클릭합니다.
- **Rename(**이름 바꾸기**):**
  a. **Rename(**이름 변경**)**을 클릭합니다.
  b. 영향을 받는 네트워크 정책 및 디바이스에 변경 사항을 저장하고 **Confirm(**확인**)**을 클릭합니다.
- **Convert to Overrides(**재정의로 변환**)(**일치하지 않는 공유 개체의 경우**)**: 공유 개체를 재정의와 비교할 때, 비교 패널의 **Inconsistent Values(**일관되지 않는 값**)** 필드에 기본값만 표시됩니다.
  a. **Convert to Overrides(**재정의로 변환**)**를 클릭합니다. 일치하지 않는 모든 개체는 재정의가 포함된 단일 공유 개체로 변환됩니다.
  b. **OK(**확인**)**를 클릭합니다. **Edit Shared Object(**공유 개체 편집**)**를 클릭하여 새로 형성된 개체의 세부 정보를 볼 수 있습니다. 위쪽 및 아래쪽 화살표를 사용하여 기본값과 재정의 간에 값을 이동할 수 있습니다.
- **Convert to Additional Values(**추가 값으로 변환**)(**일치하지 않는 네트워크 그룹의 경우**):**
  a. **Convert to Additional Values(**추가 값으로 변환**)**를 클릭합니다. 일치하지 않는 모든 개체는 추가 값이 있는 단일 공유 개체로 변환됩니다.
  b. 영향을 받는 네트워크 정책 및 디바이스에 변경 사항을 저장하고 **Confirm(**확인**)**을 클릭합니다.

단계 **6** 불일치를 해결한 후 변경 사항을 검토하고 지금 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

대량의 개체 문제 해결

사용되지 않거나 중복되거나 불일치 개체 문제 해결, on page 7 문제가 있는 개체를 해결하는 한 가지 방법은 이러한 개체를 무시하는 것입니다. 개체에 둘 이상의 문제가 있더라도 여러 개체를 선택하고 무시할 수 있습니다. 예를 들어 개체가 일치하지 않고 사용되지 않는 경우 한 번에 하나의 문제 유형만 무시할 수 있습니다.

Important 나중에 개체가 다른 문제 유형과 연결될 경우 커밋한 무시 작업은 해당 시점에 선택한 문제에만 영향을 미칩니다. 예를 들어, 개체가 중복되었기 때문에 개체를 무시했고 개체가 나중에 일치하지 않는 것으로 표시되는 경우, 중복 개체로 무시한다고 해서 일치하지 않는 개체로 무시되는 것은 아닙니다.

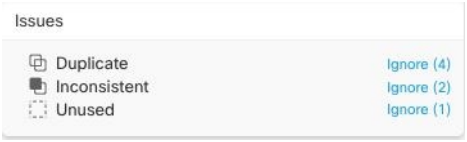
대량으로 문제를 무시하려면 다음 절차를 수행합니다.

Procedure

단계 **1** 왼쪽 창에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 검색 범위를 좁히기 위해 개체 문제를 필터링할 수 있습니다.

단계 **3** Object(개체) 테이블에서 무시할 적용 가능한 모든 개체를 선택합니다. Issues(문제) 창은 문제 유형별로 개체를 그룹화합니다.



단계 **4** 유형별로 문제를 무시하려면 **Ignore(**무시**)**를 클릭합니다. 각 문제 유형을 개별적으로 무시해야 합니다.

단계 **5** **OK(**확인**)**를 클릭하여 해당 개체를 무시할 것임을 확인합니다.

디바이스 연결 상태

Security Cloud Control 테넌트에 온보딩된 디바이스의 연결 상태를 볼 수 있습니다. 이 항목은 다양한 연결 상태를 이해하는 데 도움이 됩니다. **Security Devices(**보안 디바이스**)** 페이지에서 **Connectivity(**연결성**)** 열은 디바이스 연결 상태를 표시합니다.

디바이스 연결 상태가 '온라인'이면 디바이스의 전원이 켜져 있고 Security Cloud Control에 연결되어 있음을 의미합니다. 아래 표에 설명된 다른 상태는 일반적으로 여러 가지 이유로 디바이스에 문제가 발생할 때 발생합니다. 이 표는 이러한 문제에서 복원하는 방법을 제공합니다. 연결 실패를 일으키는

문제가 두 개 이상 있을 수 있습니다. 다시 연결을 시도하면, Security Cloud Control는 다시 연결을 수행하기 전에 먼저 이러한 모든 문제를 편집하라는 메시지를 표시합니다.

디바이스 연결 상태	가능한 이유	해결 방법
온라인	디바이스의 전원이 켜져 있고 Security Cloud Control에 연결되어 있습니다.	해당 없음
오프라인	디바이스의 전원이 꺼졌거나 네트워크 연결이 끊겼습니다.	디바이스가 오프라인 상태인지 확인합니다.
불충분한 라이선스	디바이스에 충분한 라이선스가 없습니다.	라이선스 부족 문제 해결, on page 11
유효하지 않은 자격 증명	디바이스에 연결하기 위해 Security Cloud Control에서 사용하는 사용자 이름과 암호 조합이 올바르지 않습니다.	유효하지 않은 자격 증명 문제 해결, on page 12
온보딩	디바이스 온보딩이 시작되었지만 완료되지 않았습니다.	디바이스의 연결을 확인하고 디바이스 등록을 완료해야 합니다.
Unknown	디바이스 온보딩에 실패했으며 Security Cloud Control에서 디바이스의 연결성 상태를 가져올 수 없습니다.	보안 디바이스 페이지에서 디바이스를 선택하고 오른쪽 창에서 **Check for Changes(**변경 사항 확인**)**를 선택하여 디바이스에서 최신 구성 가져오기를 시도합니다.
새 인증서 탐지됨	디바이스의 인증서가 변경되었습니다. 디바이스가 자체 서명된 인증서를 사용하는 경우 디바이스의 전원을 껐다 켜서 이 문제가 발생했을 수 있습니다.	새 인증서 문제 해결, on page 13
온보딩 오류	Security Cloud Control는 디바이스를 온보딩할 때 디바이스와의 연결이 끊어졌을 수 있습니다.	온보딩 오류 문제 해결, on page 22

라이선스 부족 문제 해결

디바이스 연결 상태가 "Insufficient License(라이선스 부족)"로 표시되면 다음을 수행합니다.

- 디바이스가 라이선스를 획득할 때까지 잠시 기다립니다. 일반적으로 Cisco Smart Software Manager가 디바이스에 새 라이선스를 적용하는 데 시간이 걸립니다.

- 디바이스 상태가 변경되지 않으면 Security Cloud Control에서 로그아웃하고 다시 로그인하여 Security Cloud Control 포털을 새로 고침한 후 라이선스 서버와 디바이스 간의 네트워크 통신 문제를 해결합니다.
- 포털을 새로 고침해도 디바이스 상태가 변경되지 않으면 다음을 수행합니다.

Procedure

단계 **1** Cisco Smart Software Manager에서 새 토큰을 생성하고 복사합니다. 자세한 내용은 스마트 라이선싱 생성 동영상를 참조하십시오.

단계 **2** 왼쪽 창에서 보안 디바이스를 클릭합니다.

단계 **3** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **4** 적절한 디바이스 유형 탭을 클릭하고 **Insufficient License(**라이선스 부족**)** 상태의 디바이스를 선택합니다.

단계 **5** **Device Details(**디바이스 세부 정보**)** 창에서 **Insufficient Licenses(**불충분한 라이선스**)**에 표시되는 **Manage Licenses(**라이선스 관리**)**를 클릭합니다. **Manage Licenses(**라이선스 관리**)** 창이 나타납니다.

단계 **6** 활성화 필드에 새 토큰을 붙여넣고 디바이스 등록를 클릭합니다.

토큰이 디바이스에 성공적으로 적용되면 연결 상태가 온라인으로 바뀝니다.

유효하지 않은 자격 증명 문제 해결

유효하지 않은 자격 증명으로 인한 디바이스 연결 끊김을 해결하려면 다음을 수행합니다.

Procedure

단계 **1** 왼쪽 창에서 보안 디바이스를 클릭합니다.

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

단계 **3** 적절한 디바이스 유형 탭을 클릭하고 **Invalid Credentials(**유효하지 않은 자격 증명**)** 상태의 디바이스를 선택합니다.

단계 **4** **Device Details(**디바이스 세부 정보**)** 창에서 **Invalid Credentials(**잘못된 자격 증명**)**에 나타나는 **Reconnect(**재연결**)**을 클릭합니다. Security Cloud Control가 디바이스에 재연결을 시도합니다.

단계 **5** 프롬프트가 나타나면 Linux 사용자 이름 및 비밀번호를 입력합니다.

단계 **6** **Continue(**계속**)**를 클릭합니다.

단계 **7** 디바이스가 온라인 상태가 되고 사용할 준비가 되면 **Close(**닫기**)**를 클릭합니다.

단계 **8** Security Cloud Control가 잘못된 자격 증명을 사용하여 디바이스에 연결하려고 시도했기 때문에 Security Cloud Control가 디바이스에 연결하는 데 사용해야 하는 사용자 이름 및 비밀번호 조합이 디바이스에서 직접 변경되었을 수 있습니다. 이제 디바이스가 "Online(온라인)"이지만 구성 상태가 "Conflict Detected(충돌 탐지됨)"인 것을 확인할

수 있습니다. Resolve Configuration Conflicts(구성 충돌 해결)를 사용하여 Security Cloud Control와 디바이스 간의 구성 차이를 검토하고 해결합니다.

새 인증서 문제 해결

Security Cloud Control의 인증서 사용

Security Cloud Control는 디바이스에 연결할 때 인증서의 유효성을 확인합니다. 특히 Security Cloud Control는 다음을 요구합니다.

1. 디바이스에서 1.0 이상의 TLS 버전을 사용합니다.
2. 디바이스에서 제시한 인증서가 만료되지 않았으며 발급 날짜가 과거입니다(즉, 이미 유효하며 나중에 유효해질 예정이 아님).
3. 인증서는 SHA-256 인증서여야 합니다. SHA-1 인증서는 허용되지 않습니다.
4. 다음 조건 중 하나가 참입니다.
   - 디바이스가 자체 서명 인증서를 사용하며, 인증된 사용자가 신뢰하는 최신 인증서와 동일합니다.
   - 디바이스는 신뢰할 수 있는 CA(Certificate Authority)에서 서명한 인증서를 사용하며, 제공된 리프 인증서를 관련 CA에 연결하는 인증서 체인을 제공합니다.

다음은 Security Cloud Control가 브라우저와 다른 방식으로 인증서를 사용하는 방법입니다.

- 자체 서명 인증서의 경우 Security Cloud Control는 도메인 이름 확인을 재정의하며, 그 대신 디바이스 온보딩 또는 재연결 중에 인증된 사용자가 신뢰하는 인증서와 인증서가 정확히 일치하는지 확인합니다.
- Security Cloud Control는 아직 내부 CA를 지원하지 않습니다. 현재는 내부 CA가 서명한 인증서를 확인할 수 있는 방법이 없습니다.

  디바이스별로 ASA 디바이스에 대한 인증서 확인을 비활성화할 수 있습니다. Security Cloud Control에서 ASA의 인증서를 신뢰할 수 없는 경우 해당 디바이스에 대한 인증서 검사를 비활성화할 수 있습니다. 디바이스에 대한 인증서 확인을 비활성화하려고 시도했지만 여전히 디바이스를 온보딩할 수 없는 경우, 디바이스에 대해 지정한 IP 주소 및 포트가 잘못되었거나 연결할 수 없는 것일 수 있습니다. 인증서 검사를 전역적으로 비활성화하거나 지원되는 인증서가 있는 디바이스에 대한 인증서 검사를 비활성화할 수 있는 방법은 없습니다. 비 ASA 디바이스에 대한 인증서 확인을 비활성화할 수 있는 방법은 없습니다.

  디바이스에 대한 인증서 확인을 비활성화하면 Security Cloud Control은 TLS를 사용하여 디바이스에 연결하지만 연결을 설정하는 데 사용된 인증서를 검증하지 않습니다. 즉, 수동적인 중간자 공격자는 연결을 도청할 수 없지만, 활성 상태의 중간자 공격자는 Security Cloud Control에 유효하지 않은 인증서를 제공하여 연결을 가로챌 수 있습니다.

인증서 문제 식별

Security Cloud Control가 디바이스를 온보딩하지 못할 수 있는 몇 가지 이유가 있습니다. UI에 "Security Cloud Control cannot connect to the device using the certificate presented(제공된 인증서를 사용하여 디바이스에 연결할 수 없음)"라는 메시지가 표시되면 인증서에 문제가 있는 것입니다. UI에 이 메시지가 표시되지 않으면 연결 문제(디바이스에 연결할 수 없음) 또는 기타 네트워크 오류와 관련이 있을 가능성이 높습니다.

Security Cloud Control가 지정된 인증서를 거부하는 이유를 확인하려면 SDC 호스트 또는 관련 디바이스에 연결할 수 있는 다른 호스트에서 openssl 명령줄 툴을 사용할 수 있습니다. 다음 명령을 사용하여 디바이스에서 제공하는 인증서를 보여주는 파일을 생성합니다.

```
openssl s_client -showcerts -connect <host>:<port> &> <filename>.txt
```

이 명령은 인터랙티브 세션을 시작하므로 몇 초 후에 종료하려면 Ctrl-c를 사용해야 합니다.

이제 다음과 같은 출력이 포함된 파일이 생성됩니다.

```
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify return:1
depth=1 C = US, O = Google Inc, CN = Google Internet Authority G2
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google Inc, CN = *.google.com
verify return:1 CONNECTED(00000003)
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
  i:/C=US/O=Google Inc/CN=Google Internet Authority G2
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
  i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
  i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE-----
---
Server certificate
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: ECDH, P-256, 256 bits

---
SSL handshake has read 4575 bytes and written 434 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit Secure Renegotiation IS supported
Compression: NONE
```

```
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol : TLSv1.2
    Cipher : ECDHE-RSA-AES128-GCM-SHA256
    Session-ID: 48F046F3360225D51BE3362B50CE4FE8DB6D6B80B871C2A6DD5461850C4CF5AB
    Session-ID-ctx:
    Master-Key:
9A9CCBAA4F5A25B95C37EF7C6870F8C5DD3755A9A7B4CCE4535190B793DEFF53F94203AB0A62F9F70B9099FBFEBAB1B6

    Key-Arg : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 100800 (seconds)
    TLS session ticket:
    0000 - 7a eb 54 dd ac 48 7e 76-30 73 b2 97 95 40 5b de z.T..H~v0s...@[.
    0010 - f3 53 bf c8 41 36 66 3e-5b 35 a3 03 85 6f 7d 0c .S..A6f>[5...o}.
    0020 - 4b a6 90 6f 95 e2 ec 03-31 5b 08 ca 65 6f 8f a6 K..o....1[..eo..
    0030 - 71 3d c1 53 b1 29 41 fc-d3 cb 03 bc a4 a9 33 28 q=.S.)A.......3(
    0040 - f8 c8 6e 0a dc b3 e1 63-0e 8f f2 63 e6 64 0a 36 ..n....c...c.d.6
    0050 - 22 cb 00 3a 59 1d 8d b2-5c 21 be 02 52 28 45 9d "..:Y...\!..R(E.
    0060 - 72 e3 84 23 b6 f0 e2 7c-8a a3 e8 00 2b fd 42 1d r..#...|....+.B.
    0070 - 23 35 6d f7 7d 85 39 1c-ad cd 49 f1 fd dd 15 de #5m.}.9...I.....
    0080 - f6 9c ff 5e 45 9c 7c eb-6b 85 78 b5 49 ea c4 45 ...^E.|.k.x.I..E
    0090 - 6e 02 24 1b 45 fc 41 a2-87 dd 17 4a 04 36 e6 63 n.$.E.A....J.6.c
    00a0 - 72 a4 ad
    00a4 - <SPACES/NULS> Start Time: 1476476711 Timeout : 300 (sec)
Verify return code: 0 (ok)
---
```

이 출력에서 가장 먼저 확인할 사항은 반환 코드 확인이 표시되는 마지막 줄입니다. 인증서 문제가 있는 경우 반환 코드는 0이 아니며 오류에 대한 설명이 표시됩니다.

일반적인 오류 및 해결 방법을 보려면 이 인증서 오류 코드 목록을 확장합니다.

0 X509_V_OK 작업에 성공했습니다.

2 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT 신뢰할 수 없는 인증서의 발급자 인증서를 찾을 수 없습니다.

3 X509_V_ERR_UNABLE_TO_GET_CRL 인증서의 CRL을 찾을 수 없습니다.

4 X509_V_ERR_UNABLE_TO_DECRYPT_CERT_SIGNATURE 인증서 서명을 해독할 수 없습니다. 이는 실제 서명 값이 예상 값과 일치하지 않는 것이 아니라 확인할 수 없음을 의미합니다. 이는 RSA 키에만 의미가 있습니다.

5 X509_V_ERR_UNABLE_TO_DECRYPT_CRL_SIGNATURE CRL 서명을 해독할 수 없습니다. 이는 실제 서명 값이 예상 값과 일치하지 않는 것이 아니라 확인할 수 없음을 의미합니다. 사용되지 않음.

6 X509_V_ERR_UNABLE_TO_DECODE_ISSUER_PUBLIC_KEY 인증서 SubjectPublicKeyInfo의 공개 키를 읽을 수 없습니다.

7 X509_V_ERR_CERT_SIGNATURE_FAILURE 인증서의 서명이 유효하지 않습니다.

8 X509_V_ERR_CRL_SIGNATURE_FAILURE 인증서의 서명이 유효하지 않습니다.

9 X509_V_ERR_CERT_NOT_YET_VALID 인증서가 아직 유효하지 않습니다. notBefore 날짜가 현재 시간 이후입니다. 자세한 내용은 아래의 반환 코드 확인: 9(인증서가 아직 유효하지 않음)를 참조하십시오.

10 X509_V_ERR_CERT_HAS_EXPIRED 인증서가 만료되었습니다. 즉, notAfter 날짜는 현재 시간 이전입니다. 자세한 내용은 아래의 반환 코드 확인: 10(인증서가 만료되었습니다)을 참조하십시오.

11 X509_V_ERR_CRL_NOT_YET_VALID CRL이 아직 유효하지 않습니다.

12 X509_V_ERR_CRL_HAS_EXPIRED CRL이 만료되었습니다.

13 X509_V_ERR_ERROR_IN_CERT_NOT_BEFORE_FIELD 인증서 notBefore 필드에 잘못된 시간이 포함되어 있습니다.

14 X509_V_ERR_ERROR_IN_CERT_NOT_AFTER_FIELD 인증서 notAfter 필드에 유효하지 않은 시간이 포함되어 있습니다.

15 X509_V_ERR_ERROR_IN_CRL_LAST_UPDATE_FIELD CRL lastUpdate 필드에 잘못된 시간이 포함되어 있습니다.

16 X509_V_ERR_ERROR_IN_CRL_NEXT_UPDATE_FIELD CRL nextUpdate 필드에 유효하지 않은 시간이 포함되어 있습니다.

17 X509_V_ERR_OUT_OF_MEM 메모리를 할당하는 동안 오류가 발생했습니다. 이러한 현상은 발생해서는 안 됩니다.

18 X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT 전달된 인증서가 자체 서명되었으며 신뢰할 수 있는 인증서 목록에서 동일한 인증서를 찾을 수 없습니다.

19 X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN 신뢰할 수 없는 인증서를 사용하여 인증서 체인을 구축할 수 있지만 루트를 로컬에서 찾을 수 없습니다.

20 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY 로컬로 조회된 인증서의 발급자 인증서를 찾을 수 없습니다. 이는 일반적으로 신뢰할 수 있는 인증서 목록이 완전하지 않음을 의미합니다.

21 X509_V_ERR_UNABLE_TO_VERIFY_LEAF_SIGNATURE 체인에 하나의 인증서만 포함되어 있으며 자체 서명되지 않았으므로 서명을 확인할 수 없습니다. 자세한 내용은 아래의 "반환 코드 확인: 21(첫 번째 인증서를 확인할 수 없음)"를 참조하십시오. 자세한 내용은 아래의 반환 코드 확인: 21(첫 번째 인증서를 확인할 수 없음)을 참조하십시오.

22 X509_V_ERR_CERT_CHAIN_TOO_LONG 인증서 체인 길이가 제공된 최대 깊이보다 큽니다. 사용되지 않음.

23 X509_V_ERR_CERT_REVOKED 인증서가 해지되었습니다.

24 X509_V_ERR_INVALID_CA CA 인증서가 유효하지 않습니다. CA가 아니거나 확장명이 제공된 목적과 일치하지 않습니다.

25 X509_V_ERR_PATH_LENGTH_EXCEEDED basicConstraints pathlength 매개변수가 초과되었습니다.

26 X509_V_ERR_INVALID_PURPOSE 제공된 인증서를 지정된 용도로 사용할 수 없습니다.

27 X509_V_ERR_CERT_UNTRUSTED 루트 CA가 지정된 용도로 신뢰할 수 있는 것으로 표시되지 않았습니다.

28 X509_V_ERR_CERT_REJECTED 루트 CA가 지정된 용도를 거부하도록 표시되었습니다.

29 X509_V_ERR_SUBJECT_ISSUER_MISMATCH 해당 주체 이름이 현재 인증서의 발급자 이름과 일치하지 않아 현재 후보 발급자 인증서가 거부되었습니다. -issuer_checks 옵션이 설정된 경우에만 표시됩니다.

30 X509_V_ERR_AKID_SKID_MISMATCH 현재 후보 발급자 인증서가 거부되었습니다. 해당 주체 키 식별자가 있고 인증 기관 키 식별자가 현재 인증서와 일치하지 않기 때문입니다. -issuer_checks 옵션이 설정된 경우에만 표시됩니다.

31 X509_V_ERR_AKID_ISSUER_SERIAL_MISMATCH 발급자 이름 및 일련 번호가 존재하고 현재 인증서의 기관 키 식별자와 일치하지 않으므로 현재 발급자 인증서가 거부되었습니다. -issuer_checks 옵션이 설정된 경우에만 표시됩니다.

32 X509_V_ERR_KEYUSAGE_NO_CERTSIGN keyUsage 확장이 인증서 서명을 허용하지 않으므로 현재 발급자 인증서가 거부되었습니다.

50 X509_V_ERR_APPLICATION_VERIFICATION 애플리케이션 관련 오류입니다. 사용되지 않음.

새 인증서 탐지됨

자체 서명 인증서가 있는 디바이스를 업그레이드하고 업그레이드 프로세스 후에 새 인증서가 생성되는 경우 Security Cloud Control는 **Configuration Status(**구성 상태**)** 및 **Connectivity(**연결성**)** 상태로 "New Certificate Detected(새 인증서 탐지됨)" 메시지를 생성할 수 있습니다. Security Cloud Control에서 계속 관리하려면 이 문제를 수동으로 확인하고 해결해야 합니다. 인증서가 동기화되고 디바이스가 정상 상태가 되면 디바이스를 관리할 수 있습니다.

Note 두 개 이상의 매니지드 디바이스를 Security Cloud Control에 동시에 대량으로 재연결하는 경우, Security Cloud Control는 디바이스에서 새 인증서를 자동으로 검토 및 수락하고 계속해서 다시 연결합니다.

다음 절차를 사용하여 새 인증서를 확인합니다.

1. 왼쪽 창에서 보안 디바이스를 클릭합니다.
2. 필터를 사용하여 **New Certificate Detected(**새 인증서 탐지됨**)** 연결 또는 구성 상태의 디바이스를 표시하고 원하는 디바이스를 선택합니다.
3. 작업창에서 **Review Certificate(**인증서 검토**)**를 클릭합니다. Security Cloud Control에서는 검토를 위해 인증서를 다운로드하고 새 인증서를 수락할 수 있습니다.
4. Device Sync(디바이스 동기화) 창에서 **Accept(**수락**)**를 클릭하거나 Reconnecting to Device(디바이스에 다시 연결 중) 창에서 **Continue(**계속**)**를 클릭합니다.

   Security Cloud Control는 디바이스를 새 자체 서명 인증서와 자동으로 동기화합니다. 디바이스가 동기화된 후 디바이스를 확인하려면 페이지를 수동으로 새로 고쳐야 할 수 있습니다.

인증서 오류 코드

반환 코드 확인**: 0 (ok)** 하지만 **Security Cloud Control**에서 인증서 오류를 반환합니다**.**

Security Cloud Control에 인증서가 있으면 "https://<device_ip>:<port>"에 GET 호출을 하여 URL에 연결을 시도합니다. 그래도 문제가 해결되지 않으면 Security Cloud Control에 인증서 오류가 표시됩니다. 인증서가 유효한 경우(openssl에서 0 ok 반환) 연결하려는 포트에서 다른 서비스가 수신 대기하는 문제일 수 있습니다. 다음 명령을 사용할 수 있습니다.

```
curl -k -u <username>:<password> https://<device_id>:<device_port>/admin/exec/show%20version
```

ASA와 통신하고 있는지 확인하고 HTTPS 서버가 ASA의 올바른 포트에서 실행 중인지 확인합니다.

```
 # show asp table socket
Protocol         Socket         State         Local Address              Foreign Address
SSL             00019b98        LISTEN        192.168.1.5:443              0.0.0.0:*
SSL             00029e18        LISTEN        192.168.2.5:443              0.0.0.0:*
TCP             00032208        LISTEN        192.168.1.5:22               0.0.0.0:*
```

반환 코드 확인**: 9(**인증서가 아직 유효하지 않음**)**

이 오류는 제공된 인증서의 발급 날짜가 미래이므로 클라이언트가 이를 유효한 것으로 처리하지 않음을 의미합니다. 이는 잘못 구성된 인증서로 인해 발생할 수 있으며, 자체 서명 인증서의 경우 인증서를 생성할 때 잘못된 디바이스 시간이 원인일 수 있습니다.

인증서의 notBefore 날짜를 포함하는 오류에 줄이 표시되어야 합니다.

```
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=9:certificate is not yet valid
notBefore=Oct 21 19:43:15 2016 GMT
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
notBefore=Oct 21 19:43:15 2016 GMT
```

이 오류를 통해 인증서가 유효한 시점을 확인할 수 있습니다.

치료

인증서의 notBefore 날짜는 과거여야 합니다. 이전 날짜의 인증서를 재발급할 수 있습니다. 이 문제는 클라이언트 또는 발급 디바이스에서 시간이 올바르게 설정되지 않은 경우에도 발생할 수 있습니다.

반환 코드 확인**: 10(**인증서가 만료되었습니다**)**

이 오류는 제공된 인증서 중 하나 이상이 만료되었음을 의미합니다. 인증서의 notBefore 날짜를 포함하는 오류에 줄이 표시되어야 합니다.

```
 error 10 at 0 depth lookup:certificate has expired
```

만료 날짜는 인증서 본문에 있습니다.

치료

인증서가 실제로 만료된 경우 유일한 교정 방법은 다른 인증서를 가져오는 것입니다. 인증서의 만료 날짜가 아직 미래이지만 openssl이 만료되었다고 주장하는 경우, 컴퓨터의 시간과 날짜를 확인합니다. 예를 들어 인증서가 2020년에 만료되도록 설정되어 있지만 컴퓨터의 날짜가 2021년이면 컴퓨터는 해당 인증서를 만료된 것으로 처리합니다.

반환 코드 확인**: 21(**첫 번째 인증서를 확인할 수 없음**)**

이 오류는 인증서 체인에 문제가 있음을 나타내며, openssl은 디바이스에서 제공하는 인증서를 신뢰할 수 있는지 확인할 수 없습니다. 인증서 체인이 작동하는 방식을 확인하려면 위의 예에서 인증서 체인을 살펴보겠습니다.

```
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
i:/C=US/O=Google Inc/CN=Google Internet Authority G2

-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA

-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority

-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE----- ---
```

인증서 체인은 서버에서 제공하는 인증서 목록으로, 서버의 자체 인증서부터 시작하여 점점 더 높은 수준의 중간 인증서를 포함하여 서버의 인증서를 인증 기관의 최상위 인증서와 연결합니다. 각 인증서에는 해당 주체(':'로 시작하는 줄) 및 발급자('i'로 시작하는 줄)가 나열됩니다.

주체는 인증서로 식별되는 엔티티입니다. 여기에는 조직 이름이 포함되며 경우에 따라 인증서가 발급된 엔티티의 공용 이름이 포함됩니다.

발급자는 인증서를 발급한 엔티티입니다. 여기에는 Organization(조직) 필드도 포함되며, 경우에 따라 Common Name(일반 이름)도 포함됩니다.

서버에 신뢰할 수 있는 인증 기관에서 직접 발급한 인증서가 있는 경우 인증서 체인에 다른 인증서를 포함할 필요가 없습니다. 다음과 같은 인증서를 제공합니다.

```
--- Certificate chain 0 s:/C=US/ST=California/L=Anytown/O=ExampleCo/CN=*.example.com
i:/C=US/O=Trusted Authority/CN=Trusted Authority
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE----- ---
```

이 인증서가 제공되면 openssl은 ***.example.com**에 대한 ExampleCo 인증서가 신뢰할 수 있는 기관 인증서에 의해 올바르게 서명되었는지 확인합니다. 이 인증서는 openssl의 기본 제공 신뢰 저장소에 있습니다. 확인 후 openssl이 디바이스에 성공적으로 연결됩니다.

그러나 대부분의 서버에는 신뢰할 수 있는 CA에서 직접 서명한 인증서가 없습니다. 대신 첫 번째 예에서와 같이 서버의 인증서가 하나 이상의 중간 인증서에 의해 서명되고, 최상위 중간 인증서에는 신

뢰할 수 있는 CA가 서명한 인증서가 있습니다. OpenSSL은 기본적으로 이러한 중간 CA를 신뢰하지 않으며, 신뢰할 수 있는 CA로 끝나는 완전한 인증서 체인이 제공되는 경우에만 이를 확인할 수 있습니다.

중간 기관이 인증서에 서명한 서버는 모든 중간 인증서를 포함하여 이를 신뢰할 수 있는 CA에 연결하는 모든 인증서를 제공해야 합니다. 이 전체 체인을 제공하지 않는 경우 openssl의 출력은 다음과 같습니다.

```
depth=0 OU = Example Unit, CN = example.com
verify error:num=20:unable to get local issuer certificate
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=27:certificate not trusted
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=21:unable to verify the first certificate
verify return:1

CONNECTED(00000003)

---
Certificate chain
0 s:/OU=Example Unit/CN=example.com
i:/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
-----BEGIN CERTIFICATE-----
...lots of b64...
-----END CERTIFICATE-----
---
Server certificate
subject=/OU=Example Unit/CN=example.com
issuer=/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
---
No client certificate CA names sent
---
SSL handshake has read 1509 bytes and written 573 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: 24B45B2D5492A6C5D2D5AC470E42896F9D2DDDD54EF6E3363B7FDA28AB32414B
Session-ID-ctx:
Master-Key:
21BAF9D2E1525A5B935BF107DA3CAF691C1E499286CBEA987F64AE5F603AAF8E65999BD21B06B116FE9968FB7C62EF7C

Key-Arg : None
Krb5 Principal: None
PSK identity: None
PSK identity hint: None
Start Time: 1476711760
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

이 출력은 서버가 하나의 인증서만 제공했으며 제공된 인증서가 신뢰할 수 있는 루트가 아닌 중간 기관에 의해 서명되었음을 보여줍니다. 출력에는 특성 확인 오류도 표시됩니다.

치료

이 문제는 디바이스에서 제공하는 인증서가 잘못 구성되어 발생합니다. Security Cloud Control 또는 다른 프로그램이 디바이스에 안전하게 연결할 수 있도록 이 문제를 해결하는 유일한 방법은 올바른 인증서 체인을 디바이스에 로드하여 연결하는 클라이언트에 완전한 인증서 체인을 제공하도록 하는 것입니다.

트러스트 포인트에 중간 CA를 포함하려면 아래 링크 중 하나를 따르십시오(CSR이 ASA에서 생성되었는지 여부에 따라).

- https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc13
- https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc15

새 인증서 탐지됨

자체 서명 인증서가 있는 디바이스를 업그레이드하고 업그레이드 프로세스 후에 새 인증서가 생성되는 경우 Security Cloud Control는 **Configuration Status(**구성 상태**)** 및 **Connectivity(**연결성**)** 상태로 "New Certificate Detected(새 인증서 탐지됨)" 메시지를 생성할 수 있습니다. Security Cloud Control에서 계속 관리하려면 이 문제를 수동으로 확인하고 해결해야 합니다. 인증서가 동기화되고 디바이스가 정상 상태가 되면 디바이스를 관리할 수 있습니다.

참고 두 개 이상의 매니지드 디바이스를 Security Cloud Control에 동시에 CDO에 대량으로 다시 연결하는 경우, Security Cloud Control는 디바이스에서 새 인증서를 자동으로 검토 및 수락하고 계속해서 다시 연결합니다.

다음 절차를 사용하여 새 인증서를 확인합니다.

프로시저

단계 **1** 왼쪽 창에서 보안 디바이스를 클릭합니다.

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

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 필터를 사용하여 **New Certificate Detected(**새 인증서 탐지됨**)** 연결 또는 구성 상태의 디바이스를 표시하고 원하는 디바이스를 선택합니다.

단계 **5** 작업창에서 **Review Certificate(**인증서 검토**)**를 클릭합니다. Security Cloud Control에서는 검토를 위해 인증서를 다운로드하고 새 인증서를 수락할 수 있습니다.

단계 **6** Device Sync(디바이스 동기화) 창에서 **Accept(**수락**)**를 클릭하거나 Reconnecting to Device(디바이스에 다시 연결 중) 창에서 **Continue(**계속**)**를 클릭합니다.

Security Cloud Control는 디바이스를 새 자체 서명 인증서와 자동으로 동기화합니다. 디바이스가 동기화된 후 디바이스를 확인하려면 페이지를 수동으로 새로 고쳐야 할 수 있습니다.

온보딩 오류 문제 해결

디바이스 온보딩 오류는 여러 가지 이유로 발생할 수 있습니다.

다음과 같은 작업을 수행할 수 있습니다.

Procedure

단계 **1** 왼쪽 창에서 보안 디바이스를 클릭합니다.

단계 **2** 적절한 디바이스 유형 탭을 클릭하고 이 오류가 발생하는 디바이스를 선택합니다. 경우에 따라 오른쪽에 오류 설명이 표시됩니다. 설명에 언급된 필요한 조치를 취하십시오.

또는

단계 **3** Security Cloud Control에서 디바이스 인스턴스를 제거하고 디바이스 온보딩을 다시 시도하십시오.

충돌 탐지됨 상태 해결

Security Cloud Control를 사용하면 각 라이브 디바이스에서 충돌 탐지를 활성화하거나 비활성화할 수 있습니다. 충돌 탐지이 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.

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.

연결할 수 없는 연결 상태 문제 해결

다음과 같은 여러 가지 이유로 디바이스가 "접근 불가" 상태일 수 있습니다.

Procedure

단계 **1** 왼쪽 창에서 보안 디바이스를 클릭합니다.

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

단계 **3** 적절한 디바이스 유형 탭을 클릭하고 접근 불가 상태의 디바이스를 선택합니다.

단계 **4** **Reconnect(**다시 연결**)**를 클릭합니다.

단계 **5** 오른쪽에 나타나는 메시지에 따라 다음 작업 중 하나를 수행합니다.

a. IP 주소 및 디바이스 자격 증명을 사용하여 FDM 관리 디바이스를 온보딩한 경우 다음 메시지가 나타납니다.

"이 디바이스에 연결할 수 없습니다. *IP* 주소와 포트를 검토하십시오," 메시지 상자에 디바이스의 새 IP 주소 및/또는 새 포트 정보를 입력하십시오. Security Cloud Control가 잘못된 IP 주소에 연결을 시도했기 때문에 디바이스의 IP 주소가 디바이스에서 직접 변경되었을 수 있습니다.

Note
디바이스가 재부팅되고 보류 중인 다른 변경 사항이 없는 경우 디바이스는 온라인 연결 상태로 돌아가야 하며 추가 작업이 필요하지 않습니다.

이제 디바이스가 "Online(온라인)"이지만 구성 상태가 "Conflict Detected(충돌 탐지됨)"인 것을 확인할 수 있습니다. Resolve Configuration Conflicts(구성 충돌 해결)를 사용하여 Security Cloud Control와 디바이스 간의 구성 차이를 검토합니다.

b. 등록 토큰 또는 일련 번호를 사용하여 FDM 관리 디바이스를 온보딩하는 경우 다음 메시지가 나타납니다.

" 디바이스가 *Cisco Cloud*에서 삭제되었습니다. *RMA(Return Material Authorization)* 프로세스의 일부로 삭제될 수 있습니다." RMA 팀에 반환한 결함 있는 디바이스가 RMA 프로세스의 일부로 Cisco Cloud에서 삭제되었음을 의미합니다.

결과적으로 디바이스 연결 상태가 Security Cloud Control에서 "연결할 수 없음"임을 알 수 있습니다.

- RMA 케이스의 경우 Security Cloud Control에서 다음 단계를 수행해야 합니다.

1. 디바이스가 성공적으로 온보딩된 경우 디바이스 구성을 템플릿으로 저장해야 합니다. FDM 템플릿 구성을 참조하십시오.

   Security Cloud Control에서 디바이스 인스턴스를 삭제합니다.

2. RMA 팀에서 받은 새 교체 디바이스의 전원을 켜고 Security Cloud Control에 온보딩합니다.

디바이스의 일련 번호를 사용하여 FDM 매니지드 디바이스 온보딩을 참조하십시오.

Important
교체 디바이스의 일련 번호가 다를 수 있으며 새 디바이스로 온보딩해야 합니다.

이제 디바이스가 "온라인"이지만 구성 상태는 "충돌 감지됨"임을 알 수 있습니다.

3. Resolve Configuration Conflicts(구성 충돌 해결)를 사용하여 Security Cloud Control와 디바이스 간의 구성 차이를 검토합니다.

   이전에 저장한 템플릿을 새 디바이스에 적용합니다. FDM 템플릿 적용을 참조하십시오.

- 디바이스 구성을 지우지 않고 디바이스를 판매하거나 소유권을 테넌트 외부의 다른 사용자에게 양도한 경우 더 이상 디바이스를 소유하지 않습니다. 이 오류는 구매자가 디바이스의 이미지를 다시 만들 때 발생합니다. 디바이스가 올바르게 구성되고 이전에 동기화된 경우 디바이스 구성을 템플릿으로 저장한 다음 Security Cloud Control에서 디바이스 인스턴스를 제거할 수 있습니다.

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.