온보딩된 디바이스 설정 관리

이 장에서는 온보딩된 디바이스의 디바이스 설정 관리에 대한 지침을 제공합니다.

- Security Cloud Control에서 디바이스의 IP 주소 변경, on page 1
- Security Cloud Control에서 디바이스 이름 변경, on page 2
- 디바이스 및 서비스 목록 내보내기, on page 3
- 디바이스 구성 내보내기, 3 페이지
- 디바이스의 외부 링크, on page 4
- Security Cloud Control에 디바이스 대량 재연결, on page 7
- 테넌트 간 디바이스 이동, on page 8
- 디바이스 인증서 만료 감지, 8 페이지
- 디바이스 메모 작성, on page 9
- Security Cloud Control에서 디바이스 삭제, 9 페이지
- 보안 디바이스 관리, 9 페이지
- Security Cloud Control 매니지드 Firewall Threat Defense 디바이스 백업, 10 페이지
- Security Cloud Control를 통해 Firewall Threat Defense 디바이스 관리, 11 페이지
- 보안 디바이스 개요, 12 페이지
- Security Cloud Control 레이블 및 필터링, 13 페이지
- Security Cloud Control 검색 기능 사용, 15 페이지

Security Cloud Control에서 디바이스의 IP 주소 변경

IP 주소를 사용하여 Security Cloud Control에 디바이스를 온보딩하면 Security Cloud Control는 해당 IP 주소를 데이터베이스에 저장하고 해당 IP 주소를 사용하여 디바이스와 통신합니다. 디바이스의 IP 주소가 변경되면 새 주소와 일치하도록 Security Cloud Control에 저장된 IP 주소를 업데이트할 수 있습니다. Security Cloud Control에서 디바이스의 IP 주소를 변경해도 디바이스의 구성은 변경되지 않습니다.

Security Cloud Control가 디바이스와 통신하는 데 사용하는 IP 주소를 변경하려면 다음 절차를 수행합니다.

Procedure

단계 **1** 왼쪽 창에서 **Manage(관리)** > **Security Devices(보안 디바이스)**를 클릭합니다.

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

단계 **3** 해당 디바이스 탭을 클릭합니다.

필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 **4** IP 주소를 변경할 디바이스를 선택합니다.

단계 **5** **Device Details(디바이스 세부 정보)** 창 위에서 디바이스의 IP 주소 옆에 있는 편집 버튼을 클릭합니다.

단계 **6** 필드에 새 IP 주소를 입력하고 파란색 확인 버튼을 클릭합니다.

디바이스 자체는 변경되지 않으므로 디바이스의 Configuration Status(구성 상태)는 계속해서 Synced(동기화됨)로 표시됩니다.

관련 정보:

- 테넌트 간 디바이스 이동, on page 8
- Security Cloud Control에 디바이스 대량 재연결, on page 7

Security Cloud Control에서 디바이스 이름 변경

모든 디바이스, 모델, 템플릿 및 서비스는 온보딩되거나 Security Cloud Control에서 생성될 때 이름이 지정됩니다. 디바이스 자체의 구성을 변경하지 않고 해당 이름을 변경할 수 있습니다.

Procedure

단계 **1** 왼쪽 창에서 **Manage(관리)** > **Security Devices(보안 디바이스)**를 클릭합니다.

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

단계 **3** 이름을 변경하려는 디바이스를 선택합니다.

단계 **4** **Device Details(디바이스 세부 정보)** 창 위에서 디바이스의 이름 옆에 있는 편집 버튼을 클릭합니다.

단계 **5** 필드에 새 이름을 입력하고 파란색 확인 버튼을 클릭합니다.

디바이스 자체는 변경되지 않으므로 디바이스의 Configuration Status(구성 상태)는 계속해서 Synced(동기화됨)로 표시됩니다.

디바이스 및 서비스 목록 내보내기

이 문서에서는 디바이스 및 서비스 목록을 쉼표로 구분된 값(.csv) 파일로 내보내는 방법을 설명합니다. 이 형식이 되면 Microsoft Excel과 같은 스프레드시트 애플리케이션에서 파일을 열어 목록의 항목을 정렬하고 필터링할 수 있습니다.

내보내기 버튼은 디바이스 및 템플릿 탭에서 사용할 수 있습니다. 또한 선택한 디바이스 유형 탭의 디바이스에서 세부 정보를 내보낼 수 있습니다.

디바이스 및 서비스 목록을 내보내기 전에 필터 창을 살펴보고 **Security Devices(**보안 디바이스**)** 테이블에 내보내려는 정보가 표시되는지 확인합니다. 모든 필터를 지워 모든 매니지드 디바이스 및 서비스를 확인하거나 정보를 필터링하여 모든 디바이스 및 서비스의 하위 집합을 표시합니다. 내보내기 기능은 **Security Devices(**보안 디바이스**)** 테이블에서 확인할 수 있는 내용을 내보냅니다.

Procedure

단계 **1** 왼쪽 창에서 **Manage(**관리**)** > **Security Devices(**보안 디바이스**)**를 클릭합니다.

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

단계 **3** 해당 디바이스 유형 탭을 클릭하여 해당 탭 아래의 디바이스에서 세부 정보를 내보내거나 **All(**모두**)**을 클릭하여 모든 디바이스에서 세부 정보를 내보냅니다.

필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 **4** **Export list to CSV(CSV**로 목록 내보내기**)**를 클릭합니다.

단계 **5** 메시지가 표시되면 .csv 파일을 저장합니다.

단계 **6** 스프레드시트 애플리케이션에서 .csv 파일을 열어 결과를 정렬하고 필터링합니다.

디바이스 구성 내보내기

한 번에 하나의 디바이스 구성만 내보낼 수 있습니다. 다음 절차를 사용하여 디바이스의 구성을 JSON 파일로 내보냅니다.

프로시저

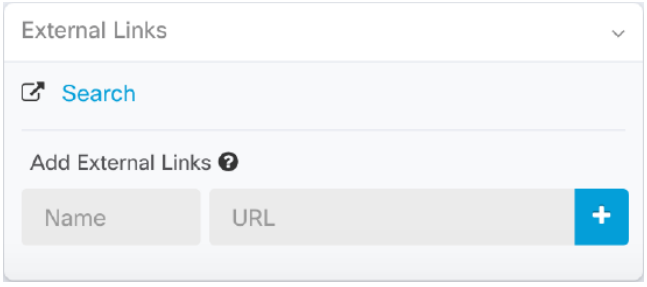
단계 1 왼쪽 창에서 **Manage(관리)** > **Security Devices(보안 디바이스)**를 클릭합니다.
단계 2 **Devices(디바이스)** 탭을 클릭하여 디바이스를 찾거나 **Templates(템플릿)** 탭을 클릭하여 모델 디바이스를 찾습니다.
단계 3 해당 디바이스 탭을 클릭합니다.

필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 4 원하는 디바이스를 선택하여 강조 표시하십시오.
단계 5 **Actions(작업)** 창에서 **Export Configuration(구성 내보내기)**를 선택합니다.
단계 6 **Confirm(확인)**을 선택하여 구성을 JSON 파일로 저장합니다.

디바이스의 외부 링크

외부 리소스에 대한 하이퍼링크를 생성하여 Security Cloud Control로 관리하는 디바이스와 연결할 수 있습니다. 이 기능을 사용하여 디바이스 중 하나의 로컬 관리자에 대한 편리한 링크를 생성할 수 있습니다(ASA의 경우 ASDM(Adaptive Security Device Manager), FTD의 경우). 또한 이를 사용하여 검색 엔진, 설명서 리소스, 회사 Wiki 또는 선택한 다른 URL에 연결할 수 있습니다. 외부 링크를 원하는 만큼 디바이스에 연결할 수 있습니다. 동일한 링크를 여러 디바이스와 동시에 연결할 수도 있습니다.



생성한 링크는 어디에나 연결할 수 있지만 회사의 보안 요구 사항은 변경되지 않습니다. 예를 들어 특정 URL에 도달하기 위해 온프레미스 또는 VPN 연결을 통해 일반적으로 기업 네트워크에 연결해야 하는 경우 이러한 요구 사항은 그대로 유지됩니다. 회사에서 특정 URL을 차단하는 경우 해당 URL은 계속 차단됩니다. 제한되지 않은 URL은 계속해서 제한되지 않습니다.

위치 변수

URL에 통합할 수 있는 {location} 변수를 생성했습니다. 이 변수는 디바이스의 IP 주소로 채워집니다. 예를 들면 다음과 같습니다.

```
https://{location}
```

ASA의 ASDM에 도달 또는

관련 정보:

• 디바이스 메모 작성, on page 9
• 디바이스 및 서비스 목록 내보내기, on page 3

디바이스에서 외부 링크 생성

Procedure

단계 **1** 왼쪽 창에서 **Manage(**관리**)** > **Security Devices(**보안 디바이스**)**를 클릭합니다.
단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.
단계 **3** 해당 디바이스 탭을 클릭합니다.
단계 **4** 디바이스 또는 모델을 선택합니다.

필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 **5** 세부 정보 창의 오른쪽에서, **External Links(**외부 링크**)** 섹션으로 이동합니다.
단계 **6** 링크 이름을 입력합니다.
단계 **7** URL 필드에 링크의 URL을 입력합니다. 예를 들어 Cisco의 경우 http://www.cisco.com을 입력하는 것과 같이 전체 URL을 지정해야 합니다.
단계 **8** +를 클릭하여 링크를 디바이스와 연결합니다.

ASDM 에 대한 외부 링크 생성

다음은 Security Cloud Control에서 직접 ASA의 ASDM(Adaptive Security Device Manager)과 을 여는 편리한 방법입니다.

Procedure

단계 **1** 왼쪽 창에서 **Manage(**관리**)** > **Security Devices(**보안 디바이스**)**를 클릭합니다.
단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.
단계 **3** 해당 디바이스 탭을 클릭합니다.

필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 **4** 디바이스 또는 모델을 선택합니다.
단계 **5** 세부 정보 창의 오른쪽에서, **External Links(**외부 링크**)** 섹션으로 이동합니다.
단계 **6** ASDM 과 같은 링크 이름을 입력합니다.
단계 **7** URL 필드에 https://{location}을 입력합니다. {location} 변수는 디바이스의 IP 주소로 채워집니다.

단계 **8** + 상자를 클릭합니다.

여러 디바이스에 대한 외부 링크 생성

Procedure

단계 **1** 왼쪽 창에서 **Manage(**관리**)** > **Security Devices(**보안 디바이스**)**를 클릭합니다.
단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.
단계 **3** 해당 디바이스 탭을 클릭합니다.

필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 **4** 여러 디바이스 또는 모델을 선택합니다.
단계 **5** 세부 정보 창의 오른쪽에서, **External Links(**외부 링크**)** 섹션으로 이동합니다.
단계 **6** 링크 이름을 입력합니다.
단계 **7** 다음 방법 중 하나를 사용하여 도달하려는 URL을 입력하십시오.

- 입력

  ```
  https://{location}
  ```

  URL 필드에. {location} 변수는 디바이스의 IP 주소로 채워집니다. 이렇게 하면 디바이스의 ASDM에 대한 자동 링크가 생성됩니다.

- URL 필드에 링크의 URL을 입력합니다. 예를 들어 Cisco의 경우 http://www.cisco.com을 입력하는 것과 같이 전체 URL을 지정해야 합니다.

단계 **8** +를 클릭하여 링크를 디바이스와 연결합니다.

외부 링크 편집 또는 삭제

Procedure

단계 **1** 왼쪽 창에서 **Manage(**관리**)** > **Security Devices(**보안 디바이스**)**를 클릭합니다.
단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.
단계 **3** 해당 디바이스 탭을 클릭합니다.

필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 **4** 디바이스 또는 모델을 선택합니다.
단계 **5** 세부 정보 창의 오른쪽에서, **External Links(**외부 링크**)** 섹션으로 이동합니다.

단계 **6** 편집 및 삭제 아이콘을 표시하려면 링크 이름에 마우스를 올려놓습니다.
단계 **7** 해당 아이콘을 클릭하여 외부 링크를 편집하거나 삭제하고 작업을 확인합니다.

여러 디바이스에 대한 외부 링크 편집 또는 삭제

Procedure

단계 **1** 왼쪽 창에서 **Manage(**관리**)** > **Security Devices(**보안 디바이스**)**를 클릭합니다.
단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.
단계 **3** 해당 디바이스 탭을 클릭합니다.

필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 **4** 여러 디바이스 또는 모델을 선택합니다.
단계 **5** 세부 정보 창의 오른쪽에서, **External Links(**외부 링크**)** 섹션으로 이동합니다.
단계 **6** 편집 및 삭제 아이콘을 표시하려면 링크 이름에 마우스를 올려놓습니다.
단계 **7** 해당 아이콘을 클릭하여 외부 링크를 편집하거나 삭제하고 작업을 확인합니다.

Security Cloud Control에 디바이스 대량 재연결

관리자는 Security Cloud Control를 통해 둘 이상의 매니지드 디바이스를 Security Cloud Control에 동시에 다시 연결할 수 있습니다. Security Cloud Control가 관리하는 디바이스가 "unreachable(연결할 수 없음)"로 표시되면 Security Cloud Control는 더 이상 대역 외 구성 변경 사항을 탐지하거나 디바이스를 관리할 수 없습니다. 연결이 끊어지는 데에는 여러 가지 이유가 있을 수 있습니다. 디바이스에 대한 Security Cloud Control 관리를 복원하는 첫 번째 단계는 디바이스를 다시 연결하는 것입니다.

Note 새 인증서가 있는 디바이스를 다시 연결하는 경우 Security Cloud Control는 디바이스에서 새 인증서를 자동으로 검토 및 수락하고 계속해서 다시 연결합니다. 그러나 하나의 디바이스에만 다시 연결하는 경우 Security Cloud Control는 계속해서 다시 연결하려면 인증서를 수동으로 검토하고 수락하라는 메시지를 표시합니다.

Procedure

단계 **1** 왼쪽 창에서 **Manage(**관리**)** > **Security Devices(**보안 디바이스**)**를 클릭합니다.
단계 **2** 디바이스를 찾으려면 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

필터를 사용하여 연결 상태가 "unreachable(연결할 수 없음)"인 디바이스를 찾습니다.

단계 **4** 필터링된 결과에서 다시 연결을 시도할 디바이스를 선택합니다.

단계 **5** **Reconnect(**다시 연결**)** 를 클릭합니다. Security Cloud Control는 선택한 모든 디바이스에 적용할 수 있는 작업에 대해서만 명령 버튼을 제공합니다.

단계 **6** 알림 탭에서 대량 디바이스 다시 연결 작업의 진행 상황을 확인합니다. 대량 디바이스 다시 연결 작업의 성공 또는 실패에 대한 자세한 내용을 보려면 파란색 Review(검토) 링크를 클릭합니다. 그러면 Security Cloud Control에서 작업 모니터링로 이동합니다.

Tip
디바이스의 인증서 또는 자격 증명이 변경되어 재연결 실패가 발생한 경우, 해당 디바이스에 개별적으로 다시 연결하여 새 자격 증명을 추가하고 새 인증서를 수락해야 합니다.

테넌트 간 디바이스 이동

디바이스를 Security Cloud Control 테넌트에 온보딩하면 한 Security Cloud Control 테넌트 간에 디바이스를 마이그레이션할 수 없습니다. 디바이스를 새 테넌트로 이동하려면 이전 테넌트에서 디바이스를 제거하고 새 테넌트에 다시 온보딩해야 합니다.

디바이스 인증서 만료 감지

관리 인증서는 Security Cloud Control에서 FDM 관리 및 ASA 디바이스에 액세스하는 데 사용되지만, Cisco Secure Client(이전 AnyConnect)는 Security Cloud Control의 ASA, FDM 관리 및 FTD 디바이스에서 가상 프라이빗 네트워크 기능을 사용하는데 필요합니다.

Security Cloud Control는 이러한 인증서의 만료 상태를 적극적으로 모니터링하고 이러한 인증서가 만료 날짜에 가까워지거나 만료되면 사용자에게 알립니다. 이렇게 하면 인증서 만료로 인해 디바이스 작동이 중단되는 것을 방지할 수 있습니다. 이 문제를 해결하려면 해당 인증서를 갱신해야 합니다.

관리 인증서 만료 확인은 ASA 및 FDM 매니지드 디바이스에 적용되며, Secure Client 인증서 만료 확인은 ASA, FDM 관리 및 FTD 디바이스에 적용됩니다.

인증서 만료 알림 보기

오른쪽 상단에서 알림( ) 아이콘을 클릭하여 테넌트에 온보딩한 디바이스에 발생했거나 영향을 미친 가장 최신 알림을 확인합니다. 우선순위가 높은 섹션에는 인증서 만료 알림이 표시됩니다.

이러한 알림은 인증서 만료일 30, 14 및 7일 전에 전송되며, 그 이후에는 인증서가 만료되거나 유효한 인증서로 갱신할 때까지 매일 전송됩니다. 사용자 환경설정 페이지의 알림 설정 섹션에서 이러한 알림을 이메일로 수신하도록 구독할 수도 있습니다. 자세한 내용은 사용자 알림 환경설정을 참조하십시오.

디바이스 메모 작성

이 절차를 사용하여 디바이스에 대한 단일 일반 텍스트 메모 파일을 생성합니다.

Procedure

단계 **1** 왼쪽 창에서 **Manage(**관리**)** > **Security Devices(**보안 디바이스**)**를 클릭합니다.
단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.
단계 **3** 해당 디바이스 탭을 클릭합니다.
단계 **4** 메모를 작성할 디바이스 또는 모델을 선택합니다.
단계 **5** 오른쪽의 **Management(**관리**)** 창에서 **Notes(**메모**)**를 클릭합니다. Notes.
단계 **6** 오른쪽의 편집기 버튼을 클릭하고 기본 텍스트 편집기, Vim 또는 Emacs 텍스트 편집기를 선택합니다.
단계 **7** 메모 페이지를 수정합니다.
단계 **8** **Save(**저장**)**를 클릭합니다.
메모가 탭에 저장됩니다.

Security Cloud Control에서 디바이스 삭제

Security Cloud Control에서 디바이스를 삭제하려면 다음 절차를 따르십시오.

프로시저

단계 **1** Security Cloud Control에 로그인합니다.
단계 **2** 왼쪽 창에서 **Manage(**관리**)** > **Security Devices(**보안 디바이스**)**를 클릭합니다.
단계 **3** 삭제할 디바이스를 찾아 디바이스 행에서 디바이스를 확인하고 선택합니다.
단계 **4** 오른쪽에 있는 디바이스 작업 패널에서 **Remove(**제거**)**를 선택합니다.
단계 **5** 메시지가 표시되면 **OK(**확인**)**를 선택하여 선택한 디바이스 제거를 확인합니다. 디바이스를 온보딩 상태로 유지하려면 **Cancel(**취소**)**을 선택합니다.

보안 디바이스 관리

Security Cloud Control **Security Devices(**보안 디바이스**)** 페이지에서 온보딩된 디바이스를 보고, 관리하고, 필터링하고, 평가할 수 있는 기능을 제공합니다. **Security Devices(**보안 디바이스**)** 페이지에서 다음을 수행할 수 있습니다.

- Security Cloud Control 관리를 위한 디바이스 및 서비스를 온보딩합니다.
- 매니지드 디바이스 및 서비스의 구성 상태 및 연결 상태를 봅니다.
- 별도의 탭으로 분류된 온보딩된 디바이스 및 템플릿을 봅니다. 보안 디바이스 개요, 12 페이지를 참조하십시오.
- 개별 디바이스 및 서비스를 평가하고 조치를 취합니다.
- 디바이스 및 서비스별 정보를 보고 문제를 해결합니다.
- 다음에서 관리하는 위협 방어 디바이스의 디바이스 상태를 확인합니다.
  - 클라우드 제공 Firewall Management Center
  - 온프레미스 관리 센터

  클라우드 제공 Firewall Management Center에서 관리하는 위협 방어 디바이스의 경우, 클러스터에 있는 디바이스의 노드 상태도 볼 수 있습니다.
- 이름, 유형, IP 주소, 모델 이름, 일련 번호 또는 레이블로 디바이스 또는 템플릿을 검색합니다. 검색은 대/소문자를 구분하지 않습니다. 여러 검색어를 제공하면 검색어 중 하나 이상과 일치하는 디바이스 및 서비스가 나타납니다. 페이지 레벨 검색, 15 페이지를 참조하십시오.
- 디바이스 유형, 하드웨어 및 소프트웨어 버전, snort 버전, 구성 상태, 연결 상태, 충돌 감지, 보안 디바이스 커넥터 및 레이블을 기준으로 디바이스 또는 템플릿 필터를 필터링합니다. 필터를 참조하십시오.
- 디바이스 삭제

Security Cloud Control 매니지드 Firewall Threat Defense 디바이스 백업

Security Cloud Control 매니지드 Firewall Threat Defense 디바이스 유형을 백업하는 방법을 알아보려면 다음을 참조하십시오.

클라우드 제공 **Firewall Management Center** 매니지드 **Firewall Threat Defense** 디바이스 백업

- Security Cloud Control 왼쪽 창에서 **Administration(관리)** > **Firewall Management Center**를 선택합니다.
- **FMC** 탭에서 **Cloud-delivered FMC(클라우드 제공 FMC)**를 선택합니다.
- 오른쪽 창에서 **Devices(디바이스)**를 클릭하여 클라우드 제공 Firewall Management Center로 이동합니다.
- 클라우드 제공 Firewall Management Center에서 위협 방어 Threat Defense Device 백업 단계를 계속 진행합니다.

Security Cloud Control에 온보딩된 온프레미스 방화벽 **Management Center** 매니지드 **Firewall Threat Defense** 디바이스 백업

- Security Cloud Control 왼쪽 창에서 **Administration(관리) > Firewall Management Center**를 선택합니다.
- Firewall Threat Defense 디바이스가 백업하려는 온프레미스 방화벽 Management Center를 선택합니다.
- 오른쪽 창 에서 **FMC Cross Launch URL**을 클릭하여 온프레미스 관리 센터로 이동하거나 온프레미스 관리 센터에 수동으로 로그인합니다.
- Cisco Secure Firewall Management Center 관리 가이드에서 *Management Center*에서 디바이스 백업 단계를 계속합니다.

Security Cloud Control에 온보딩된 **Firewall Device Manager** 매니지드 **Firewall Threat Defense** 디바이스 백업

FDM 매니지드 디바이스 백업 단계를 수행합니다.

Security Cloud Control를 통해 Firewall Threat Defense 디바이스 관리

시작하기 전에

Security Cloud Control는 하드웨어 및 가상 형식 모두로 Firewall Threat Defense 디바이스를 관리할 수 있는 통합 인터페이스를 제공합니다.

이 세 가지 관리 애플리케이션과 연결된 Firewall Threat Defense 디바이스는 Security Cloud Control 플랫폼에서 관리할 수 있습니다.

- 보안 Firewall Device Manager
- Secure Firewall Management Center
- 보안 클라우드 제공 Firewall Management Center

프로시저

단계 **1** Security Cloud Control 플랫폼에 로그인합니다.

단계 **2** 왼쪽 창에서 **Security Devices(보안 디바이스)**를 클릭합니다.

단계 **3** **FTD** 탭을 클릭합니다.

단계 **4** 왼쪽 위 모서리에 있는  를 클릭합니다.

디바이스/서비스 아래에서, 필터창은 해당 Security Cloud Control 디바이스가 액세스되는 관리 애플리케이션에 따라 Firewall Threat Defense 디바이스를 표시하는 필터를 제공합니다.

- **FDM**: Firewall Device Manager에서 관리하는 Firewall Threat Defense 디바이스
- **FMC-FTD**: Firepower Management Center를 사용하여 관리되는 Firewall Threat Defense 디바이스
- **FTD**: 클라우드 제공 Firewall Management Center에서 관리하는 Firewall Threat Defense 디바이스

단계 **5** 관리 애플리케이션에서 Firewall Threat Defense 디바이스를 보려면 해당 체크 박스를 선택합니다.

보안 디바이스 개요

Security Devices(보안 디바이스**)** 페이지에는 모든 물리적 및 가상 온보딩된 디바이스와 온보딩된 디바이스에서 생성된 템플릿이 표시됩니다. 이 페이지는 유형에 따라 디바이스 및 템플릿을 분류하고 각 디바이스 유형 전용 해당 탭에 표시합니다.

Security Devices(보안 디바이스**)** 페이지에서 다음 세부 정보를 볼 수 있습니다.

- **Device(**디바이스**)** 탭에는 Security Cloud Control에 온보딩된 모든 라이브 디바이스가 표시됩니다.
- **Templates(**템플릿**)**에는 Security Cloud Control로 가져온 라이브 디바이스 또는 구성 파일에서 생성된 모든 템플릿 디바이스가 표시됩니다.

보안 디바이스의 필터

Security Devices(보안 디바이스**)** 페이지의 **Filter(**필터**)** 패널에서는 결과 범위를 좁히고 특정 속성을 기준으로 디바이스를 찾을 수 있는 여러 옵션이 제공됩니다. 여기에는 디바이스/서비스**,** 하드웨어 버전**,** 디바이스 단종**,** 소프트웨어 버전**, Snort** 버전**,** 구성 상태**,** 연결 상태**,** 탐지**,** 상태**, Secure Device Connector** 및 레이블이 포함됩니다.

하드웨어 단종**(EoL)** 필터

하드웨어 단종**(EoL)** 필터를 사용 하면 하드웨어 지원 만료일이 임박했거나 사용한 디바이스를 식별할 수 있습니다. 지원 종료일 이후에는 Cisco가 더 이상 소프트웨어 업데이트, 보안 패치 또는 기술 지원을 제공하지 않으므로 지원되지 않는 하드웨어를 사용하면 운영 및 보안 위험이 발생할 수 있습니다.

참고 하드웨어 EoL 필터는 현재 온프레미스 관리 센터 및 클라우드 제공 Firewall Management Center에서 관리하는 Firewall Threat Defense 디바이스와 ASA 디바이스를 지원합니다.

절차

1. **Devices(**디바이스**)** 탭에서 필터 아이콘을 클릭합니다.
2. 사용 가능한 필터 목록의 **Device End-of-Life(**디바이스 단종**)** 아래에서 **Hardware End-of-Life(**하드웨어 단종**)**를 선택합니다.

목록에는 이제 하드웨어 수명이 다해가는 중이거나 이미 다한 모든 디바이스가 표시됩니다.

3. 디바이스를 선택하여 오른쪽 창에서 자세한 정보를 봅니다.
4. **Device End of Life(**디바이스 단종**)** 섹션까지 아래로 스크롤하여 다음 세부 정보를 확인합니다.
   - 정확한 단종 날짜입니다.
   - 지원 종료일까지 남은 시간입니다.
5. **Know more(**자세히 알아보기**)**를 클릭합니다.

   다음 정보를 제공하는 세부 정보 페이지를 볼 수 있습니다.
   - 시스코가 권장하는 교체용 디바이스와 제품 사양, 그리고 공식 데이터 시트를 확인할 수 있는 링크입니다.
   - Cisco에 문의 페이지를 통해 요청을 제출하는 방법 및 Cisco 전문가에게 직접 문의할 수 있는 옵션에 대한 지침.
   - 제품 재활용 프로그램에 대한 정보입니다.
6. **Export(**내보내기**)**를 클릭하여 오프라인 분석을 위해 디바이스 보고서를 CSV 형식으로 다운로드합니다.

Security Cloud Control 레이블 및 필터링

레이블은 디바이스 또는 개체를 그룹화하는 데 사용됩니다. 온보딩 중에 또는 온보딩 후에 언제든지 하나 이상의 디바이스에 레이블을 적용할 수 있습니다. 개체를 생성한 후 개체에 레이블을 적용할 수 있습니다. 디바이스 및 개체에 레이블을 적용한 후에는 해당 레이블을 사용하여 디바이스 테이블 또는 개체 테이블의 내용을 필터링할 수 있습니다.

참고 디바이스에 적용된 레이블은 연결된 개체로 확장되지 않으며, 공유 개체에 적용된 레이블은 연결된 개체로 확장되지 않습니다.

group name:label 구문을 사용하여 레이블 그룹을 생성할 수 있습니다(예: Region:East 또는 Region:West). 이 두 레이블을 생성하는 경우 그룹 레이블은 Region(지역)이 되며 해당 그룹의 East(동부) 또는 West(서부) 중에서 선택할 수 있습니다.

디바이스 및 개체에 레이블 적용

디바이스에 레이블을 적용하려면 다음 단계를 수행합니다.

프로시저

단계 **1** 왼쪽 창에서 **Manage(**관리**)** > **Security Devices(**보안 디바이스**)**를 클릭합니다.
단계 **2** 왼쪽 창에서 **Objects(**개체**)**를 클릭합니다.
단계 **3** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.
단계 **4** 해당 디바이스 탭을 클릭합니다.
단계 **5** 하나 이상의 디바이스를 선택합니다.
단계 **6** 오른쪽의 **Add Groups and Labels(**그룹 및 레이블 추가**)** 필드에서 디바이스의 레이블을 지정합니다.
단계 **7** + 아이콘을 클릭합니다.

필터

Security Devices(보안 디바이스**)** 및 **Objects(**개체**)** 페이지에서 다양한 필터를 사용하여 원하는 디바이스 및 개체를 찾을 수 있습니다.

필터링하려면 Security Devices(보안 디바이스), Policies(정책) 및 Objects(개체) 탭의 왼쪽 창에서 을 클릭합니다.

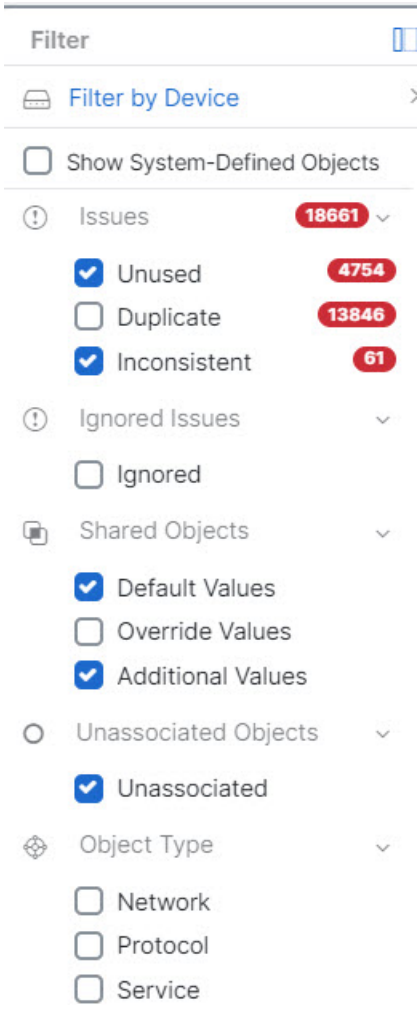
보안 디바이스 필터를 사용하면 디바이스 유형, 하드웨어 및 소프트웨어 버전, snort 버전, 구성 상태, 연결 상태, 충돌 탐지, 보안 디바이스 커넥터 및 레이블을 기준으로 필터링할 수 있습니다. 필터를 적용하여 선택한 디바이스 유형 탭 내에서 디바이스를 찾을 수 있습니다. 필터를 사용하여 선택한 디바이스 유형 탭 내에서 디바이스를 찾을 수 있습니다.

개체 필터를 사용하면 디바이스, 문제 유형, 공유 개체, 연결되지 않은 개체 및 개체 유형을 기준으로 필터링할 수 있습니다. 결과에 시스템 개체를 포함하거나 포함하지 않을 수 있습니다. 또한 검색 필드를 사용하여 필터 결과에서 특정 이름, IP 주소 또는 포트 번호를 포함하는 개체를 검색할 수 있습니다.

개체 유형 필터를 사용하면 네트워크 개체, 네트워크 그룹, URL 개체, URL 그룹, 서비스 개체, 서비스 그룹 등의 유형별로 개체를 필터링할 수 있습니다. 공유 개체 필터를 사용하면 기본값 또는 재정의 값이 있는 개체를 필터링할 수 있습니다.

디바이스 및 개체를 필터링할 때 검색 용어를 결합하여 몇 가지 잠재적 검색 전략을 생성하여 관련 결과를 찾을 수 있습니다.

다음 예제에서는 "문제(미사용 또는 일관성 없음) 및 공유 개체(기본값 또는 추가값 있음) 및 연결되지 않은 개체" 검색에 필터를 적용합니다.



Security Cloud Control 검색 기능 사용

Security Cloud Control 플랫폼에는 필요한 모든 항목을 쉽게 찾을 수 있는 매우 효율적인 검색 기능이 있습니다. 각 페이지의 검색 창은 해당 페이지의 콘텐츠에 따라 맞춤화되지만, 전역 검색을 사용하면 전체 테넌트에 대한 포괄적인 검색이 가능합니다. 이렇게 하면 필요한 정보를 신속하게 찾을 수 있으므로 시간과 노력을 절약할 수 있습니다.

페이지 레벨 검색

페이지 레벨 검색을 사용하면 보안 디바이스, 정책, 개체, VPN, 변경 로그 및 작업 페이지에서 특정 항목을 검색할 수 있습니다.

- **Security Devices(**보안 디바이스**)** 공간에서 검색 창에 입력을 시작하면 검색 기준에 맞는 디바이스가 표시됩니다. 디바이스의 일부 부분 이름, IP 주소 또는 물리적 디바이스의 일련 번호를 입력하여 디바이스를 찾을 수 있습니다.

- **Policies(**정책**)** 영역에서는 이름, 구성 요소 또는 사용된 개체를 기준으로 정책을 검색할 수 있습니다.
- **Objects(**개체**)** 영역에서는 개체 이름 또는 IP 주소 일부, 포트나 프로토콜을 입력하여 개체를 검색할 수 있습니다.
- **VPN** 영역에서는 터널 이름, 디바이스 이름 및 VPN 정책에 사용된 IP 주소를 기준으로 검색할 수 있습니다.
- **Change log(**변경 로그**)** 영역에서는 이벤트, 디바이스 이름 또는 작업을 기준으로 로그를 검색할 수 있습니다.

Procedure

단계 **1** 인터페이스 상단 근처의 검색 창으로 이동합니다.

단계 **2** 검색 표시줄에 검색 기준을 입력하면 해당 결과가 표시됩니다.

글로벌 검색

전체 검색 기능을 사용하면 Security Cloud Control에서 관리하는 디바이스를 빠르게 찾고 탐색할 수 있습니다.

모든 검색 결과는 선택한 인덱싱 옵션을 기반으로 합니다. 인덱싱 옵션은 다음과 같습니다.

- 전체 인덱싱 - 전체 인덱싱 프로세스를 호출해야 합니다. 이 프로세스는 시스템의 모든 디바이스와 개체를 검색하고 인덱싱을 호출한 후에만 검색 인덱스에 표시합니다. 전체 인덱싱을 호출하려면 관리 권한이 있어야 합니다.

  자세한 내용은 전체 인덱싱 시작을 참조하십시오.

- 증분 인덱싱 - 디바이스 또는 개체가 추가, 수정 또는 삭제될 때마다 검색 인덱스가 자동으로 업데이트되는 이벤트 기반 인덱싱 프로세스입니다.

검색 필드에 입력하는 정보는 대소문자를 구분하지 않습니다. 다음 엔터티를 사용하여 전역 검색을 수행할 수 있습니다.

- 디바이스 이름 - 부분 디바이스 이름, URL, IP 주소 또는 범위를 지원합니다.
- 개체 유형 - 개체 이름, 개체 설명 및 구성된 값을 지원합니다.
- 정책 유형 - 정책 이름, 정책 설명, 규칙 이름 및 규칙 설명을 지원합니다.

  Security Cloud Control에서 관리되는 클라우드 제공 방화벽 관리 센터 및 온프레미스 FMC는 다음 정책 유형을 지원합니다.

  - 액세스 제어 정책
  - 사전 필터 정책

- 위협 방어 NAT 정책

검색식을 입력하면 인터페이스에 검색 결과가 표시되기 시작하므로 검색을 실행하기 위해 *Enter* 키를 누를 필요가 없습니다.

검색 결과에는 검색 문자열과 일치하는 모든 디바이스 및 개체가 표시됩니다. 검색 문자열이 디바이스 또는 개체보다 더 많이 일치하면 결과가 범주(디바이스, 개체 및 connected_fmc) 아래에 나타납니다.

기본적으로 검색 결과의 첫 번째 항목이 강조 표시되고 해당 항목에 대한 관련 정보가 오른쪽 창에 나타납니다. 검색 결과를 스크롤하고 항목을 클릭하면 해당 정보를 볼 수 있습니다. 항목 옆의 화살표 아이콘을 클릭하여 해당 페이지로 이동할 수 있습니다.

참고

- 전역 검색은 중복 검색 결과를 표시하지 않습니다. 개체의 경우 공유 개체의 UID는 개체 보기로 이동하는 데 사용됩니다.
- Security Cloud Control에서 디바이스를 삭제하면, 연결된 모든 개체가 전역 검색 인덱스에서 제거됩니다.
- 정책에서 개체를 삭제하고 전체 인덱싱을 시작하기 전에 디바이스를 유지하면, 개체가 디바이스와 연결되어 있기 때문에 전역 검색 인덱스에 남아 있습니다.

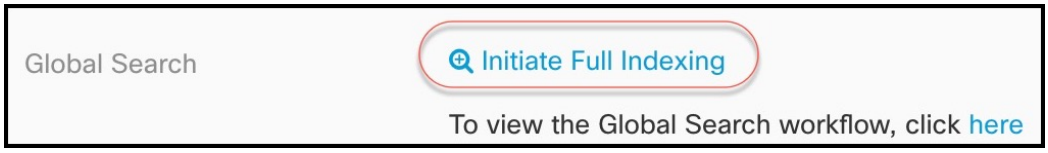
전체 인덱싱 시작

프로시저

단계 **1** Security Cloud Control 플랫폼 메뉴에서, **Products(**제품**)** > **Firewall(**방화벽**)**을 클릭합니다.

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

단계 **3** 전역 검색에서 **Initiate Full Indexing(**전체 인덱싱 시작**)**을 클릭하여 인덱싱을 트리거합니다.



참고
전체 인덱싱을 시작하면 Security Cloud Control 테넌트의 기존 인덱싱이 지워집니다.

단계 **4** 글로벌 검색 워크플로우를 보려면 **here(**여기**)**를 클릭합니다.

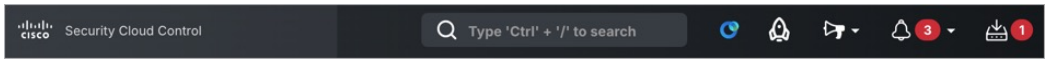
전역 검색 수행

프로시저

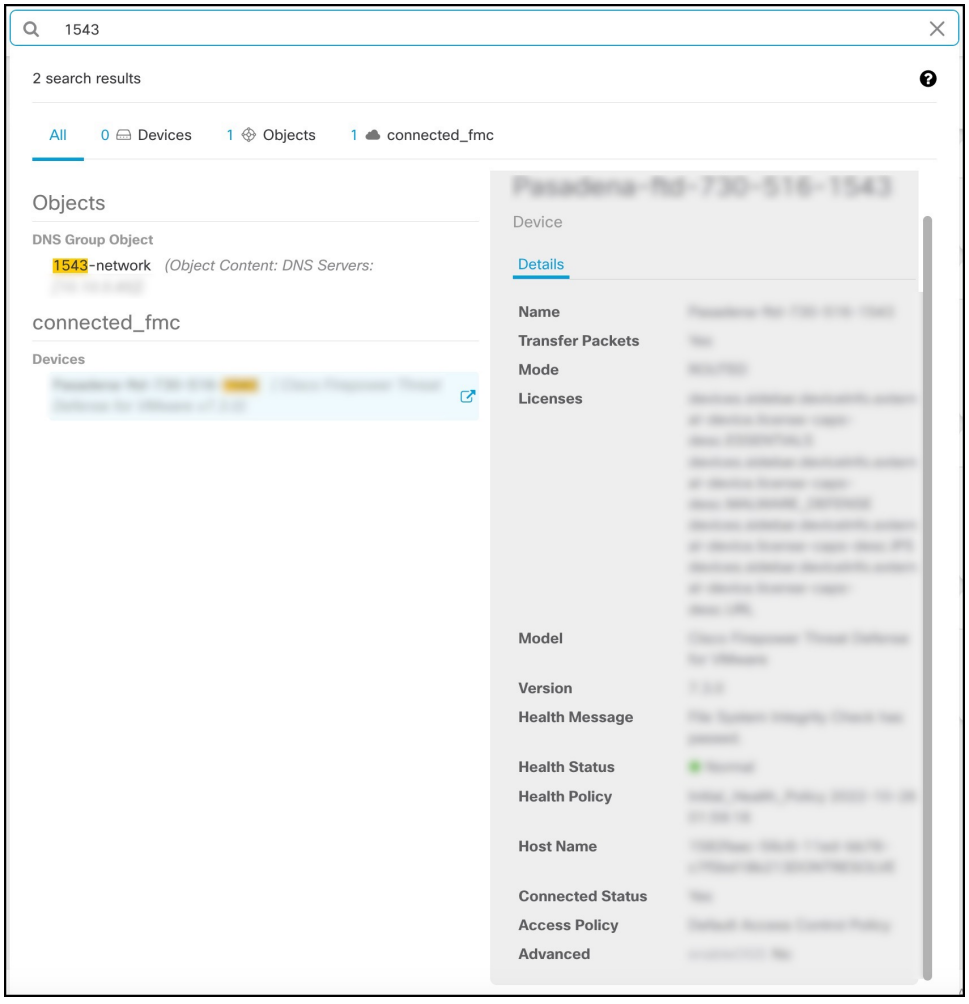
단계 **1** Security Cloud Control에 로그인합니다.

단계 **2** Security Cloud Control 페이지에서 검색 아이콘을 클릭하고 표시되는 검색 필드에 검색 문자열을 입력합니다.

또는 Windows에서는 **Ctrl** 키와 / 키를 동시에 누르고, Mac에서는 **Command** 키와 / 키를 동시에 눌러 검색창을 열 수 있습니다.



검색 문자열을 입력하기 시작하면 검색 결과에 가능한 항목 목록이 표시됩니다. 검색 결과는 모두, 디바이스, 개체 및 클라우드 제공 Firewall Management Center의 네 가지 범주 아래에 나타납니다. 오른쪽 창에는 선택한 검색 결과에 대한 정보가 표시됩니다.



단계 **3** 검색 결과에서 디바이스 또는 개체를 선택하고 화살표 아이콘을 클릭하여 검색 결과에서 해당 디바이스 및 개체 페이지로 이동합니다. 검색 결과에서 항목을 선택하고 화살표 아이콘을 클릭하여 검색 결과에서 해당 페이지로 이동합니다.

참고
클라우드 제공 Firewall Management Center에서 디바이스 검색 결과를 선택하면, Security Cloud Control에서 클라우드 제공 Firewall Management Center 사용자 인터페이스로 이동할 수 있습니다.

단계 **4** **X**를 클릭하여 검색 표시줄을 닫습니다.