테넌트 및 사용자 관리

Security Cloud Control 테넌트 관리

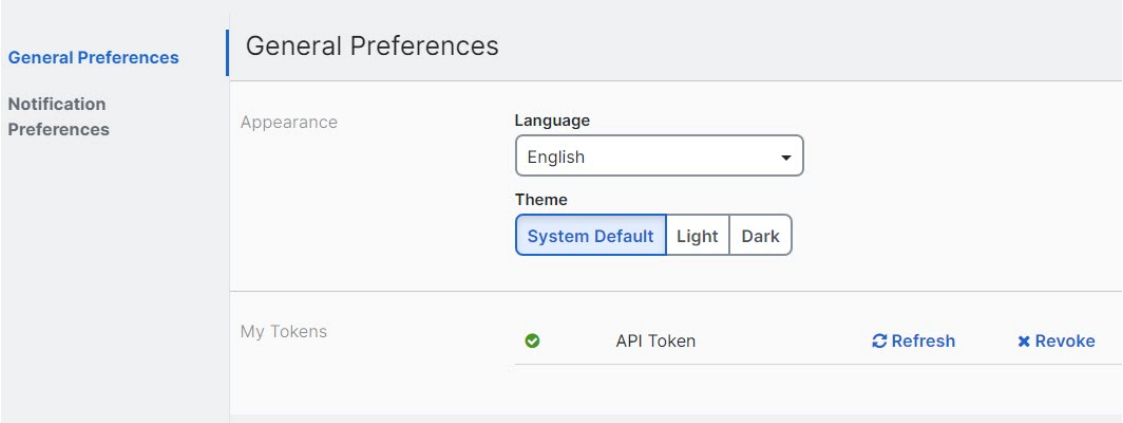
Security Cloud Control를 사용하면 테넌트, 사용자 및 알림 환경설정의 특정 측면을 사용자 지정할 수 있습니다. 사용자 지정 구성에 사용할 수 있는 다음 설정을 검토하십시오.

사용자 환경설정 구성

일반 Security Cloud Control 설정에 관한 다음 항목을 참조하십시오.

일반 환경설정

Security Cloud Control UI를 표시할 언어와 테마를 선택합니다. 이 선택은 이 변경을 수행하는 사용자에게만 영향을 미칩니다.



Security Cloud Control 웹 인터페이스 모양 변경

웹 인터페이스가 표시되는 방식을 변경할 수 있습니다.

프로시저

단계 **1** 사용자 이름 하단에 있는 드롭다운 목록에서 **Preferences(**환경설정**)**를 선택합니다.

단계 **2** **General Preferences(**일반 환경설정**)** 영역에서 **Theme(**테마**)**를 선택합니다.

- 라이트
- 다크

사용자 알림 환경설정

Security Cloud Control 테넌트에 연결된 디바이스에 특정 이벤트가 발생할 때마다 알림을 생성합니다. 여기에는 디바이스에서 수행한 작업, 만료 또는 만료된 디바이스 인증서 또는 보고서 생성 작업의 시작, 완료 또는 실패가 포함됩니다. 기본적으로 이러한 알림은 활성화되어 있으며 역할에 관계없이 테넌트와 연결된 모든 사용자에게 표시됩니다. 관심 있는 알림만 표시하도록 개인 알림 환경설정을 사용자 지정할 수 있습니다. 이러한 환경설정은 사용자에게 고유하며 테넌트에 연결된 다른 사용자에게 영향을 주지 않습니다.

참고 또한 아래에 나열된 알림에 대한 변경 사항은 실시간으로 자동 업데이트되며 구축이 필요하지 않습니다.

Username ID(사용자 이름 **ID)** > **Preferences(**환경설정**)** > **Notification Preferences(**알림 환경설정**)** 페이지에서 개인 환경설정을 확인합니다. 사용자 이름 ID는 항상 모든 페이지에서 Security Cloud Control의 오른쪽 상단에 있습니다. 이 페이지에서 아래의 "**Notify Me in Security Cloud Control When(**다음의 경우 알림**)**" 알림을 구성할 수 있습니다.

디바이스 워크플로우에 대한 알림 전송

- 구축 - 이 작업은 하며, SSH 또는 IOS 디바이스에 대한 통합 인스턴스는 포함하지 않습니다.
- 백업 - 이 작업은 FDM 관리 디바이스에만 적용됩니다.
- 업그레이드 - 이 작업은 ASA 및 FDM 관리 디바이스에만 적용됩니다.
- **Firewall Threat Defense**를 클라우드로 마이그레이션 - 이 작업은 Firewall Threat Defense Device Manager를 Firewall Management Center에서 Security Cloud Control로 변경할 때 적용됩니다.

디바이스 이벤트에 대한 알림 전송

- 오프라인 상태 - 이 작업은 테넌트와 연결된 모든 디바이스에 적용됩니다.
- 온라인 재전환 - 이 작업은 테넌트와 연결된 모든 디바이스에 적용됩니다.
- 충돌 탐지됨 - 이 작업은 테넌트와 연결된 모든 디바이스에 적용됩니다.
- **HA** 상태 변경됨 - 이 작업은 HA 또는 페일오버 쌍 내의 디바이스, 현재 상태 및 변경된 상태를 나타냅니다. 이 작업은 테넌트와 연결된 모든 HA 및 페일오버 구성에 적용됩니다.
- 사이트 간 세션 연결 끊김 - 이 작업은 테넌트에 구성된 모든 사이트 간 VPN 구성에 적용됩니다.

이벤트 검색 보고서 생성을 위한 알림 전송

- 보고서 생성 시작됨: 보고서 생성 작업이 시작되면 알림을 수신합니다. 이는 즉시 및 예약된 검색에 모두 적용됩니다.
- 보고서 생성 완료: 보고서 생성 작업이 종료되면 알림을 받습니다. 이는 즉시 및 예약된 검색에 모두 적용됩니다.
- 보고서 생성 실패: 보고서 생성 작업이 실패하면 알림을 받습니다. 이는 즉시 및 예약된 검색에 모두 적용됩니다. 매개변수 또는 쿼리를 확인하고 다시 시도하십시오.

알림 환경설정 선택 취소

기본적으로 모든 이벤트는 활성화되고 알림을 생성합니다. 위에서 언급한 이벤트에 의해 생성된 알림을 선택 취소하려면 알림 유형을 수동으로 선택 취소 해야 합니다. 변경 사항을 확인하려면 **Save(**저장**)**를 클릭해야 합니다.

이메일 공지

위에서 언급한 알림을 수신하려면 **Email Alerts(**이메일 알림**)** 토글을 활성화합니다. 이메일로 수신할 알림을 선택하고 **Save(**저장**)** 버튼을 클릭합니다. 기본적으로 **Use Security Cloud Control notification settings above(**위의 알림 설정 사용**)**는 선택되어 있습니다. 즉, 이 페이지의 "Send Alerts When...(다음의 경우 알림 전송...)" 섹션에서 선택한 것과 동일한 모든 알림 및 이벤트에 대한 이메일 알림을 수신하게 됩니다.

위에서 언급한 이벤트 또는 경고 중 일부만 이메일로 전달하려면 **Use Security Cloud Control notification settings above(**위의 알림 설정 사용**)**의 선택을 취소합니다. 이 작업은 사용 가능한 알림을 수정하고 개인화하기 위한 추가 위치를 생성합니다. 이는 리던던시(redundancy)를 줄이는 데 도움이 될 수 있습니다.

Security Cloud Control 알림 보기

알림  아이콘을 클릭하여 테넌트에 온보딩한 디바이스에 발생했거나 영향을 미친 최신 알림을 확인합니다. **Notification Settings(**알림 설정**)** 페이지에서 선택하는 항목은 Security Cloud Control에 표시되는 알림 유형에 영향을 미칩니다. 자세한 내용을 보려면 계속 읽으십시오.

이 드롭다운 페이지는 Overview(개요), All(모두), Dismissed(해제됨)의 3개 탭으로 그룹화됩니다.

개요 탭

Overview(개요**)** 탭은 가장 최근의 우선 순위가 높은 알림 및 구독한 이벤트를 조합하여 표시합니다. 우선순위가 높은 이벤트는 다음과 같습니다.

- 구축 실패
- 백업 실패
- 업그레이드 실패
- FTD를 cdFMC로 마이그레이션 실패
- 디바이스가 오프라인 상태가 됨
- 디바이스 HA 상태가 변경됨
- 디바이스 인증서 만료

Notifications(알림 설정) 창에서 Notification Settings(알림 설정)를 클릭하거나 **UserID(**사용자 **ID)** > **User Preferences(**사용자 환경설정**)** 페이지에서 수신할 알림을 구성할 수 있습니다. 대시보드 오른쪽 상단 모서리에 있는 User ID(사용자 ID) 버튼.

All(모두) 탭

All(모두**)** 탭은 이메일 구독 알림 및 높은 우선 순위로 나열된 모든 항목을 포함하여 우선 순위와 상관없이 모든 알림을 표시합니다.

Dismissed(해제됨) 탭

Dismissed(해제됨**)** 탭에는 해제한 알림이 표시됩니다. 알림의 "**x**"를 클릭하면 개별 알림을 무시할 수 있습니다.

드롭다운 메뉴에서 알림 **Dismiss(**해제**)**를 선택하면 "개요" 및 "모두" 탭 모두 에서 알림이 해제됩니다. **Dismiss(**해제**)** 탭에 30일 동안 유지되며, 그 이후에는 Security Cloud Control에서 제거됩니다.

알림 검색

알림 드롭다운 창을 보는 경우, 위에서 언급한 탭 중 하나를 사용하여 키워드나 알림을 쿼리할 수 있습니다.

테넌트 설정

디바이스 변경 사항 자동 수락 옵션 활성화

디바이스 변경에 대한 자동 수락을 활성화하면 Security Cloud Control가 디바이스에서 직접 수행된 모든 변경 사항을 자동으로 수락할 수 있습니다. 이 옵션을 비활성화된 상태로 두거나 나중에 비활성화하는 경우 수락하기 전에 각 디바이스 충돌을 검토해야 합니다.

디바이스 변경 사항에 대한 자동 수락을 활성화하려면 다음 절차를 따르십시오.

Procedure

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

단계 **2** **Enable the option to auto-accept device changes(**디바이스 변경 사항을 자동으로 수락하는 옵션 활성화**)** 아래의 슬라이더를 클릭합니다.

Multicloud Defense와의 개체 공유 활성화

Security Cloud Control에서 Multicloud Defense 네트워크 개체 공유를 활성화하려면 다음 절차를 수행합니다.

SUMMARY STEPS

1. 왼쪽 창에서 **Administration(**관리**)** > **General Settings(**일반 설정**)**를 클릭합니다.
2. **Enable object Sharing with Multicloud Defense(Multicloud Defense**로 개체 공유 활성화**)**아래의 슬라이더를 클릭합니다.

DETAILED STEPS

프로시저

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

단계 **2** **Enable object Sharing with Multicloud Defense(Multicloud Defense**로 개체 공유 활성화**)**아래의 슬라이더를 클릭합니다.

기본 충돌 탐지 간격

이 간격은 Security Cloud Control가 변경 사항을 위해 온보딩된 디바이스를 폴링하는 빈도를 결정합니다. 이 선택은 이 테넌트로 관리되는 모든 디바이스에 영향을 주며 언제든지 변경할 수 있습니다.

Note 하나 이상의 디바이스를 선택한 후 **Security Devices(**보안 디바이스**)** 페이지에서 사용 가능한 **Conflict Detection(**충돌 탐지**)** 옵션을 통해 이 선택 항목을 재정의할 수 있습니다.

이 옵션을 구성하고 충돌 탐지를 위한 새 간격을 선택하려면 다음 절차를 수행합니다.

Procedure

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

단계 **2** **Default Conflict Detection Interval(**기본 충돌 탐지 간격**)**의 드롭다운 메뉴를 클릭하고 시간 값을 선택합니다.

웹 분석

웹 분석은 페이지 히트를 기반으로 익명의 제품 사용 정보를 Cisco에 제공합니다. 이 정보에는 확인한 페이지, 특정 페이지를 사용한 시간, 브라우저 버전, 제품 버전, 디바이스 호스트 이름 등이 포함됩니다. Cisco는 이 정보를 활용해 기능 사용 패턴을 확인하고 제품을 개선할 수 있습니다. 모든 사용량 데이터는 익명으로 전송되며 민감한 데이터는 전송되지 않습니다.

웹 분석은 기본적으로 활성화됩니다. 웹 분석을 비활성화하거나 나중에 활성화하려면 다음 절차를 따르십시오.

Procedure

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

단계 **2** 웹 분석 아래의 토글을 클릭합니다.

Cisco Talos 와 이벤트 데이터 공유

시스코의 위협 인텔리전스 조직인 Talos와 디바이스의 악의적인 이벤트 데이터를 공유합니다. 이벤트 데이터를 공유하면 Talos 위협 탐지 및 대응 기능을 개선하는 데 도움이 되며, 이를 통해 네트워크에 더 맞춤형 보안 업데이트를 제공하고 새로운 위협에 대한 보호를 강화할 수 있습니다.

Talos에 대한 자세한 내용은 Cisco Talos 제품 페이지를 참조하십시오.

Talos와 이벤트 데이터 공유 활성화 토글 버튼을 활성화해도 클라우드 제공 Firewall Management Center에서 **Talos** 위협 추적 텔레메트리 기능이 자동으로 활성화되지는 않습니다. 이 기능으로 최상

의 결과를 얻으려면 클라우드 제공 Firewall Management Center에서 **Talos** 위협 추적 텔레메트리도 활성화해야 합니다. 자세한 내용은 침입 정책 환경설정을 참조하십시오.

Talos와 이벤트 데이터 공유는 기본적으로 활성화되어 있습니다. 옵트아웃하려면 다음 절차를 따르십시오.

프로시저

단계 **1** 왼쪽 탐색 모음에서 **Administration(**관리**)** > **General Settings(**일반 설정**)**를 클릭합니다.

단계 **2** 설정을 비활성화하려면 **Talos**와 이벤트 데이터 공유 활성화 토글 버튼을 클릭합니다.

참고
이벤트 데이터를 공유하면 Talos 네트워크에 대한 관련 보안 인사이트를 제공할 수 있습니다. 이 설정을 비활성화하면 Talos의 기능을 완전히 활용하는 기능이 제한되어 진화하는 위협에 대한 네트워크 방어에 영향을 줄 수 있습니다.

테넌트 ID

테넌트 ID는 테넌트를 식별합니다. 이 정보는Cisco TAC(Technical Assistance Center)에 문의해야 하는 경우에 유용합니다.

테넌트 이름

테넌트 이름도 테넌트를 식별합니다. 테넌트 이름은 조직 이름이 아닙니다. 이 정보는Cisco TAC(Technical Assistance Center)에 문의해야 하는 경우에 유용합니다.

Security Cloud Control Platform Navigator

Platform Navigator는 9개의 블록으로 구성된 애플리케이션 크로스 런처()로, Security Cloud Control의 오른쪽 상단에 표시됩니다. 다음 Cisco 네트워킹 및 보안 애플리케이션으로 쉽게 교차 실행할 수 있습니다.

네트워킹 애플리케이션

- **Catalyst** - Cisco Catalyst 제품에는 다양한 네트워크 스위치, 무선 컨트롤러, 무선 액세스 포인트, 에지 플랫폼 및 라우터가 포함되어 있어 엔터프라이즈급 비즈니스 요구 사항부터 고강도 및 견고한 네트워킹 환경까지 지원합니다.
- **Intersight** - Cisco Intersight는 고급 인프라, 워크로드 최적화, Kubernetes 서비스의 선택적 모듈식 기능으로 구성된 클라우드 운영 플랫폼입니다. Cisco Intersight 인프라 서비스에는 물리적 및 가상 인프라의 구축, 모니터링, 관리 및 지원이 포함됩니다. Cisco UCS (Unified Computing System) 및 Cisco HCI(HyperFlex hyperconverged infrastructure), 및 기타 타사 Intersight 연결 대상을 지원합니다.

- **IoT** 운영 대시보드 - Cisco IoT 운영 대시보드는 운영팀이 산업용 네트워킹 디바이스와 연결된 산업 자산을 대규모로 안전하게 연결, 유지 관리하고 인사이트를 얻을 수 있도록 지원하는 클라우드 기반 IoT 서비스 플랫폼입니다. 운영팀은 연결된 모든 산업 자산을 종합적으로 파악하여 운영을 간소화하고 비즈니스 연속성을 촉진하는 데 도움이 되는 귀중한 인사이트를 발견할 수 있습니다.
- **Meraki** - Cisco Meraki는 Cisco Meraki 디바이스를 위한 중앙 집중식 관리 플랫폼을 제공하는 IT 및 IoT 클라우드 관리 플랫폼입니다.
- **Spaces** - Cisco Spaces는 클라우드 기반 위치 서비스 플랫폼으로, 조직이 물리적 공간에서 사람과 사물이 어떻게 움직이는지에 대한 인사이트를 얻을 수 있도록 지원합니다. 이러한 인사이트를 통해 가치 있고 관련성 있는 컨텍스트 인게이지먼트를 제공할 수 있습니다. 조직은 사람들의 이동 경로를 파악하는 것 외에도 자산의 위치, 이동 및 활용도를 모니터링하여 운영 효율성을 높일 수 있습니다.
- **ThousandEyes** - Cisco ThousandEyes는 웹 애플리케이션, 서비스 및 네트워크의 가용성과 성능을 모니터링하고 측정하는 데 도움이 되는 클라우드 서비스 제품군입니다. 모든 네트워크에서 모든 사용자부터 모든 애플리케이션에 대한 엔드투엔드 가시성을 제공하여 기업이 문제의 원인을 신속하게 파악하고, 더 빠르게 문제를 해결하며, 성능을 효과적으로 관리할 수 있도록 지원합니다.
- **Workflows** - Cisco Workflows는 더 큰 Cisco 네트워킹 클라우드 비전의 일부인 클라우드 호스팅 자동화 애플리케이션입니다. Workflows는 Cisco에서 제공하거나 직접 구축할 수 있는 맞춤형 및 사전 제작된 자동화 템플릿과 다양한 어댑터 옵션을 통해 Cisco 및 타사 애플리케이션 모두에서 반복적이고 오류가 발생하기 쉬운 작업을 간소화하여 클라우드 또는 온프레미스의 목표에 도달함으로써 현재 Cisco 고객에게 도메인 간 자동화 기능을 이용할 수 있는 권한을 제공합니다.

보안 애플리케이션

- **Duo Security** - Cisco Duo는 모든 사용자, 디바이스, 애플리케이션의 민감한 데이터에 대한 액세스를 보호하는 2단계 인증 기능을 갖춘 사용자 중심의 제로 트러스트 보안 플랫폼입니다. 적응형 정책, SSO(Single Sign-On, 단일 인증), 고급 엔드포인트 가시성 등의 기능을 제공하여 원격 액세스를 보호하고 비즈니스 연속성을 유지하기 위한 종합적인 솔루션입니다.
- **Secure Access** - Cisco Secure Access는 단일 클라우드 관리 콘솔, 통합 클라이언트, 중앙 집중식 정책 생성 및 통합 보고를 통해 IT 운영을 간소화합니다. 하나의 솔루션에 통합된 광범위한 보안 기능(ZTNA, SWG, CASB, FWaaS, DNS 보안, RBI 등)은 제로 트러스트 원칙을 적용하고 세분화된 보안 정책을 시행하여 보안 위험을 완화합니다. 시장을 선도하는 Talos Threat Intelligence는 탁월한 위협 차단 기능을 통해 위험을 완화하고 조사 속도를 높입니다.
- **Secure Endpoint** - Cisco Secure Endpoint는 이전에 엔드포인트용 Cisco AMP였으며, 이 솔루션은 침해를 방지하고 위협을 신속하게 탐지, 억제 및 수정하도록 설계된 클라우드 관리형 엔드포인트 보안 솔루션입니다. 보안 분석가가 초기 발생 원인을 파악하고 격리할 수 있는 고급 추적 기능을 갖춘 클라우드 기반 스캐너를 통해 파일을 즉시 검사하고, 악성 파일로 확인된 파일을 소급하여 격리할 수 있습니다.
- **Cisco Security Provisioning** 및 **Administration**—Cisco Security Provisioning 및 Administration는 Cisco Security Cloud 전반에서 Cisco 보안 제품 인스턴스, 사용자 ID 및 사용자 액세스 관리를 중

앙 집중식으로 관리하는 웹 애플리케이션입니다. Security Cloud Control 관리자는 새로운 Security Cloud 엔터프라이즈를 생성하고, 엔터프라이즈의 사용자를 관리하고, 도메인을 클레임하고, 조직의 SSO ID 제공자를 통합하는 등의 작업을 수행할 수 있습니다.

- **XDR** - Cisco XDR(Extended Detection and Response)는 보안 운영을 간소화하고 보안팀이 정교한 위협을 탐지하고 우선 순위를 지정하여 대응할 수 있도록 설계된 클라우드 기반 솔루션입니다. Cisco XDR은 Cisco 및 타사 보안 솔루션을 통합 플랫폼에 통합함으로써 위협 관리에 대한 포괄적인 접근 방식을 제공합니다. Talos에서 제공하는 Threat Intelligence와 통합된 Cisco XDR은 추가적인 컨텍스트 및 자산 인사이트를 통해 사고 데이터를 보강하여 오탐을 줄이고 전반적인 위협 탐지, 대응 및 포렌식 기능을 강화합니다.

테넌트 알림 설정

Security Cloud Control 툴바에서 알림 버튼  을 클릭합니다.

테넌트과 연결된 모든 사용자가 이러한 알림을 자동으로 수신합니다. 또한 이러한 알림의 일부 또는 모두가 사용자에게 전달될 수 있습니다.

Note 이러한 설정을 변경하려면 슈퍼 관리자 사용자 역할이 있어야 합니다. 자세한 내용은 사용자 역할을 참조하십시오.

이메일 가입자

Security Cloud Control 테넌트의 알림을 수신하는 이메일을 추가하거나 수정합니다. 자세한 내용은 이메일 가입자 활성화, on page 9을 참조하십시오.

서비스 통합

메시징 앱에서 수신 **Webhook**를 활성화하고 앱 대시보드에서 직접 Security Cloud Control 알림을 수신합니다. 자세한 내용은 Security Cloud Control 알림에 대한 서비스 통합 활성화를 참조하십시오.

이메일 가입자 활성화

Security Cloud Control의 이메일 알림은 작업 유형 및 영향을 받는 디바이스를 나타냅니다.

디바이스의 현재 상태 및 작업 내용에 대한 자세한 정보를 알아보려면 Security Cloud Control에 로그인하여 영향을 받는 디바이스의 변경 로그를 검토하는 것이 좋습니다.

경고! 메일러를 추가하는 경우 올바른 이메일을 입력해야 합니다. Security Cloud Control는 테넌트와 연결된 알려진 사용자에 대한 이메일 주소를 확인하지 않습니다.

이메일 구독 추가

시작하기 전에

이메일 구독 목록을 보려면 관리자여야 하며, 이메일 구독을 추가, 제거 또는 편집하려면 슈퍼 관리자여야 합니다.

프로시저

단계 **1** 왼쪽 창에서 **Administration(**관리**)** > **Notification Settings(**알림 설정**)**를 클릭합니다.

단계 **2** 페이지의 오른쪽 상단에 있는 **+** 아이콘을 클릭합니다.

단계 **3** 텍스트 필드에 유효한 이메일 주소를 입력합니다.

단계 **4** 가입자에게 알리려는 이벤트 및 알림의 해당 체크 박스를 선택하고 선택 취소합니다.

단계 **5** **Save(**저장**)**를 클릭합니다. 언제든지 **Cancel(**취소**)**을 클릭하여 테넌트에 대한 새 이메일 구독을 생성할 수 있습니다.

이메일 구독 편집

시작하기 전에

이메일 구독 목록을 보려면 관리자여야 하며, 이메일 구독을 추가, 제거 또는 편집하려면 슈퍼 관리자여야 합니다.

프로시저

단계 **1** 왼쪽 창에서 **Administration(**관리**)** > **Notification Settings(**알림 설정**)**를 클릭합니다.

단계 **2** 이메일 구독을 위해 편집하도록 활성화하려는 이메일 주소를 찾습니다.

단계 **3** 편집 아이콘을 클릭합니다.

단계 **4** 구성된 이메일 주소로 알림을 전송하려면 Security Cloud Control에 대한 다음 속성을 수정합니다.

- 이메일 주소
- 디바이스 워크플로우
- 디바이스 이벤트
- 이벤트 로그 보고서

단계 **5** **Ok(**확인**)**를 클릭합니다. 언제든지 **Cancel(**취소**)**을 클릭하여 이메일 구독에 대한 변경 사항을 무효화할 수 있습니다.

이메일 구독 삭제

이메일 구독 목록에서 메일러를 삭제하려면 다음 절차를 사용합니다.

시작하기 전에

이메일 구독 목록을 보려면 관리자여야 하며, 이메일 구독을 추가, 제거 또는 편집하려면 슈퍼 관리자여야 합니다.

프로시저

단계 **1** 왼쪽 창에서 **Administration(**관리**)** > **Notification Settings(**알림 설정**)**를 클릭합니다.

단계 **2** 테넌트의 이메일 구독에서 제거할 사용자를 찾습니다.

단계 **3** 제거할 사용자에 대해 **Remove(**제거**)** 아이콘을 클릭합니다.

단계 **4** 구독 목록에서 사용자를 제거할지 확인합니다. 이는 사용자 기능에 영향을 주지 않습니다.

Security Cloud Control 알림을 위한 서비스 통합 활성화

서비스 통합을 활성화하여 지정된 메시징 애플리케이션 또는 서비스를 통해 Security Cloud Control 알림을 전달합니다. 알림을 받으려면 메시지 프로그램에서 웹후크 URL을 생성하고 Security Cloud Control의 **Notification Settings(**알림 설정**)** 페이지에서 해당 웹후크를 Security Cloud Control에 지정해야 합니다.

Security Cloud Control는 기본적으로 Cisco Webex, Microsoft Teams 및 Slack을 서비스 통합으로 지원합니다. 이러한 서비스로 전송되는 메시지는 채널 및 자동화된 봇용으로 특별히 형식이 지정됩니다.

참고 Webhook별로 수신할 알림에 대해 해당 상자를 선택해야 합니다.

Webex Teams용 수신 **Webhook**

시작하기 전에

Security Cloud Control 알림은 지정된 작업 공간에 표시되거나 비공개 메시지에 자동 봇으로 표시됩니다. 이 절차를 완료하기 전에 다음을 수행해야 합니다.

- Webex 어카운트.
- Security Cloud Control 어카운트 및 테넌트.

Webex Teams에 대해 수신 웹후크를 허용하려면 다음 절차를 따르십시오.

프로시저

단계 1 Webex apphub를 엽니다.

단계 2 페이지 맨 위에서 **Connect(**연결**)**를 클릭합니다.

단계 3 페이지 하단으로 스크롤하여 다음을 구성합니다.

- **Webhook** 이름 - 이 애플리케이션에서 제공하는 메시지를 식별하기 위한 이름을 입력합니다.
- **Space(**공간**)** 선택 - 드롭다운 메뉴를 사용하여 Webex **Space(**공간**)**를 선택합니다. 공간이 이미 Webex 팀에 존재해야 하며 이 공간에 대한 액세스 권한이 있어야 합니다. 공간이 존재하지 않는 경우 Webex Teams에서 새 공간을 만들고 애플리케이션의 구성 페이지를 새로 고쳐 새 공간을 표시할 수 있습니다.

참고
과거에 Webex 수신 웹훅을 구성한 적이 있고 다시 활성화하는 경우, 이전 웹훅은 이 페이지 하단에 유지됩니다. 이전 웹훅이 더 이상 필요하지 않거나 웹엑스 공간이 더 이상 존재하지 않는 경우 삭제할 수 있습니다.

단계 4 **Add(**추가**)**를 선택합니다. 선택한 Webex Space는 애플리케이션이 추가되었다는 알림을 받게 됩니다.

단계 5 웹후크 URL을 복사합니다.

단계 6 Security Cloud Control에 로그인합니다.

단계 7 왼쪽 창에서 **Administration(**관리**)** > **Notification Settings(**알림 설정**)**를 클릭합니다.

단계 8 선택한 알림이 올바른지 검사하고 확인합니다. 그렇지 않은 경우 서비스 통합에 연결하기 전에 알림 선택을 수정할 것을 강력하게 권장합니다.

단계 9 **Service Integrations(**서비스 통합**)**으로 스크롤합니다.

단계 10 파란색 플러스 버튼을 클릭합니다.

단계 11 **Name(**이름**)**을 입력합니다. 이 이름은 구성된 서비스 통합으로 Security Cloud Control에 나타납니다. 구성된 서비스로 전달되는 이벤트에는 나타나지 않습니다.

단계 12 드롭다운 메뉴를 확장하고 **Webex**를 서비스 유형으로 선택합니다.

단계 13 서비스에서 생성한 웹후크 URL을 붙여넣습니다.

단계 14 **OK(**확인**)**를 클릭합니다.

Microsoft Teams용 수신 Webhook

Security Cloud Control에서 Microsoft Teams에 알림을 전달할 수 있습니다. 이러한 메시지는 Microsoft Teams에서 지정된 채널에 표시되거나 개인 채팅 메시지 내 자동화된 봇으로 표시됩니다. 이 기능 활성화하려면 Microsoft Teams에서 Webhook URL을 생성하고 Security Cloud Control가 해당 Webhook를 가리키도록 해야 합니다. Microsoft Teams 채널에 수신 Webhook를 추가하는 방법에 대한 자세한 내용은 Microsoft Teams용 워크플로우를 사용하여 수신 Webhook 생성 문서를 참조하십시오.

사전 요건

다음은 Microsoft Teams에서 Security Cloud Control 알림을 허용하기 위한 사전 요건입니다.

- Microsoft Teams 어카운트.

- Security Cloud Control 어카운트 및 테넌트.

이 절차를 Use Microsoft Teams에서 Webhook URL을 생성하고 Security Cloud Control에서 알림을 활성화합니다.

프로시저

단계 **1** Microsoft Teams 어카운트에 로그인합니다.

단계 **2** **New Teams** 클라이언트에서 **Teams**를 클릭하고 수신 Webhook을 추가할 채널로 이동합니다.

단계 **3** 채널 이름 옆에 있는 **More options •••(**추가 옵션 **•••)**를 클릭합니다.

단계 **4** **Workflows(**워크플로우**)**를 클릭합니다.

단계 **5** **Webhook** 요청이 수신되면 채널에 게시를 클릭합니다.

단계 **6** webhook의 이름을 제공하고 **Next(**다음**)**를 클릭합니다.

단계 **7** 게시해야 하는 채널을 선택합니다.

Microsoft Teams 채팅이나 채널에서 이 워크플로를 사용하면 해당 필드에 자동으로 값이 채워집니다.

단계 **8** 요구하는 세부 정보를 입력한 후 **Add workflow(**워크플로우 추가**)**를 클릭합니다.

단계 **9** 표시되는 대화 상자에서 고유한 웹후크 URL을 복사합니다. URL은 채널에 매핑됩니다. Teams에 정보를 전송할 수 있습니다.

단계 **10** Security Cloud Control에 로그인합니다.

단계 **11** 왼쪽 창에서 **Administration(**관리**)** > **Notification Settings(**알림 설정**)**를 클릭합니다.

단계 **12** **Service Integrations(**서비스 통합**)**으로 스크롤합니다.

단계 **13** 파란색 플러스 버튼을 클릭합니다.

단계 **14** **Name(**이름**)**을 입력합니다.

이 이름은 구성된 서비스 통합으로 Security Cloud Control에 표시됩니다. 단, 구성된 서비스로 전달되는 이벤트에는 나타나지 않습니다.

단계 **15** 드롭다운 목록을 확장하고 **Service Type(**서비스 유형**)**으로 **Microsoft Teams**를 선택합니다.

단계 **16** Microsoft Teams에서 생성한 웹후크 URL을 **URL**에 붙여넣습니다.

단계 **17** **Send Alerts When(**다음 경우에 알림 전송**)**에서 선택한 알림이 올바른지 검사하고 확인합니다. 그렇지 않은 경우 계속하기 전에 알림 선택을 수정합니다.

단계 **18** **Save(**저장**)**를 클릭합니다.

Slack용 수신 **Webhook**

Security Cloud Control 알림은 지정된 채널에 표시되거나 비공개 메시지에 자동 봇으로 표시됩니다. Slack이 수신 웹후크를 처리하는 방법에 대한 자세한 내용은 Slack 앱을 참조하십시오.

Slack에 대해 수신 웹후크를 허용하려면 다음 절차를 따르십시오.

프로시저

단계 **1** Slack어카운트에 로그인합니다.

단계 **2** 왼쪽 패널에서 아래로 스크롤하여 **Add Apps(**앱 추가**)**를 선택합니다.

단계 **3** **Incoming Webhooks(**수신 웹후크**)**에 대한 애플리케이션 디렉토리를 검색하고 앱을 찾습니다. **Add(**추가**)**를 선택합니다.

단계 **4** Slack 워크스페이스의 관리자가 아닌 경우, 조직의 관리자에게 요청을 보내고 앱이 어카운트에 추가될 때까지 기다려야 합니다. **Request Configuration(**요청 구성**)**을 선택합니다. 선택적 메시지를 입력하고 **Submit Request(**요청 제출**)**을 선택합니다.

단계 **5** 워크스페이스에 수신 웹후크 앱이 활성화되면 Slack 설정 페이지를 새로고침하고 **Add New Webhook to Workspace(**워크스페이스에 새 웹후크 추가**)**를 선택합니다.

단계 **6** 드롭다운 메뉴를 사용하여 Security Cloud Control 알림을 표시할 Slack 채널을 선택합니다. **Authorize(**승인**)**을 선택합니다. 요청이 활성화되기를 기다리는 동안 이 페이지에서 다른 곳으로 이동하려면 Slack에 로그인하고 왼쪽 상단 모서리에서 작업 공간 이름을 선택하기만 하면 됩니다. 드롭다운 메뉴에서 **Customize Workspace(**작업 공간 사용자 지정**)**을 선택하고 **Configure Apps(**앱 구성**)**을 선택합니다. **Custom Integrations(**사용자 지정 통합**)** > **Manage (**관리**)**로 이동합니다. **Incoming Webhooks(**수신 웹후크**)**를 선택하여 앱의 랜딩 페이지를 연 다음 탭에서 **Configuration(**구성**)**을 선택합니다. 그러면 이 앱이 활성화된 작업 공간 내의 모든 사용자가 나열됩니다. 어카운트 구성만 보고 편집할 수 있습니다. 작업 공간 이름을 선택하여 구성을 편집하고 계속 진행합니다.

단계 **7** Slack 설정 페이지는 앱의 구성 페이지로 리디렉션됩니다. 웹후크 URL을 찾아 복사합니다.

단계 **8** Security Cloud Control에 로그인합니다.

단계 **9** 왼쪽 창에서 **Administration(**관리**)** > **Notification Settings(**알림 설정**)**를 클릭합니다.

단계 **10** 선택한 알림이 올바른지 검사하고 확인합니다. 그렇지 않은 경우 서비스 통합에 연결하기 전에 알림 선택을 수정할 것을 강력하게 권장합니다.

단계 **11** **Service Integrations(**서비스 통합**)**으로 스크롤합니다.

단계 **12** 파란색 플러스 버튼을 클릭합니다.

단계 **13** **Name(**이름**)**을 입력합니다. 이 이름은 구성된 서비스 통합으로 Security Cloud Control에 나타납니다. 구성된 서비스로 전달되는 이벤트에는 나타나지 않습니다.

단계 **14** 드롭다운 메뉴를 확장하고 서비스 유형으로 **Slack**을 선택합니다.

단계 **15** 서비스에서 생성한 웹후크 URL을 붙여넣습니다.

단계 **16** OK(확인)를 클릭합니다.

맞춤형 통합용 수신 **Webhook**

시작하기 전에

Security Cloud Control는 사용자 지정 통합을 위한 메시지 형식을 지정하지 않습니다. 사용자 지정 서비스 또는 애플리케이션을 통합하기로 선택한 경우 Security Cloud Control는 JSON 메시지를 보냅니다.

수신 웹후크를 활성화하고 웹후크 URL을 생성하는 방법에 대한 서비스 설명서를 참조하십시오. 웹후크 URL이 있으면 아래 절차를 사용하여 웹후크를 활성화합니다.

프로시저

단계 **1** 선택한 사용자 지정 서비스 또는 애플리케이션에서 웹후크 URL을 생성하고 복사합니다.

단계 **2** Security Cloud Control에 로그인합니다.

단계 **3** 왼쪽 창에서 **Administration(**관리**)** > **Notification Settings(**알림 설정**)**를 클릭합니다.

단계 **4** 선택한 알림이 올바른지 검사하고 확인합니다. 그렇지 않은 경우 서비스 통합에 연결하기 전에 알림 선택을 수정할 것을 강력하게 권장합니다.

단계 **5** **Service Integrations(**서비스 통합**)**으로 스크롤합니다.

단계 **6** 파란색 플러스 버튼을 클릭합니다.

단계 **7** **Name(**이름**)**을 입력합니다. 이 이름은 구성된 서비스 통합으로 Security Cloud Control에 나타납니다. 구성된 서비스로 전달되는 이벤트에는 나타나지 않습니다.

단계 **8** 드롭다운 메뉴를 확장하고 서비스 유형으로 **Custom(**사용자 지정**)**을 선택합니다.

단계 **9** 서비스에서 생성한 웹후크 URL을 붙여넣습니다.

단계 **10** OK(확인)를 클릭합니다.

로깅 설정

월별 이벤트 로깅 한도와 한도가 재설정될 때까지 남은 일수를 확인합니다. 저장된 로깅은 Cisco cloud가 수신한 압축된 이벤트 데이터를 나타냅니다.

지난 12개월 동안 테넌트가 받은 로그를 보려면 **View Historical Usage(**기록 히스토리 보기**)**를 클릭합니다.

추가 스토리지를 요청하는 데 사용할 수 있는 링크도 있습니다.

SAML SSO(Single Sign-On)를 Security Cloud Control과 통합

Security Cloud Control는 Cisco Secure Sign-On을 SAML Single Sign-On IdP(Identity Provider) 및 MFA(다단계 인증)용 Duo Security로 사용합니다. 이는 Security Cloud Control의 기본 인증 방법입니다.

그러나 고객이 자신의 SAML SSO(Single Sign-On) IdP 솔루션을 Security Cloud Control와 통합하려는 경우 IdP가 SAML 2.0 및 IdP(Identity Provider) 시작 워크플로를 지원하는 경우라면 가능합니다.

자체 또는 서드파티 IdP(Identity Provider)를 Cisco Security Cloud Sign On과 통합하려면 Cisco Security Cloud Sign On ID 제공자 통합 가이드를 참조하십시오.

자체 SAML 솔루션을 Security Cloud Control와 통합하는 데 추가 지원이 필요한 경우 지원팀에 문의하여 케이스를 생성합니다.

Attention 케이스를 열 때 요청이 올바른 팀에 전달되도록 **Manually Select A Technology(**기술 수동 선택**)**을 선택하고 요청이 올바른 팀에 전달되도록 **SecureX -** 로그인 및 관리를 선택했는지 확인합니다.

SSO 인증서 갱신

ID 공급자(IdP)는 일반적으로 SecureX SSO와 통합됩니다. Cisco TAC 사례를 열고 metadata.xml 파일을 제공하십시오. 자세한 내용은 Cisco SecureX Sign-On 타사 ID 제공자 통합 가이드를 참조하십시오.

주의 케이스를 열 때 요청이 올바른 팀에 전달되도록 **Manually Select A Technology(**기술 수동 선택**)**을 선택하고 요청이 올바른 팀에 전달되도록 **SecureX -** 로그인 및 관리를 선택했는지 확인합니다.

(레거시만 해당) IdP(Identity Provider) 통합이 Security Cloud Control와 직접 통합된 경우 Security Cloud Control TAC로 지원 티켓을 열고 metadata.xml 파일을 제공하십시오.

내 토큰

자세한 내용은 API Tokens(API 토큰)을 참조하십시오.

API 토큰

개발자는 Security Cloud Control REST API 호출을 할 때 Security Cloud Control API 토큰을 사용합니다. 호출이 성공하려면 REST API 인증 헤더에 API 토큰이 반드시 포함되어야 합니다. API 토큰은 "장기 유효" 액세스 토큰 역할을 하며 만료되지 않지만, 갱신되거나 취소될 수 있습니다.

Security Cloud Control에서 API 토큰을 생성하려면, 먼저 API 전용 사용자가 존재하지 않는 경우 생성해야 합니다. 이 사용자는 API 토큰 생성 및 사용을 위해 특별히 지정되었습니다.

API 전용 사용자가 생성되면 해당 사용자에 대한 새 API 토큰 생성할 수 있습니다. 토큰은 생성 직후에만 표시되며, **General Settings(**일반 설정**)** 페이지를 유지하는 한 계속 표시됩니다. **General Settings(**일반 설정**)** 페이지에서 다른 페이지로 이동했다가 다시 돌아오면, 토큰이 발급된 것은 분명하지만 더 이상 표시되지 않습니다.

Note API 전용 사용자만 API 토큰을 생성할 수 있습니다. 개별 사용자는 자신이나 타인을 위해 API 토큰을 생성할 수 없습니다.

API 토큰 형식 및 클레임

API 토큰은 JSON 웹 토큰(JWT)입니다. JWT 토큰 형식에 대해 자세히 알아보려면 JSON 웹 토큰 소개를 읽어보십시오.

Security Cloud Control API 토큰은 다음과 같은 클레임 집합을 제공합니다.

- **id** - 사용자/디바이스 uid
- **parentId** - 테넌트 uid
- **ver** - 공개 키의 버전(초기 버전은 0, 예, **cdo_jwt_sig_pub_key.0**)
- **subscriptions** - 보안 서비스 익스체인지 구독 (선택 사항)
- **client_id** - "**api-client**"
- **jti** - 토큰 ID

토큰 관리

API 전용 사용자 생성

사용자를 생성할 때 슈퍼 관리자는 "API 전용 사용자"를 선택하여 가상 사용자 유형을 생성하고 Security Cloud Control REST API 호출 시 Security Cloud Control에 인증을 위한 API 토큰을 생성할 수 있습니다. Security Cloud Control에서는 이메일 주소 대신 사용자 이름을 제공하라는 메시지를 표시합니다. 그러면 원래 슈퍼 관리자가 조직을 떠난 후에도 권한이 계속 작동할 수 있습니다. API 전용 사용자는 Security Cloud Control 인터페이스에 로그인할 수 없습니다.

프로시저

단계 **1** Security Cloud Control에 로그인합니다.

단계 **2** 왼쪽 창에서 **Administration(**관리**)** > **API User Management(**사용자 관리**)**를 클릭합니다.

단계 **3** 테넌트에 새 사용자를 추가하려면 **Add a new user(**새 사용자 추가**)** ( ) 아이콘을 클릭합니다.

단계 **4** **API Only User(API** 전용 사용자**)** 확인란을 선택합니다.

단계 **5** **Username(**사용자 이름**)** 필드에 사용자 이름을 입력하고 **OK(**확인**)**를 클릭합니다.

중요
사용자 이름은 이메일 주소이거나 '@yourtenant' 접미사가 사용자 이름에 자동으로 추가되므로 '@' 문자를 포함할 수 없습니다.

단계 **6** 드롭다운 메뉴에서 사용자 역할을 선택합니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

API 토큰 생성

Security Cloud Control API를 사용하려면 API 토큰이 있어야 합니다. Security Cloud Control 테넌트에서 API 전용 사용자를 생성하고 해당 사용자에 대한 토큰을 생성할 것을 권장합니다.

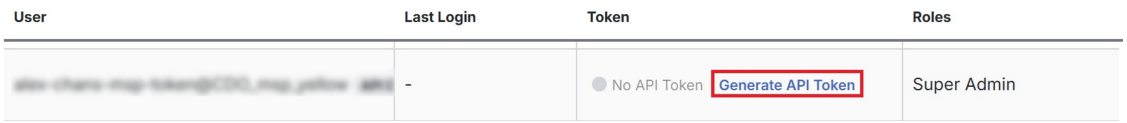
이 토큰은 REST API 호출의 인증 헤더에 사용되는 장기 유효한 무기명 토큰입니다. 동일한 토큰이 Security Cloud Control API와 클라우드 제공 Firewall Management Center API 모두에 사용됩니다.

Procedure

단계 1 Security Cloud Control에 로그인합니다.

단계 2 왼쪽 창에서 **Administration(관리)** > **API User Management(사용자 관리)**를 클릭합니다.

단계 3 **Token(토큰)** 열 아래의 **Generate API Token(API 토큰 생성)**을 클릭합니다.



단계 4 민감한 데이터를 유지하기 위한 기업의 모범 사례에 부합하는 안전한 위치에 토큰을 저장합니다.

What to do next

자세한 내용은 Security Cloud Control 방화벽 API 문서 시작하기를 참조하십시오.

API 토큰 새로 고침

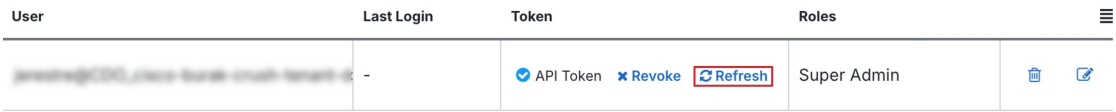
API 토큰은 만료되지 않습니다. 그러나 API 토큰을 분실하거나 유출되었을 경우, 또는 기업의 보안 지침을 준수하기 위해 기존 토큰을 갱신하는 방식으로 API 토큰을 새로 고칠 수 있습니다.

Procedure

단계 1 Security Cloud Control에 로그인합니다.

단계 2 왼쪽 창에서 **Administration(관리)** > **API User Management(사용자 관리)**를 클릭합니다.

단계 3 **Token(토큰)** 열 아래의 **Refresh(새로 고침)**을 클릭합니다. Security Cloud Control이 API 토큰을 새로 고칩니다.



단계 4 민감한 데이터를 유지하기 위한 기업의 모범 사례에 따라 안전한 위치에 새 토큰을 저장하십시오.

Note
Dynamic Attributes Connector 서비스 어카운트(csdac-service@tenantname)의 API 전용 사용자에 대한 **Revoke(취소)**, **Refresh(새로고침)**, **Delete(삭제)**및 **Edit(편집)** 옵션이 비활성됩니다. 이는 사용자가 이 API 어카운트의 API 토큰을 삭제, 편집 또는 취소하지 않도록 하기 위한 것으로, Dynamic Attributes Connector 기능에 필요합니다.

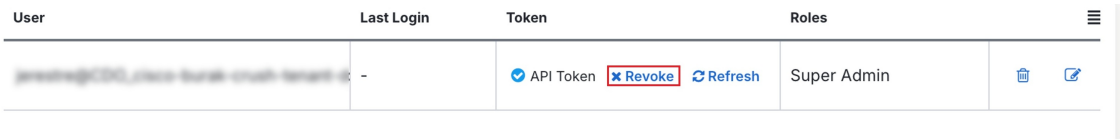
API 토큰 취소

Procedure

단계 **1** Security Cloud Control에 로그인합니다.

단계 **2** 왼쪽 창에서 **Administration(관리)** > **API User Management(사용자 관리)**를 클릭합니다.

단계 **3** **Token(토큰)** 열에서 API 토큰을 생성하려는 사용자의 **Revoke(취소)**를 클릭합니다.



Note
Dynamic Attributes Connector 서비스 어카운트(csdac-service@tenantname)의 API 전용 사용자에 대한 **Revoke(취소)**, **Refresh(새로고침)**, **Delete(삭제)**및 **Edit(편집)** 옵션이 비활성됩니다. 이는 사용자가 이 API 어카운트의 API 토큰을 삭제, 편집 또는 취소하지 않도록 하기 위한 것으로, Dynamic Attributes Connector 기능에 필요합니다.

ID 제공자 어카운트과 Security Cloud Control 사용자 레코드 간의 관계

Security Cloud Control에 로그인하려면 고객에게 SAML 2.0 호환 IdP(Identity Provider), 다단계 인증 제공자 및 Security Cloud Control의 사용자 레코드가 있는 어카운트가 필요합니다. IdP 어카운트에는 사용자의 자격 증명이 포함되며 IdP는 이러한 자격 증명을 기반으로 사용자를 인증합니다. 다단계 인증은 ID 보안의 추가 레이어를 제공합니다. Security Cloud Control 사용자 레코드에는 주로 사용자 이름, 연결된 Security Cloud Control 테넌트 및 사용자의 역할이 포함됩니다. 사용자가 로그인하면 Security Cloud Control는 IdP의 사용자 ID를 Security Cloud Control의 테넌트에 있는 기존 사용자 레코드에 매핑하려고 시도합니다. Security Cloud Control가 일치하는 항목을 찾으면 사용자는 해당 테넌트에 로그인됩니다.

엔터프라이즈에 자체 SSO(Single Sign-On) ID 제공자가 없는 경우 ID 제공자는 Cisco Secure Cloud Sign-on입니다. Cisco Secure Cloud Sign-On은 다단계 인증에 Duo를 사용합니다. 고객은 원하는 경우 자신의 IdP를 Security Cloud Control와 통합할 수 있습니다.

로그인 워크플로우

다음은 IdP 어카운트가 Security Cloud Control 사용자 레코드와 상호 작용하여 Security Cloud Control 사용자에 로그인하는 방법에 대한 간략한 설명입니다.

Procedure

단계 **1** 사용자는 인증을 위해 Cisco Secure Cloud Sign-On(https://sign-on.security.cisco.com)과 같은 SAML 2.0 호환 ID 공급자(IdP)에 로그인하여 Security Cloud Control에 대한 액세스를 요청합니다.

단계 **2** IdP는 사용자가 인증된 사용자라는 SAML 어설션을 발행하고 포털은 사용자가 액세스할 수 있는 애플리케이션을 표시합니다. 타일 중 하나는 Security Cloud Control를 나타냅니다.

단계 **3** Security Cloud Control는 SAML 어설션의 유효성을 검사하고 사용자 이름을 추출한 다음 테넌트 중에서 해당 사용자 이름에 해당하는 사용자 레코드를 찾으려고 시도합니다.

- 사용자가 Security Cloud Control의 단일 테넌트에 대한 사용자 레코드를 가지고 있는 경우 Security Cloud Control는 사용자에게 테넌트에 대한 액세스 권한을 부여하고 사용자의 역할에 따라 수행할 수 있는 작업이 결정됩니다.
- 사용자가 두 개 이상의 테넌트에 대한 사용자 레코드를 가지고 있는 경우 Security Cloud Control는 인증된 사용자에게 선택할 수 있는 테넌트 목록을 제공합니다. 사용자는 테넌트를 선택하고 해당 테넌트에 액세스할 수 있습니다. 특정 테넌트에 대한 사용자의 역할에 따라 수행할 수 있는 작업이 결정됩니다.
- Security Cloud Control에 인증된 사용자와 테넌트의 사용자 레코드에 대한 매핑이 없는 경우 Security Cloud Control는 사용자에게 Security Cloud Control에 대해 자세히 알아보거나 무료 평가판을 요청할 수 있는 기회를 제공하는 랜딩 페이지를 표시합니다.

Security Cloud Control에 사용자 레코드를 생성해도 IdP에 어카운트가 생성되지 않고 IdP에 어카운트를 생성해도 Security Cloud Control에 사용자 레코드가 생성되지 않습니다.

마찬가지로 IdP에서 어카운트를 삭제한다고 해서 Security Cloud Control에서 사용자 기록을 삭제한 것은 아닙니다. 그러나 IdP 어카운트가 없는 경우 사용자를 Security Cloud Control에 인증할 방법이 없습니다. Security Cloud Control 사용자 기록을 삭제한다고 해서 IdP 어카운트가 삭제된 것은 아닙니다. 그러나 Security Cloud Control 사용자 레코드가 없는 경우 인증된 사용자가 Security Cloud Control 테넌트에 액세스할 수 있는 방법이 없습니다.

이 아키텍처의 의미

Cisco Security Cloud 로그인을 사용하는 고객

Security Cloud Control의 Cisco Secure Cloud Sign-On ID 공급자를 사용하는 고객의 경우 슈퍼 관리자는 Security Cloud Control에 사용자 레코드를 생성할 수 있으며 사용자는 Security Cloud Control에 자체 등록할 수 있습니다. 두 사용자 이름이 일치하고 사용자가 올바르게 인증된 경우 사용자는 Security Cloud Control에 로그인할 수 있습니다.

슈퍼 관리자가 사용자가 Security Cloud Control에 액세스하지 못하도록 해야 하는 경우 Security Cloud Control 사용자의 사용자 레코드를 간단히 삭제할 수 있습니다. Cisco Secure Cloud Sign-On 어카운트는 여전히 존재하며 슈퍼 관리자가 사용자를 복원하려는 경우 Cisco Secure Cloud Sign-On에 사용된 것과 동일한 사용자 이름으로 새 Security Cloud Control 사용자 레코드를 생성하면 됩니다.

고객이 기술 지원 센터(TAC)에 전화해야 하는 Security Cloud Control 문제에 직면한 경우 고객은 TAC 엔지니어를 위한 사용자 레코드를 생성하여 테넌트를 조사하고 정보와 제안을 고객에게 다시 보고할 수 있습니다. .

자체 **ID** 제공자가 있는 고객

자체 ID 공급자가 있는 고객의 경우 ID 공급자 어카운트과 Security Cloud Control 테넌트를 모두 제어합니다. 이러한 고객은 Security Cloud Control에서 ID 공급자 어카운트 및 사용자 레코드를 만들고 관리할 수 있습니다.

사용자가 Security Cloud Control에 액세스하지 못하도록 해야 하는 경우, IdP 어카운트, Security Cloud Control 사용자 레코드 또는 둘 다를 삭제할 수 있습니다.

Cisco TAC의 도움이 필요한 경우, TAC 엔지니어를 위해 읽기 전용 역할이 있는 ID 공급자 어카운트과 Security Cloud Control 사용자 레코드를 모두 생성할 수 있습니다. 그런 다음 TAC 엔지니어는 고객의 Security Cloud Control 테넌트에 액세스하여 조사하고 고객에게 정보와 제안을 보고할 수 있습니다.3

Cisco Managed Service 제공자

Cisco MSP(Managed Service Provider)가 Security Cloud Control의 Cisco Secure Cloud Sign-On IdP를 사용하는 경우 Cisco Secure Cloud Sign-On에 자체 등록할 수 있으며 고객은 MSP가 고객의 테넌트를 관리할 수 있도록 Security Cloud Control에 사용자 레코드를 생성할 수 있습니다. 물론 고객은 원할 때 MSP의 레코드를 삭제할 수 있는 모든 권한을 가집니다.

관련 주제

- General Settings(일반 설정)
- 사용자 관리
- Security Cloud Control 사용자 역할

MSSP 포털

Security Cloud Control의 MSSP 포털은 매니지드 보안 서비스 제공자(MSSP)가 여러 테넌트에 걸쳐 디바이스를 효율적으로 모니터링하고 관리할 수 있는 멀티테넌트, 클라우드 기반 관리 플랫폼입니다.

포털 **Configuration Status(**구성 상태**)**, **Connectivity State(**연결성 상태**)**, **Software Version(**소프트웨어 버전**)**, 전체 네트워크 상태 등의 실시간 정보를 단일 인터페이스로 통합하므로, 개별 테넌트 환경에 액세스할 필요 없이 원활한 개요를 제공합니다.

시작하기 전에

- Cisco TAC 로 지원 티켓을 열어 MSSP 포털을 생성하여 테넌트를 관리합니다. 자세한 내용은 TAC를 사용하여 지원 티켓 열기을 참조하십시오.
- 브라우저 관련 문제를 방지하려면 웹 브라우저에서 캐시와 쿠키를 지우는 것이 좋습니다.

MSSP 포털 구성 요소

포털의 왼쪽 창에서 제공되는 옵션을 사용하여 포털의 보안 디바이스 및 테넌트에 대한 세부 정보를 보고 포털 설정을 구성할 수 있습니다.

- 대시보드
  - 일반 개요 디바이스, 클라우드 서비스, 방화벽 관리자의 총 수와 해당 연결 상태가 표시됩니다. 디바이스의 구성 상태에 대한 정보도 제공합니다.

- 상태 개요에서는 테넌트에 온보딩된 Secure Firewall ASA 디바이스의 중요 성능 데이터에 대한 인사이트를 제공합니다.

  자세한 내용은 MSSP 포털에서 상태 개요 대시보드 보기를 참조하십시오.

- **Security Devices(**보안 디바이스**)**

  포털에 추가된 테넌트에 온보딩된 모든 디바이스, 클라우드 서비스, 템플릿 및 방화벽 관리자에 대한 정보를 제공합니다. 자세한 내용은 보안 디바이스 세부 정보, 23 페이지을 참조하십시오.

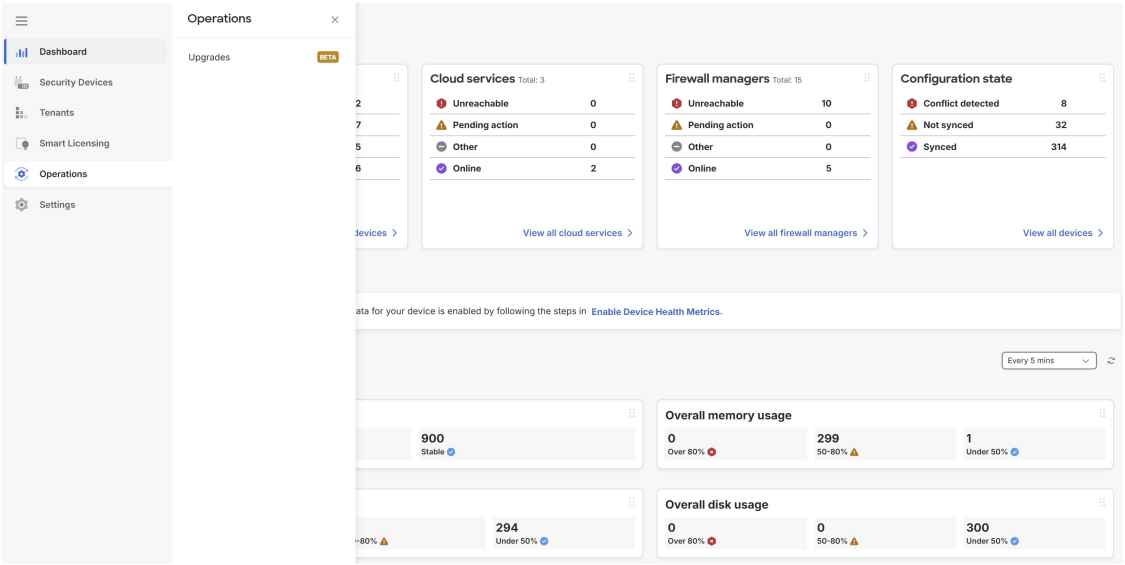
- **Tenants(**테넌트**)**

  - 포털에서 관리하는 모든 테넌트에 대한 정보를 제공합니다. 테넌트 정보로 검색하고 테넌트 정보를 쉼표로 구분된 값(.csv) 파일로 내보낼 수 있습니다.
  - **Super Admin(**슈퍼 관리자**)** 권한이 있는 사용자만 새 테넌트를 생성하거나 기존 테넌트를 포털에 추가할 수 있습니다.

- **Operations(**운영**)**

  MSSP 포털의 업그레이드 기능을 사용하면 cdFMC(Cloud-Delivered Firewall Management Center)로 관리되는 여러 테넌트에 걸쳐 Secure Firewall Threat Defense 디바이스를 일괄 업그레이드할 수 있습니다.

참고 멀티테넌트 디바이스 업그레이드는 베타 기능입니다.



- 설정

  - **General Settings(**일반 설정**)**에서는 포털 설정에 대한 정보를 제공합니다.

- **User Management(**사용자 관리**)**에서 모든 **User(**사용자**)**, **Active Directory** 그룹 및 **Audit Logs(**감사 로그**)**의 목록을 볼 수 있습니다. 자세한 내용은 User Management(사용자 관리)를 참조하십시오.

참고 슈퍼 관리자 권한이 있는 사용자는 API 엔드포인트를 사용하여 다음을 수행할 수 있습니다.

- Security Cloud Control 테넌트 생성
- 멀티테넌트 포털에 기존 Security Cloud Control 테넌트 추가

보안 디바이스 세부 정보

왼쪽 창에서 **Security Devices(**보안 디바이스**)**를 클릭하여 다음 탭이 포함된 **Security Devices(**보안 디바이스**)** 페이지를 확인합니다.

표 *1:* 보안 디바이스 페이지 탭 설명

탭 이름	설명
디바이스	포털의 테넌트에 온보딩된 모든 디바이스를 확인합니다. • **Device Details(**디바이스 세부 정보**)**, **Tenant Details(**테넌트 세부 정보**)** 및 **Actions(**작업**)**를 보려면 디바이스를 클릭합니다. • **Actions(**작업**)Manage Device on Tenant(**테넌트의 디바이스 관리**)**를 클릭하여 Security Cloud Control에서 이 디바이스를 관리할 수 있습니다. 해당 테넌트에 대한 어카운트가 있고 테넌트가 포털과 동일한 지역에 있는 경우 이 링크가 표시됩니다. 테넌트에 액세스할 수 있는 권한이 없는 경우 테넌트에 디바이스 관리 링크가 표시되지 않습니다. 필요한 권한을 얻으려면 조직의 슈퍼 관리자에게 문의하십시오. • **Filters(**필터**)**를 클릭하여 **Device/Services(**디바이스/서비스**)**, **Configuration Status(**구성 상태**)**, **Connectivity State(**연결 상태**)**, **Software Version(**소프트웨어 버전**)** 또는 **Tenant(**테넌트**)** 또는 **Conflict Detection(**충돌 탐지**)**를 기준으로 클라우드 서비스를 필터링합니다.

탭 이름	설명
클라우드 서비스	포털 의 테넌트에 온보딩된 모든 클라우드 서비스를 확인합니다. • **Device Details(**디바이스 세부 정보**)**, **Tenant Details(**테넌트 세부 정보) 및 **Actions(**작업**)**를 보려면 클라우드 서비스를 클릭합니다. • **Filters(**필터**)**를 클릭하여 **Services(**서비스**)**, **Configuration Status(**구성 상태**)**, **Connectivity State(**연결 상태**)**, **Tenant(**테넌트**)** 또는 **Conflict Detection(**충돌 탐지**)**를 기준으로 클라우드 서비스를 필터링합니다.
템플릿	포털의 테넌트에 온보딩된 모든 템플릿을 확인합니다. • **Device Details(**디바이스 세부 정보**)**, **Tenant Details(**테넌트 세부 정보) 및 **Actions(**작업**)**를 보려면 템플릿을 클릭합니다. • 클라우드 서비스를 **Template Type(**템플릿 유형**)**, **Configuration Status(**구성 상태**)**, **Software Version(**소프트웨어 버전**)** 또는 **Tenant(**테넌트**)**로 필터링하려면 필터를 클릭합니다.
방화벽 관리자	포털의 테넌트에 온보딩된 모든 방화벽 관리자를 확인합니다. • **Device Details(**디바이스 세부 정보**)**, **Tenant Details(**테넌트 세부 정보) 및 **Actions(**작업**)**를 보려면 방화벽 관리자를 클릭합니다. • **Filters(**필터**)**를 클릭하여 **Device Managers(**디바이스 관리자**)**, **Configuration Status(**구성 상태**)**, **Tenant(**테넌트**)**, **Software Version(**소프트웨어 버전**)**을 클릭합니다.

- 분석 및 규정 준수 보고를 지원하기 위해 세부 정보를 쉼표로 구분된 값(.csv) 파일로 내보낼 수 있습니다. 데이터를 내보낼 때마다 Security Cloud Control는 생성 시간 스탬프와 포털의 전역 고유 식별자가 파일 이름에 포함된 새로운 .csv 파일을 생성합니다.
- 열 선택기를 사용하면 테이블에서 볼 디바이스 속성을 선택하거나 지울 수 있습니다. 테이블 설정을 보려면 테이블의 오른쪽 상단에 있는 기어 아이콘 ( )을 클릭합니다.

  테이블을 사용자 정의하면 Security Cloud Control는 다음에 로그인할 때 **Security Devices(**보안 디바이스**)** 페이지를 볼 때 선택 사항을 기억합니다.

MSSP 포털에 테넌트 추가

슈퍼 관리자 권한이 있는 사용자는 여러 지역에서 MSSP 포털에 테넌트를 추가할 수 있습니다. 예를 들어 유럽에서 미국으로 테넌트 추가하거나 그 반대로 추가할 수 있습니다.

Important 테넌트에 대한 API 전용 사용자를 생성하고 Security Cloud Control 인증을 위한 API 토큰을 생성하는 것이 좋습니다.

Note 포털에 여러 테넌트를 추가하려면 각 테넌트에서 API 토큰을 생성하고 텍스트 파일에 붙여넣습니다. 그런 다음 토큰을 생성하기 위해 매번 테넌트로 전환하지 않고도 포털에 테넌트를 차례로 추가할 수 있습니다.

Procedure

단계 **1** 왼쪽 창에서 **Tenants(**테넌트**)**를 클릭합니다.

단계 **2** 페이지 오른쪽 상단 모서리에 있는  아이콘을 클릭합니다.

단계 **3** 새 테넌트를 추가하려면 **Next(**다음**)**을 클릭합니다.

Note

a. 기존 테넌트를 가져오려면 기존 테넌트를 가져오시겠습니까**?** 확인란을 선택합니다.

b. 여러 개의 API 토큰을 쉼표로 구분하여 붙여넣어 Security Cloud Control에서 기존 테넌트를 추가합니다.

c. **Import(**가져오기**)**를 클릭합니다.

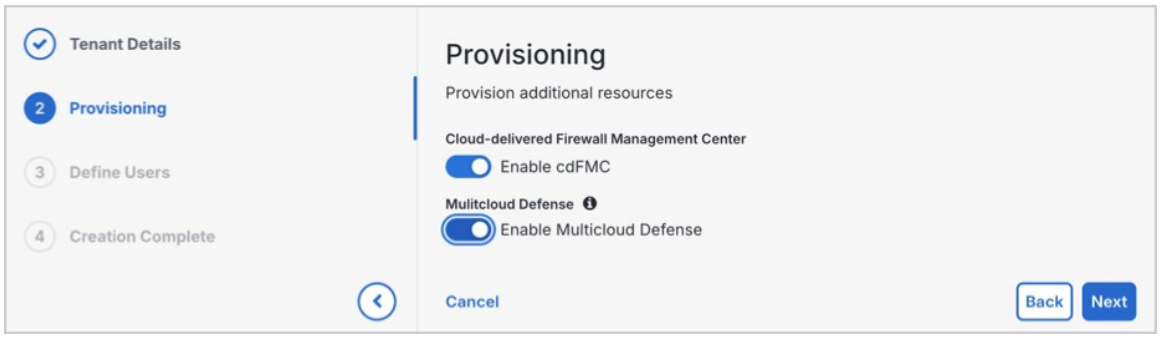
단계 **4** **Tenant Details(**테넌트 세부 정보**)**에서 **Display Name(**표시 이름**)**과 **Tenant Name(**테넌트 이름**)** 및 **Sales Order Number(**세일즈 오더 번호**)**를 입력합니다.

판매 주문 번호 없이 생성된 테넌트는 30일 가치 입증 평가판으로 제공됩니다.

단계 **5** **Next(**다음**)**를 클릭합니다.

단계 **6** **Provisioning(**프로비저닝**)**에서,

- **cdFMC** 활성화 토글 버튼을 클릭하여 테넌트에 클라우드 제공 Firewall Management Center를 프로비저닝합니다.
- **Multicloud Defense** 활성화 토글 버튼을 클릭하여 테넌트에 Multicloud Defense를 프로비저닝합니다.
- **Next(**다음**)**를 클릭합니다.



단계 **7** **Define Users(**사용자 정의**)**에서 이메일 주소를 입력하고 역할을 선택하여 사용자를 수동으로 추가하거나, CSV 파일 템플릿을 다운로드하여 필요한 세부 정보를 입력한 후 파일을 업로드합니다.

추가된 사용자는 **User list(**사용자 목록**)** 섹션에 표시됩니다.

단계 **8** **Create Tenant(**테넌트 생성**)**을 클릭합니다.

테넌트 생성이 완료되었으며 프로비저닝에는 몇 분 정도 소요될 수 있습니다.

MSSP 포털에서 테넌트 삭제

Procedure

단계 **1** 왼쪽 창에서 **Tenants(**테넌트**)**를 클릭합니다.

단계 **2** 오른쪽의 해당 삭제 아이콘을 클릭하여 테넌트를 삭제합니다.

단계 **3** **Remove(**제거**)**를 클릭합니다.

참고로 연결된 디바이스도 포털에서 제거됩니다.

MSSP 포털의 다중 테넌트 디바이스 업그레이드 정보

MSSP 포털을 사용하면 여러 테넌트에서 Secure Firewall Threat Defense 디바이스의 대량 업그레이드를 수행할 수 있습니다. **Operations(**운영**)** 대시보드의 **Upgrades(**업그레이드**)** 페이지를 사용하여 MSSP 포털에서 cdFMC(클라우드 제공 Firewall Management Center)에 의해 관리되는 여러 Secure Firewall Threat Defense 디바이스를 선택하고 업그레이드를 수행할 수 있습니다.

참고 멀티테넌트 디바이스 업그레이드는 베타 기능입니다.

다중 테넌트 디바이스 업그레이드의 이점

- 대규모 대량 업그레이드를 수행하기 위한 통합 대시보드의 가용성.

• 버전을 결정하는 데 도움이 되는 업그레이드 패키지 목록의 가용성.

MSSP 포털에서 전체 다중 테넌트 디바이스 업그레이드 시작

전체 업그레이드를 시작할 때는 패키지를 선택하고, 선택한 디바이스에 업로드한 후, 준비 상태 검사를 수행하며, 중단 없이 업그레이드 프로세스를 완료해야 합니다.

이 절차를 사용하여 전체 업그레이드할 수 있는 항목

SUMMARY STEPS

1. 왼쪽 창에서 **Operations(**작업**)** > **Upgrades(**업그레이드**)**로 이동합니다.
2. **Begin an Upgrade(**업그레이드 시작**)**를 클릭합니다.
3. 업그레이드 이름을 입력하고 업그레이드할 디바이스를 선택한 후 **Next(**다음**)**를 클릭합니다.
4. 표시되는 대화 상자에서 **Full upgrade(**전체 업그레이드**)** 버튼을 클릭하고 **Next(**다음**)**를 클릭합니다.
5. 선택한 디바이스에 사용할 수 있는 **Threat Defense** 패키지 목록에서 업그레이드 패키지를 선택하고 **Perform upgrade(**업그레이드 수행**)**를 클릭합니다. 모든 디바이스가 모든 패키지와 호환되는 것은 아닙니다.
6. **Back to Upgrades(**업그레이드로 돌아가기**)**를 클릭하여 **Upgrades(**업그레이드**)** 페이지로 돌아갑니다.

DETAILED STEPS

프로시저

단계 **1** 왼쪽 창에서 **Operations(**작업**)** > **Upgrades(**업그레이드**)**로 이동합니다.

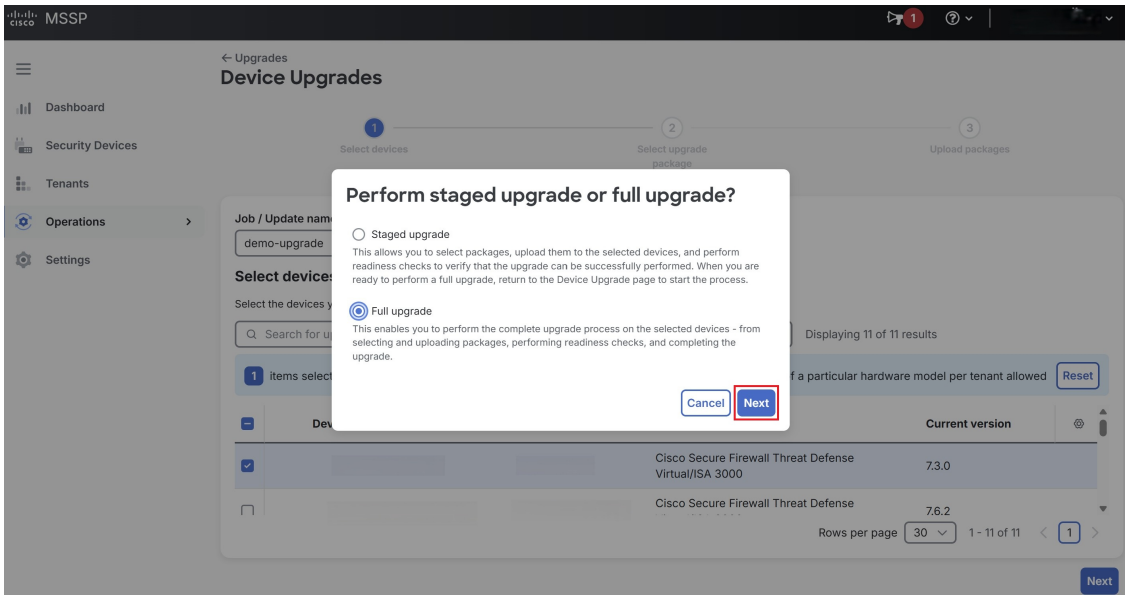
단계 **2** **Begin an Upgrade(**업그레이드 시작**)**를 클릭합니다.

단계 **3** 업그레이드 이름을 입력하고 업그레이드할 디바이스를 선택한 후 **Next(**다음**)**를 클릭합니다.

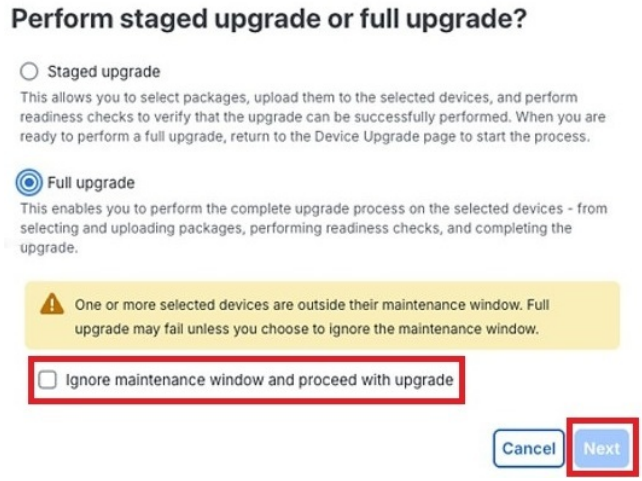
Device Upgrades(디바이스 업그레이드**)** 페이지 상단에 있는 **Model(**모델**)** 또는 **Tenant(**테넌트**)** 드롭다운 목록을 사용하여 디바이스를 필터링합니다.

참고
각 테넌트별로 특정 하드웨어 모델에 속하는 최대 50대의 디바이스를 업그레이드할 수 있습니다.

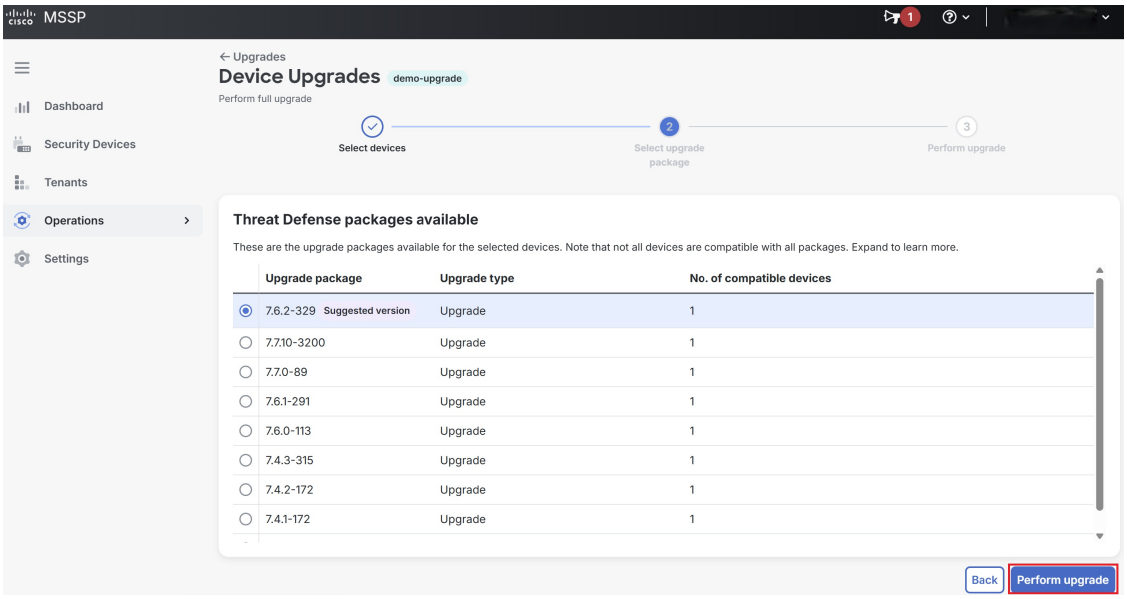
단계 **4** 표시되는 대화 상자에서 **Full upgrade(**전체 업그레이드**)** 버튼을 클릭하고 **Next(**다음**)**를 클릭합니다.



유지 관리 기간이 아닌 디바이스에서 전체 업그레이드를 수행하려면 대화 상자에서 **Ignore maintenance window and proceed with upgrade(**유지보수 시간을 무시하고 업그레이드 진행**)** 체크 박스를 클릭하고 **Next(**다음**)**를 클릭합니다. 유지보수 시간 외에 업그레이드를 수행하는 것은 권장되지 않으며, 긴급한 상황에만 수행해야 합니다.



단계 **5** 선택한 디바이스에 사용할 수 있는 **Threat Defense** 패키지 목록에서 업그레이드 패키지를 선택하고 **Perform upgrade(**업그레이드 수행**)**를 클릭합니다. 모든 디바이스가 모든 패키지와 호환되는 것은 아닙니다.



단계 **6** **Back to Upgrades(**업그레이드로 돌아가기**)**를 클릭하여 **Upgrades(**업그레이드**)** 페이지로 돌아갑니다.

업그레이드가 완료되면 **Upgrade completed(**업그레이드 완료**)** 메시지가 **Upgrades(**업그레이드**)** 페이지의 **Status(**상태**)** 열 아래에 표시됩니다. 업그레이드에 실패하면 실패 사유를 알리는 메시지가 표시됩니다.

MSSP 포털에서 준비된 다중 테넌트 디바이스 업그레이드 시작

단계별 업그레이드를 시작할 때 패키지를 선택하고, 선택한 디바이스에 업로드한 후 준비 상태 검사를 수행합니다. 이러한 검사는 업그레이드가 나중에 성공적으로 수행될 수 있는지 확인합니다.

팁 유지보수 시간 전에 단계별 업그레이드를 사용하여 업그레이드를 준비할 수 있으며, 이를 통해 실제 업그레이드 시간 동안 전체 업그레이드가 더 빠르게 완료될 수 있습니다.

이 절차를 사용하여 준비된 업그레이드를 시작할 수 있는 항목

SUMMARY STEPS

1. 왼쪽 창에서 **Operations(**작업**)** > **Upgrades(**업그레이드**)**로 이동합니다.
2. **Begin an Upgrade(**업그레이드 시작**)**를 클릭합니다.
3. 업그레이드 이름을 입력하고 업그레이드할 디바이스를 선택한 후 **Next(**다음**)**를 클릭합니다.
4. 표시되는 대화 상자에서 **Staged upgrade(**준비된 업그레이드**)** 버튼을 클릭하고 **Next(**다음**)**를 클릭합니다.
5. 선택한 디바이스에 사용할 수 있는 Threat Defense 패키지 목록에서 업그레이드 패키지를 선택하고 **Upload package(**패키지 업로드**)**를 클릭합니다. 모든 디바이스가 모든 패키지와 호환되는 것은 아닙니다.
6. 패키지 업로드를 취소하려면 **Exit(**종료**)**를 클릭합니다.

7. **Exit**를 클릭합니다.

DETAILED STEPS

프로시저

단계 **1** 왼쪽 창에서 **Operations(**작업**)** > **Upgrades(**업그레이드**)**로 이동합니다.

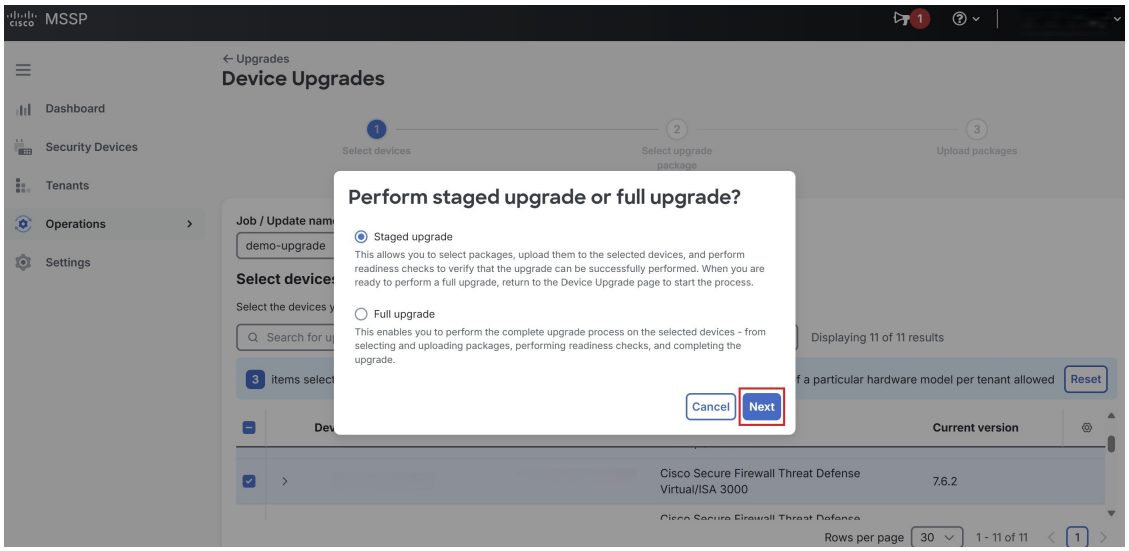
단계 **2** **Begin an Upgrade(**업그레이드 시작**)**를 클릭합니다.

단계 **3** 업그레이드 이름을 입력하고 업그레이드할 디바이스를 선택한 후 **Next(**다음**)**를 클릭합니다.

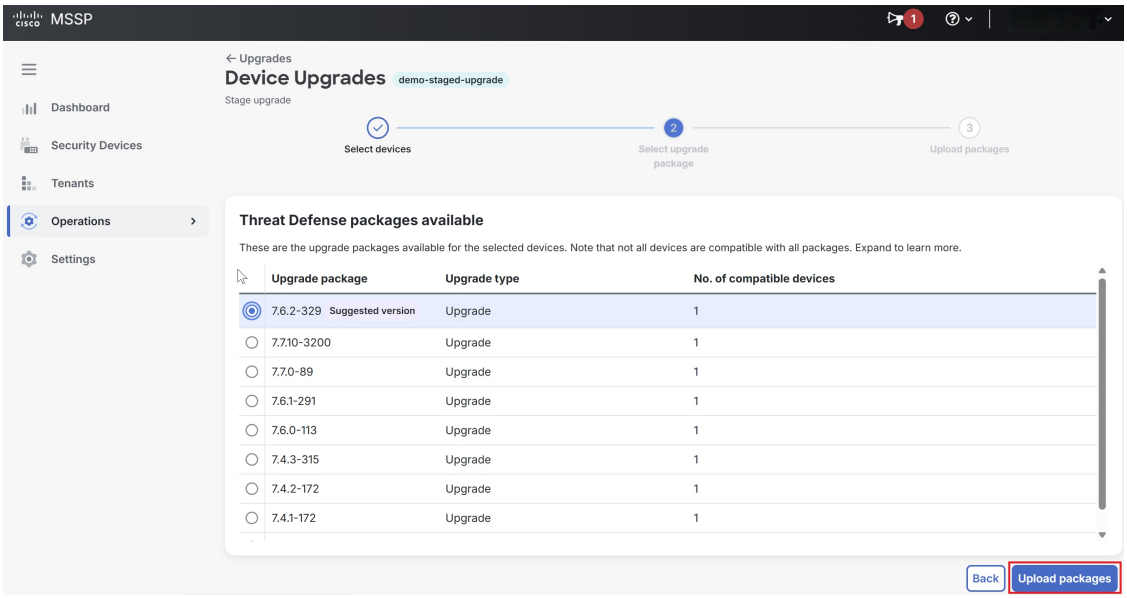
Device Upgrades(디바이스 업그레이드**)** 페이지 상단에 있는 **Model(**모델**)** 또는 **Tenant(**테넌트**)** 드롭다운 목록을 사용하여 디바이스를 필터링합니다.

참고
각 테넌트별로 특정 하드웨어 모델에 속하는 최대 50대의 디바이스를 업그레이드할 수 있습니다.

단계 **4** 표시되는 대화 상자에서 **Staged upgrade(**준비된 업그레이드**)** 버튼을 클릭하고 **Next(**다음**)**를 클릭합니다.



단계 **5** 선택한 디바이스에 사용할 수 있는 Threat Defense 패키지 목록에서 업그레이드 패키지를 선택하고 **Upload package(**패키지 업로드**)**를 클릭합니다. 모든 디바이스가 모든 패키지와 호환되는 것은 아닙니다.



단계 **6** 패키지 업로드를 취소하려면 **Exit(**종료**)**를 클릭합니다.

패키지가 업로드되면 **Upgrade package uploaded and staged(**업그레이드 패키지 업로드 및 스테이징 완료**)** 메시지가 **Upgrades(**업그레이드**)** 페이지의 **Status(**상태**)** 열 아래에 표시됩니다.

단계 **7** **Exit**를 클릭합니다.

패키지가 준비되었으며 설치할 준비가 되었습니다. **Status(**상태**)** 열의 **Upgrades(**업그레이드**)** 페이지에 **Upgrade staged(**업그레이드 준비됨**)** 상태가 표시됩니다. 완료되면 **Upgrades(**업그레이드**)** 페이지의 **Upgrade name(**업그레이드 이름**)** 열 아래에서 업그레이드의 이름을 클릭하여 전체 업그레이드를 진행합니다.

MSSP 포털의 보안 디바이스 페이지에서 대량 업그레이드 수행

Security Devices(보안 디바이스**)** 페이지에서 디바이스를 직접 업그레이드하려면 이 절차를 사용합니다.

SUMMARY STEPS

1. 왼쪽 창에서 **Security Devices(**보안 디바이스**)**를 클릭합니다.
2. 업그레이드할 디바이스를 선택하고 오른쪽의 **Actions(**작업**)** 아래에서 **Upgrade device(**디바이스 업그레이드**)**를 클릭합니다.
3. 이름을 입력하고 **Device upgrade(**디바이스 업그레이드**)** 대화 상자에서 **Staged upgrade(**준비된 업그레이드**)** 또는 **Full upgrade(**전체 업그레이드**)**를 선택한 후 **Next(**다음**)**을 클릭합니다.

DETAILED STEPS

프로시저

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

단계 **2** 업그레이드할 디바이스를 선택하고 오른쪽의 **Actions(**작업**)** 아래에서 **Upgrade device(**디바이스 업그레이드**)**를 클릭합니다.

해당 디바이스가 선택된 **Device Upgrades(**디바이스 업그레이드**)** 페이지로 리디렉션됩니다.

단계 **3** 이름을 입력하고 **Device upgrade(**디바이스 업그레이드**)** 대화 상자에서 **Staged upgrade(**준비된 업그레이드**)** 또는 **Full upgrade(**전체 업그레이드**)**를 선택한 후 **Next(**다음**)**을 클릭합니다.

전체 업그레이드를 선택하는 경우 MSSP 포털에서 전체 다중 테넌트 디바이스 업그레이드 시작, 27 페이지의 4~7 단계를 수행합니다.

Staged upgrade(준비된 업그레이드**)**를 선택하는 경우 MSSP 포털에서 준비된 다중 테넌트 디바이스 업그레이드 시작, 29 페이지의 4~7단계를 수행합니다.

MSSP 포털 설정 관리

Security Cloud Control를 사용하면 설정 페이지에서 MSSP 포털 및 개별 사용자 어카운트의 특정 측면을 사용자 지정할 수 있습니다. 왼쪽 창에서 **Settings(**설정**)**를 클릭하여 설정 페이지에 액세스합니다.

설정

일반 설정

ASA 상태 모니터링 기능을 활성화하면 MSSP 포털의 상태 개요 대시보드를 사용하여 Secure Firewall ASA 디바이스를 모니터링할 수 있습니다.

General Settings(일반 설정**)**에서 포털 **ID**, **Secure Services Exchange** 포털 **ID** 및 포털 이름을 확인할 수도 있습니다.

사용자 관리

User Management(사용자 관리**)** 화면에서 MSSP 포털과 관련된 모든 사용자, **Active Directory** 그룹 및 감사 로그를 확인할 수 있습니다.

왼쪽 창에서 **Settings(**설정**) > User Management(**사용자 관리**)** 를 클릭합니다**.**

1. 사용자: 사용자 탭에서 테넌트와 연결된 모든 사용자 레코드를 확인할 수 있습니다.
   - 사용자 탭에서 API 전용 사용자에 대한 API 토큰을 생성하려면 **Generate API Token(API** 토큰 생성**)**을 클릭합니다.

     민감한 데이터를 유지하기 위한 기업의 모범 사례에 부합하는 안전한 위치에 토큰을 저장합니다. 자세한 내용은 API 토큰 생성, on page 17을 참조하십시오.

- **Token(**토큰**)** 열 아래의 **Refresh(**새로 고침**)**을 클릭하여 API 토큰을 새로 고칩니다. 자세한 내용은 API 토큰 새로 고침, on page 18을 참조하십시오.
- **Token(**토큰**)** 열 아래의 **Refresh(**새로 고침**)**을 클릭하여 API 토큰을 새로 고칩니다. 자세한 내용은 API 토큰 취소, on page 19을 참조하십시오.

2. **Active Directory** 그룹: 이직률이 높은 테넌트의 경우, 사용자 목록 및 역할 관리를 용이하게 하기 위해 MSSP 포털에 개별 사용자를 추가하는 대신 MSSP 포털을 Active Directory 그룹에 매핑합니다. 새 사용자 추가 또는 기존 사용자 제거와 같은 모든 사용자 변경은 이제 Active Directory에서 수행할 수 있으며 더 이상 MSSP 포털에서 수행할 필요가 없습니다.
   - **Active Directory** 그룹 탭을 클릭합니다. 이 페이지에는 Active Directory 관리자에서 할당된 Active Directory 그룹의 역할이 표시됩니다.

     자세한 내용은 사용자 관리의 Active Directory 그룹, on page 35을 참조하십시오.
3. **Audit Logs(**감사 로그**)**: MSSP 포털에서 감사 로그 기능은 사용자 관련 및 시스템 수준 작업을 기록합니다.
   - **Audit Logs(**감사 로그**)** 탭을 클릭합니다.

     시스템은 현재 테넌트 내의 이벤트 및 활동 목록을 표시합니다.

     Search (검색) 텍스트 상자를 사용하여 특정 사용자 에 대한 로그를 찾습니다.
   - 검색 결과를 구체화하고 특정 이벤트를 보려면 필터 아이콘을 클릭합니다.

     Time Range(시간 범위**)** 및 **Event Action(**이벤트 동작**)**을 기준으로 로그를 필터링할 수 있습니다.
   - CSV 형식으로 세부 정보를 다운로드하려면 **Export(**내보내기**)**를 클릭합니다.

테넌트 전환

포털 테넌트가 둘 이상인 경우 Security Cloud Control에서 로그아웃하지 않고 다른 포털 또는 테넌트 간에 전환할 수 있습니다.

Procedure

단계 **1** MSSP 포털에서 오른쪽 상단 모서리의 테넌트 메뉴를 클릭합니다.

단계 **2** **Switch Tenant(**테넌트 전환**)**를 클릭합니다.

단계 **3** 보려는 포털 또는 테넌트를 선택합니다.

Cisco Success Network

Cisco Success Network는 사용자가 활성화하는 클라우드 서비스입니다. Cisco Success Network를 활성화하면 디바이스와 Cisco cloud간에 보안 연결이 설정되어 사용 정보 및 통계를 스트리밍합니다. 스트리밍 원격 측정은 디바이스에서 관심 있는 데이터를 선택하고 구조화된 형식으로 원격 관리 스테이션에 전송하는 메커니즘을 제공하여 다음과 같은 이점을 제공합니다.

- 네트워크에서 제품의 효율성을 향상시킬 수있는 활용 가능한 미사용 기능을 알려줍니다.
- 제품에 사용할 수 있는 추가 기술 지원 서비스 및 모니터링에 대해 알려줍니다.
- Cisco가 제품을 개선할 수 있습니다.

디바이스는 항상 보안 연결을 설정하고 유지하며 Cisco Success Network에 등록할 수 있습니다. 디바이스를 등록하고 나면 Cisco Success Network 설정을 변경할 수 있습니다.

참고

- Firewall Threat Defense 고가용성 쌍의 경우 활성 디바이스 선택이 대기 디바이스의 Cisco Success Network 설정을 재정의합니다.
- Security Cloud Control는 Cisco Success Network 설정을 관리하지 않습니다. Firewall Device Manager 사용자 인터페이스를 통해 관리되는 설정 및 원격 분석 정보가 제공됩니다.

Cisco Success Network 활성화 또는 비활성화

초기 시스템 설정 중에 Cisco Smart Software Manager에 디바이스를 등록하라는 메시지가 표시됩니다. 90일 평가 라이선스를 대신 선택한 경우에는 평가 기간이 종료되기 전에 디바이스를 등록해야 합니다. 디바이스를 등록하려면 Cisco Smart Software Manager(Smart Licensing 페이지)에 디바이스를 등록하거나 등록 키를 입력하여 Security Cloud Control에 등록합니다.

디바이스를 등록할 때는 가상 어카운트가 디바이스에 라이선스를 할당합니다. 디바이스를 등록하면 활성화한 선택 가능한 라이선스도 등록됩니다.

Firewall Device Manager UI를 통해서만 이 옵션을 비활성화할 수 있지만 Cisco Success Network를 비활성화하여 언제든지 이 연결을 끊을 수 있습니다. 비활성화하면 클라우드에서 디바이스의 연결이 끊어집니다. 연결 해제는 업데이트 수신 또는 스마트 라이선싱 기능 작동에 영향을 주지 않으므로 이러한 기능은 계속 정상적으로 작동됩니다. 자세한 내용은 Firepower 디바이스 매니저 구성 가이드, 버전 6.4.0+에서 시스템 관리 창의 **Cisco Success Network**에 연결 섹션을 참조하십시오.

Security Cloud Control에서 사용자 관리

Security Cloud Control에서 사용자 레코드를 생성하거나 편집하기 전에 ID 제공자 어카운트과 Security Cloud Control 사용자 레코드 간의 관계를 읽고 IdP(Identity Provider) 어카운트과 사용자 레코드의 상호 작용 방식을 확인하십시오. Security Cloud Control 사용자는 인증을 받고 Security Cloud Control 테넌트에 액세스할 수 있도록 레코드 및 해당 IdP 어카운트가 필요합니다.

엔터프라이즈에 자체 IdP가 없는 경우 Cisco Secure Sign-On은 모든 Security Cloud Control 테넌트에 대한 ID 제공자입니다. 이 문서의 나머지 부분에서는 Cisco Secure Sign-On을 ID 제공자로 사용한다고 가정합니다.

User Management(사용자 관리**)** 화면에서 테넌트와 연결된 모든 사용자 레코드를 볼 수 있습니다. 여기에는 지원 티켓을 해결하기 위해 사용자 어카운트와 일시적으로 연결된 모든 Cisco 지원 엔지니어가 포함됩니다.

테넌트에서 슈퍼 관리자 관리

테넌트의 슈퍼 관리자 수를 제한하는 것이 가장 좋습니다. 슈퍼 관리자 권한을 가져야 하는 사용자를 결정하고 User Management(사용자 관리)를 검토한 다음 다른 사용자의 역할을 "Admin(관리자)"으로 변경합니다.

테넌트와 연결된 **API** 사용자 기록 보기

프로시저

왼쪽 창에서 **Administration(**관리**)** > **API User Management(**사용자 관리**)**.

사용자 관리의 **Active Directory** 그룹

대량의 사용자에 대해 회전율이 높은 테넌트의 경우 개별 사용자를 Security Cloud Control에 추가하는 대신 Security Cloud Control를 AD(Active Directory) 그룹에 매핑하여 사용자 목록 및 사용자 역할을 더 쉽게 관리할 수 있습니다. 새 사용자 추가 또는 기존 사용자 제거와 같은 모든 사용자 변경은 이제 Active Directory에서 수행할 수 있으며 더 이상 Security Cloud Control에서 수행할 필요가 없습니다.

사용자 관리 페이지에서 AD(Active Directory) 그룹을 추가, 편집 또는 삭제하려면 **SuperAdmin** 사용자 역할이 있어야 합니다. 자세한 내용은 사용자 역할을 참조하십시오.

왼쪽 창에서, **Settings(**설정**)** > **User Management(**사용자 관리**)**를 선택합니다.

Active Directory 그룹

- 왼쪽 창에서 **Administration(**관리**)** > **API User Management(**사용자 관리**)** > **Active Directory Groups(**액티브 디렉토리 그룹**)**를 클릭합니다.
- 이 페이지에는 Active Directory 관리자에서 할당된 Active Directory 그룹의 역할이 표시됩니다.
- Active Directory 그룹 내의 사용자는 **Active Directory** 그룹 탭이나 사용자 탭에 개별적으로 나열되지 않습니다.

감사 로그

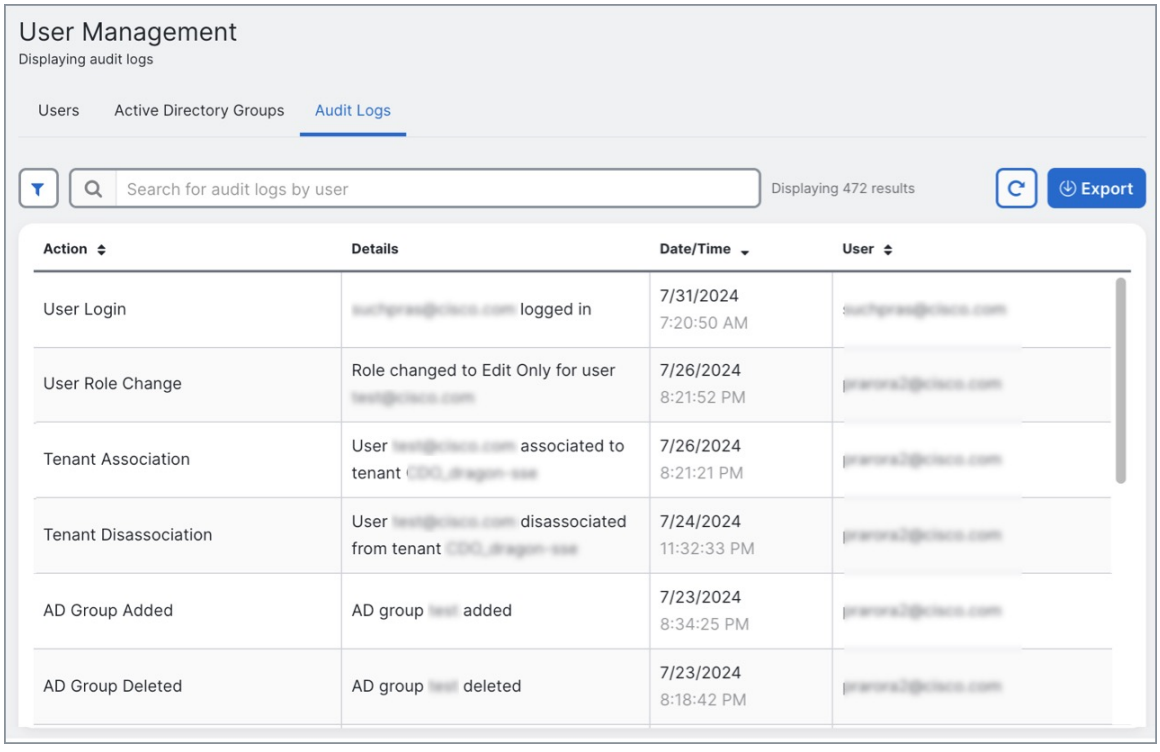
Security Cloud Control에서 감사 로그는 사용자 관련 및 시스템 수준 작업을 기록합니다. 감사 로그에 캡처되는 주요 이벤트는 다음과 같습니다.

- 사용자 로그인: 사용자 인증의 모든 인스턴스를 기록합니다.
- 테넌트 연결 및 연결 해제: 테넌트와의 사용자 연결 또는 테넌트와의 연결 해제를 추적합니다.
- 사용자 역할 변경: 사용자 역할에 대한 모든 변경 사항을 기록합니다.
- **Active Directory** 그룹: AD 그룹 내의 모든 추가, 삭제 및 역할 변경 사항을 기록합니다.

절차:

1. 왼쪽 창에서 **Administration(**관리**)** > **API User Management(**사용자 관리**)**를 클릭합니다.
2. **Audit Logs(**감사 로그**)** 탭을 클릭합니다. 로그인한 현재 테넌트의 이벤트 및 활동 목록이 표시됩니다.
3. **Search** (검색) 텍스트 상자를 사용하여 특정 사용자 에 대한 로그를 찾습니다.
4. 검색 결과를 구체화하고 특정 이벤트를 보려면 필터 아이콘을 클릭합니다. **Time Range(**시간 범위**)** 및 **Event Action(**이벤트 동작**)**을 기준으로 로그를 필터링할 수 있습니다.
5. CSV 형식으로 세부 정보를 다운로드하려면 **Export(**내보내기**)**를 클릭합니다.

그림 ***1:*** 감사 로그



다중 역할 사용자

Security Cloud Control의 IAM 기능에 따른 확장으로 이제 사용자가 여러 역할을 가질 수 있습니다.

사용자는 Active Directory에서 여러 그룹의 일부가 될 수 있으며 각 그룹은 Security Cloud Control에서 서로 다른 Security Cloud Control 역할로 정의될 수 있습니다. 로그인 시 사용자가 얻는 최종 권한은 해당 사용자가 속한 Security Cloud Control에 정의된 모든 Active Directory 그룹의 역할 조합입니다. 예를 들어 사용자가 두 개의 Active Directory 그룹에 속해 있고 두 그룹이 편집 전용 및 구축 전용과 같은 두 가지 다른 역할로 Security Cloud Control에 추가된 경우, 사용자는 편집 전용 및 구축 전용 권한을 모두 보유하게 됩니다. 이는 여러 그룹 및 역할에 적용됩니다.

Active Directory 그룹 매핑은 Security Cloud Control에서 한 번만 정의해야 하며, 이후에 다른 그룹 간에 사용자를 추가, 제거 또는 이동하여 사용자에 대한 액세스 및 권한 관리는 Active Directory에서만 독점적으로 수행할 수 있습니다.

참고 사용자가 개별 사용자이자 동일한 테넌트에 있는 Active Directory 그룹의 일부인 경우 개별 사용자의 사용자 역할이 Active Directory 그룹의 사용자 역할을 재정의합니다.

Active Directory 그룹에 대한 **API** 엔드포인트

슈퍼 관리자의 경우 API 엔드포인트를 사용하여 다음을 수행할 수 있습니다.

- Active Directory 그룹 생성
- Active Directory 그룹 제거
- Active Directory 그룹 수정
- Active Directory 그룹 가져오기
- Active Directory 그룹 가져오기

앞서 언급한 링크는 Cisco DevNet 웹사이트의 해당 섹션으로 연결됩니다.

Security Cloud Control에 Active Directory 그룹 추가 사전 요건

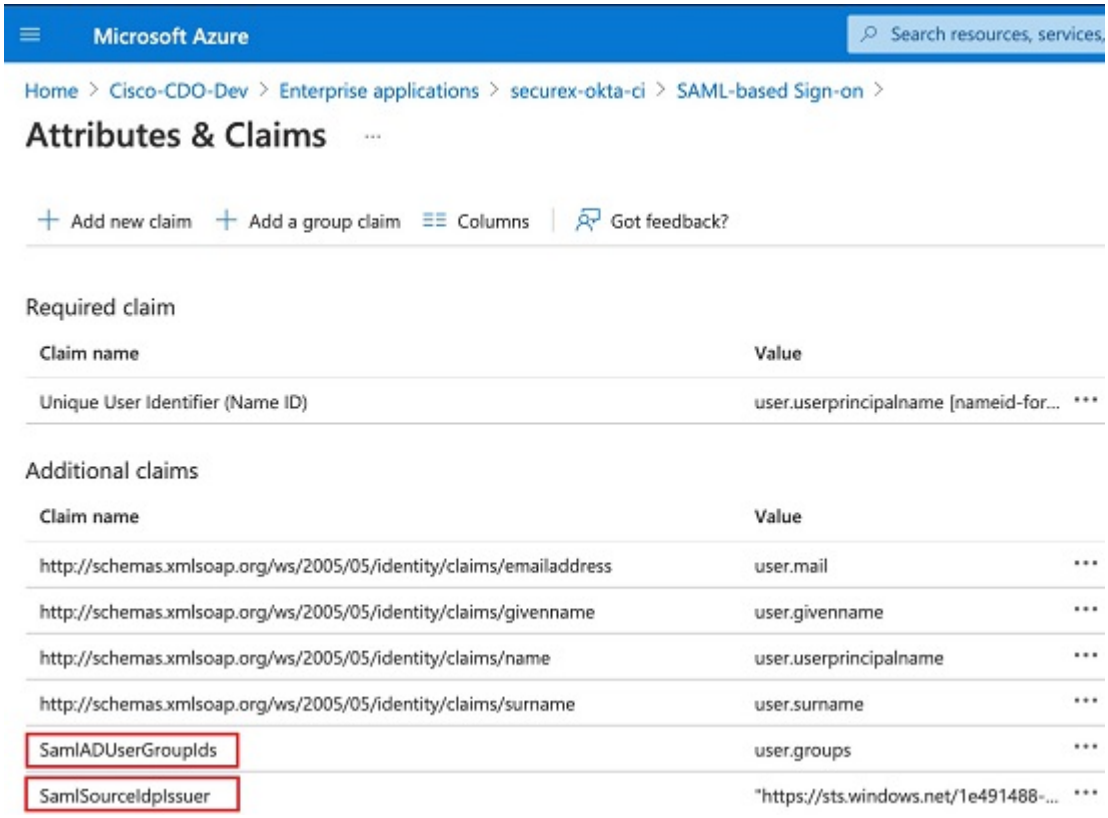
사용자 관리의 한 형태로 Active Directory 그룹 매핑을 Security Cloud Control에 추가하려면 먼저 Security Cloud Sign On와 통합된 Active Directory가 있어야 합니다. Active Directory ID 공급자(IdP)가 아직 통합되어 있지 않은 경우 다음 정보를 사용하여 사용자 지정 Active Directory IdP 통합을 통합하려면 ID 공급자 통합 가이드를 참조하십시오.

- Security Cloud Control 테넌트 이름 및 지역
- 사용자 지정 라우팅을 정의할 도메인(예: @cisco.com, @myenterprise.com)
- XML 형식의 인증서 및 페더레이션 메타데이터

Active Directory 통합이 완료되면 Active Directory에 다음 사용자 지정 SAML 클레임을 추가합니다. Active Directory 통합이 완료된 후 Security Cloud Control 테넌트에 로그인하려면 SAML 클레임 및 속성이 필요합니다. 값은 대/소문자를 구분합니다.

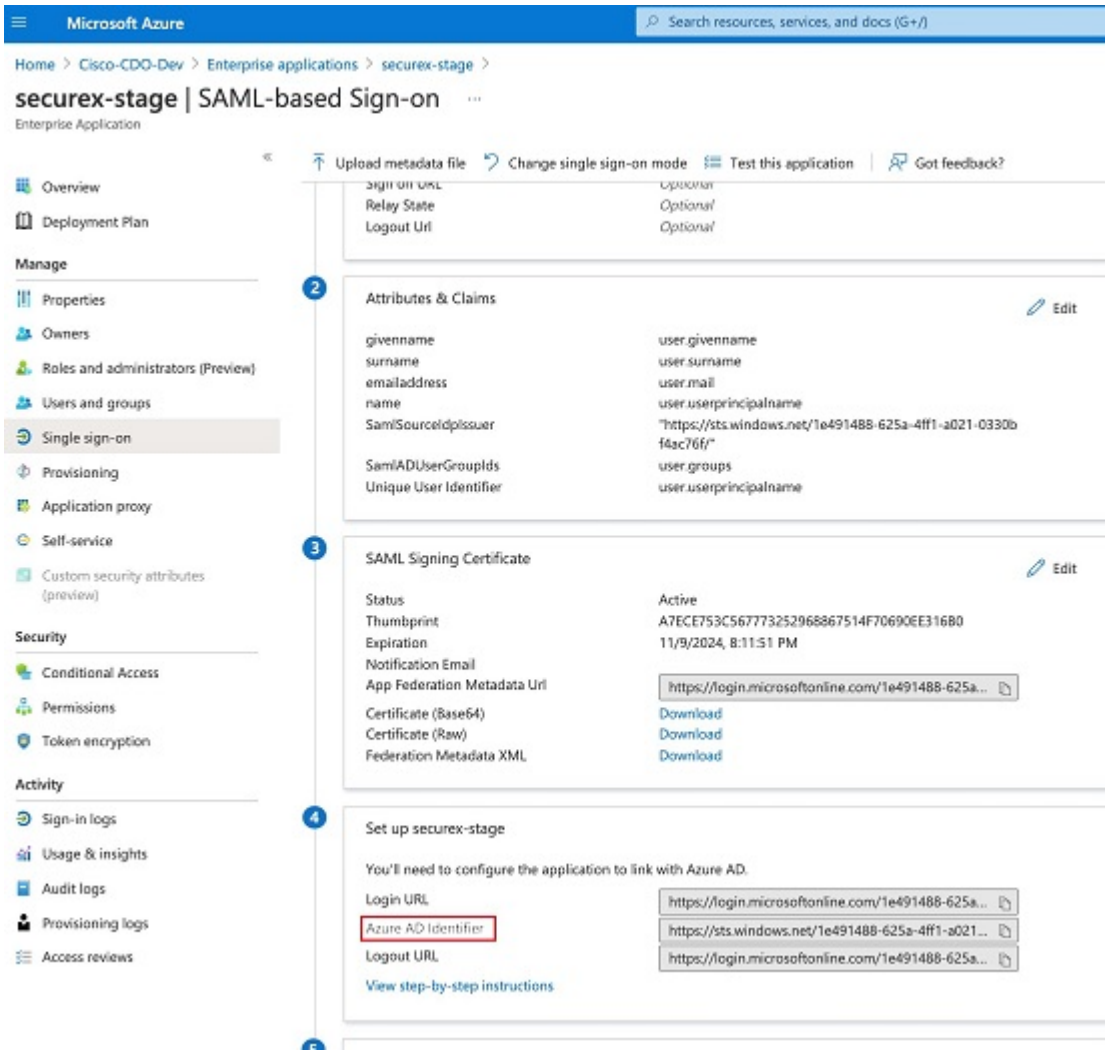
- **SamlADUserGroupIds** - 이 속성은 사용자가 Active Directory에 가지고 있는 모든 그룹 연결을 설명합니다. 예를 들어 Azure에서 아래 스크린샷과 같이 **+ Add a group claim(+** 그룹 클레임 추가**)**를 선택합니다.

  그림 ***2: Active Directory***에 정의된 사용자 지정 클레임



- **SamlSourceIdpIssuer** - 이 특성은 Active Directory 인스턴스를 고유하게 식별합니다. 예를 들어 Azure에서 **+ Add a group claim(+** 그룹 클레임 추가**)**를 선택하고 스크롤하여 아래 스크린샷과 같이 Azure Active Directory 식별자를 찾습니다.

그림 ***3: Azure Active Directory*** 식별자 찾기



사용자 관리를 위한 **Active Directory** 그룹 추가

Active Directory 그룹을 추가, 편집 또는 삭제하려면 **SuperAdmin(**슈퍼 관리자**)** 사용자 역할이 있어야 합니다.

프로시저

단계 **1** Security Cloud Control에 로그인합니다.

단계 **2** 왼쪽 창에서 **Administration(**관리**)** > **API User Management(**사용자 관리**)**를 클릭합니다.

단계 **3** **Active Directory** 그룹 탭을 클릭합니다.

단계 **4** Active Directory 그룹 추가( ) 버튼.

단계 **5** 다음 정보를 제공합니다.

- 그룹 이름: 고유한 이름을 입력합니다. 이 이름은 Active Directory의 그룹 이름과 일치하지 않아도 됩니다. Security Cloud Control에서는 이 필드에 대한 특수 문자를 지원하지 않습니다.
- 그룹 **ID**: Active Directory에서 그룹 ID를 수동으로 입력합니다. 그룹 ID의 값은 사용자 지정 클레임 정의의 그룹 ID와 동일해야 합니다. 그룹의 고유 ID에 해당하는 모든 값(예: my-favorite-group, 12345 등)이 될 수 있습니다.
- **AD** 발급자: Active Directory에서 Active Directory 발급자 값을 수동으로 입력합니다.
- 역할: 사용자 역할을 선택합니다. Active Directory 그룹에 포함된 모든 사용자의 역할을 결정합니다. 자세한 내용은 사용자 역할을 참조하십시오.
- (선택 사항) 참고: 이 Active Directory 그룹에 적용 가능한 참고를 추가합니다.

단계 **6** **OK(**확인**)**를 선택합니다.

사용자 관리를 위한 **Active Directory** 그룹 편집

시작하기 전에

Security Cloud Control에서 Active Directory 그룹의 사용자 관리를 편집하면 Security Cloud Control가 Active Directory그룹을 제한하는 방식만 편집할 수 있습니다. Security Cloud Control에서 Active Directory 그룹 자체는 편집할 수 없습니다. Active Directory 그룹 내의 사용자 목록을 편집하려면 Active Directory를 사용해야 합니다.

프로시저

단계 **1** Security Cloud Control에 로그인합니다.

단계 **2** 왼쪽 창에서 **Administration(**관리**)** > **API User Management(**사용자 관리**)**를 클릭합니다.

단계 **3** **Active Directory** 그룹 탭을 클릭합니다.

단계 **4** 편집하려는 Active Directory 그룹을 식별하고 편집 아이콘을 클릭합니다.

단계 **5** 다음 값을 수정합니다.

- 그룹 이름 - 고유한 이름을 입력합니다. Security Cloud Control에서는 이 필드에 대한 특수 문자를 지원하지 않습니다.
- 그룹 **ID**: Active Directory에서 그룹 ID를 수동으로 입력합니다. 그룹 ID의 값은 사용자 지정 클레임 정의의 그룹 ID와 동일해야 합니다. 그룹의 고유 ID에 해당하는 모든 값(예: my-favorite-group, 12345 등)이 될 수 있습니다.
- **AD** 발급자: Active Directory에서 Active Directory 발급자 값을 수동으로 입력합니다.

- 역할: 이 Active Directory 그룹에 포함된 모든 사용자의 역할을 결정합니다. 자세한 내용은 사용자 역할을 참조하십시오.
- 참고: 이 Active Directory 그룹에 적용 가능한 참고를 추가합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

사용자 관리를 위한 **Active Directory** 그룹 삭제

프로시저

단계 **1** Security Cloud Control에 로그인합니다.
단계 **2** 왼쪽 창에서 **Administration(**관리**)** > **API User Management(**사용자 관리**)**를 클릭합니다.
단계 **3** **Active Directory** 그룹 탭을 클릭합니다.
단계 **4** 삭제하려는 Active Directory 그룹을 식별합니다.
단계 **5** 삭제 아이콘을 클릭합니다.
단계 **6** **OK(**확인**)**를 클릭하여 Active Directory 그룹 삭제를 확인합니다.

새 **Security Cloud Control** 사용자 생성

이 두 가지 작업은 새 Security Cloud Control 사용자를 만드는 데 필요합니다. 순서대로 수행할 필요는 없습니다.

- 새 사용자를 위해 Cisco Secure Sign-On 어카운트 생성
- Security Cloud Control 사용자 이름으로 Security Cloud Control 사용자 레코드 생성

이러한 작업이 완료되면 사용자는 Cisco Secure Sign-On 대시보드에서 Security Cloud Control를 열 수 있습니다.

새 사용자를 위해 **Cisco Secure Cloud Sign On** 어카운트 생성

새 사용자는 할당된 테넌트의 이름을 몰라도 언제든지 Cisco Security Cloud Sign On 어카운트를 만들 수 있습니다.

Security Cloud Control에 로그인 정보

Security Cloud Control는 Cisco Secure Sign-On을 ID 제공자로 사용하며, MFA(multi-factor authentication)에는 Duo를 사용합니다. **Security Cloud Control**에 로그인하려면 먼저 **Cisco Security Cloud Sign On**에서 어카운트를 생성하고 **Duo**를 사용하여 **MFA**를 구성해야 합니다.

Security Cloud Control에는 사용자 ID를 보호하기 위해 추가 보안 레이어를 제공하는 MFA가 필요합니다. MFA 유형인 2단계 인증에서는 Security Cloud Control에 로그인하는 사용자의 ID를 확인하기 위해 두 가지 구성 요소 또는 요소가 필요합니다. 첫 번째 요소는 사용자 이름과 비밀번호이고, 두 번째 요소는 요청 시 생성되는 일회용 비밀번호(OTP)입니다.

Important **2019**년 **10**월 **14**일 이전에 **Security Cloud Control** 테넌트가 존재했다면 이 문서 대신 Cisco Secure Cloud Sign On ID 제공자로 마이그레이션를 사용하여 로그인 지침을 사용합니다.

로그인하기 전

DUO Security 설치

휴대전화에 Duo Security 앱을 설치하는 것이 좋습니다. Duo 설치에 대한 질문은 Duo 2단계 인증 가이드: 등록 가이드를 참조하십시오.

시간 동기화

모바일 디바이스를 사용하여 일회용 비밀번호를 생성합니다. OTP는 시간을 기반으로 하므로 디바이스 시계를 실시간으로 동기화하는 것이 중요합니다. 디바이스 시계가 자동으로 또는 수동으로 올바른 시간으로 설정되었는지 확인합니다.

새 Cisco Secure Cloud Sign On 어카운트 생성 및 Duo 다단계 인증 구성

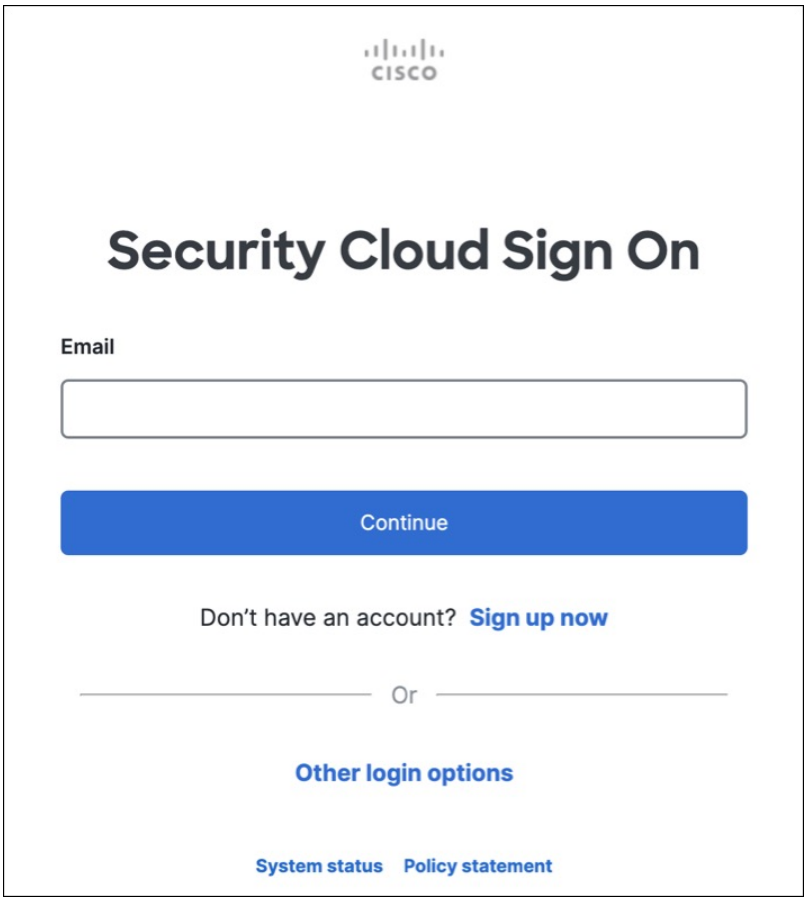
초기 로그인 워크플로우는 4단계 프로세스입니다. 4단계를 모두 완료해야 합니다.

Procedure

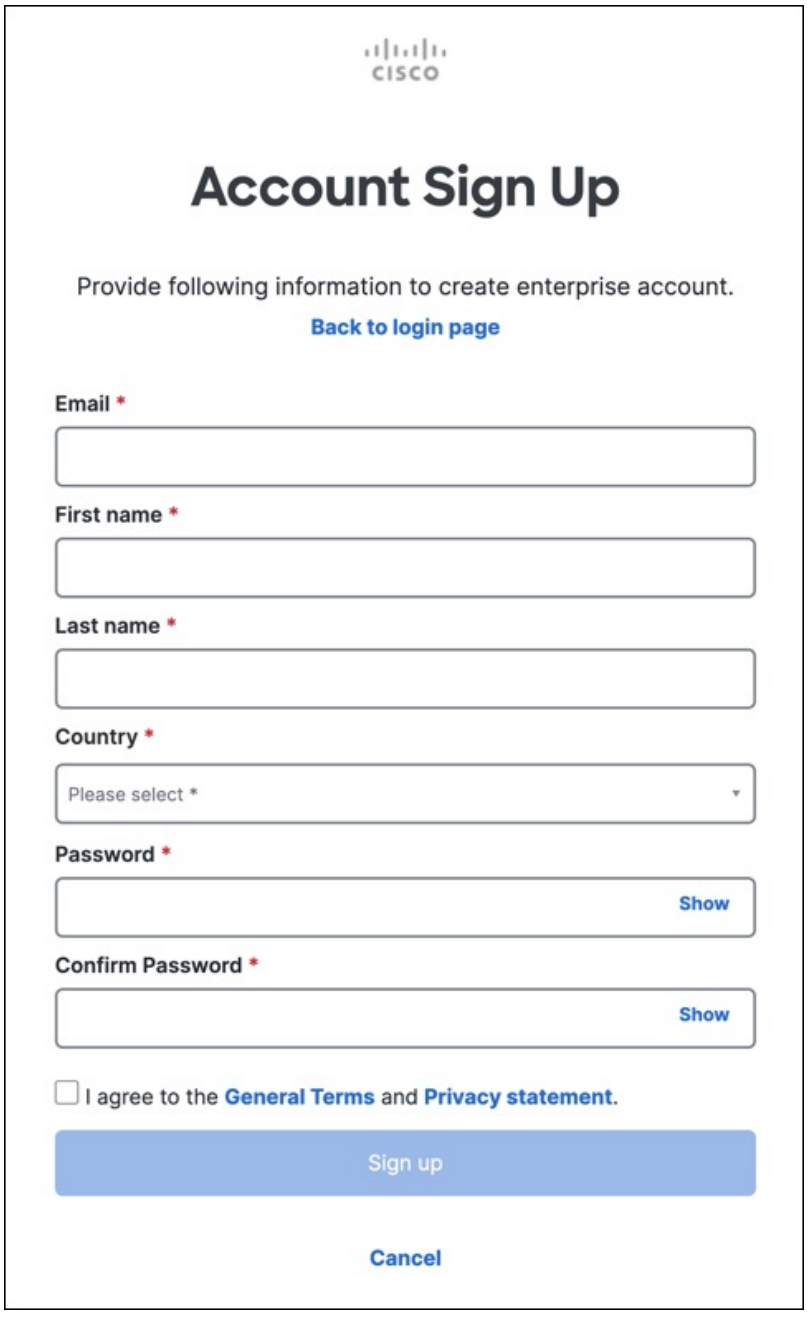
단계 **1** 새 **Cisco Security Cloud Sign On** 어카운트를 등록합니다.

a. https://sign-on.security.cisco.com을/를 엽니다.

b. 로그인 화면 하단에서 **Sign up now(**지금 등록**)**을 클릭합니다.



c. 기업 어카운트를 만들려면 다음 정보를 입력합니다.



다음은 몇 가지 팁입니다.

- **Email(**이메일**)**: Security Cloud Control에 로그인하는 데 사용할 이메일 주소를 입력합니다.
- **Password(**암호**)**: 강력한 암호를 입력하십시오.

d. **Sign up(**등록하기**)**을 클릭합니다.

Cisco는 등록한 주소로 확인 이메일을 보냅니다. 이메일을 열고 **Activate account(**어카운트 활성화**)**를 클릭합니다.

단계 **2** **Duo**를 통한 다단계 인증 설정

다단계 인증을 설정할 때는 모바일 디바이스를 사용하는 것이 좋습니다.

a. **Set up multi-factor authentication(**다단계 인증 설정**)** 화면에서 **Configure factor(**요인 구성**)**를 클릭합니다.

b. **Start setup(**설정 시작**)**을 클릭하고 프롬프트에 따라 모바일 디바이스를 선택하고 해당 모바일 디바이스와 어카운트의 페어링을 확인합니다.

자세한 내용은 Duo Guide to Two Factor Authentication: Enrollment Guide를 참조하십시오. 디바이스에 이미 Duo 앱이 있는 경우 이 어카운트에 대한 활성화 코드를 받게 됩니다. Duo는 하나의 디바이스에서 여러 어카운트를 지원합니다.

c. 마법사가 끝나면 **Continue to Login(**계속 로그인**)**를 클릭합니다.

d. 2단계 인증을 사용하여 Cisco Security Cloud Sign On에 로그인합니다.

단계 **3** **(**선택 사항**) Google OTP**를 추가 인증자로 설정

a. Google Authenticator와 페어링할 모바일 디바이스를 선택하고 **Next(**다음**)**를 클릭합니다.

b. 설정 마법사의 프롬프트에 따라 Google 인증기를 설정합니다.

단계 **4** **Cisco Security Cloud Sign On**에 대한 어카운트 복구 옵션 구성

a. SMS를 사용하여 어카운트를 재설정하려면 복원 전화번호를 선택합니다.

b. 보안 이미지를 선택합니다.

c. **Create My Account(**내 어카운트 생성**)**를 클릭합니다.

Security Cloud Control 사용자 이름으로 사용자 레코드 생성

슈퍼 관리자 권한이 있는 Security Cloud Control 사용자만 Security Cloud Control 사용자 레코드를 생성할 수 있습니다. 슈퍼 관리자는 위의 **Create Your Security Cloud Control Username(**사용자 이름 생성**)** 작업에서 지정한 것과 동일한 이메일 주소로 사용자 레코드를 만들어야 합니다.

적절한 사용자 역할이 있는 사용자 레코드를 생성하려면 다음 절차를 수행합니다.

Procedure

단계 **1** Security Cloud Control에 로그인합니다.

단계 **2** 왼쪽 창에서, **Settings(**설정**)** > **User Management(**사용자 관리**)**를 선택합니다.

단계 **3** 테넌트에 새 사용자를 추가하려면  를 클릭합니다.

단계 **4** 사용자의 이메일 주소를 입력합니다.

Note

사용자의 이메일 주소는 Cisco Secure Log-On 어카운트의 이메일 주소와 일치해야 합니다.

단계 **5** **Role(**역할**)** 드롭다운 목록에서 사용자의 역할을 선택합니다.
단계 **6** **OK(**확인**)**를 클릭합니다.

새 사용자가 **Cisco Secure Sign-On** 대시보드에서 **Security Cloud Control** 열기

Procedure

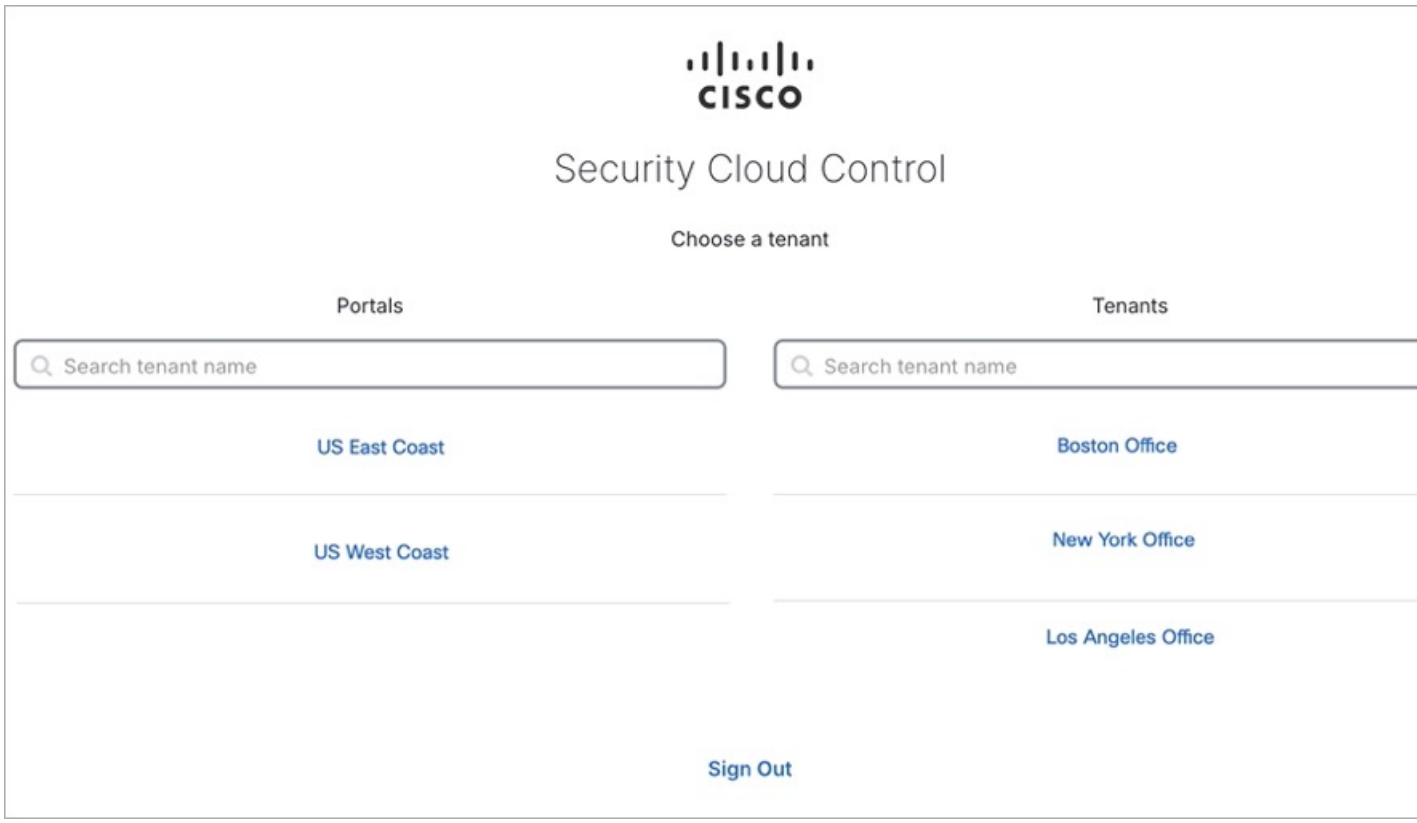
단계 **1** 테넌트 지역의 Cisco Secure Sign-on 대시보드에서 적절한 **Security Cloud Control** 타일을 클릭합니다.
단계 **2** 두 인증자를 모두 설정한 경우 인증자 로고를 클릭하여 Duo Security 또는 Google Authenticator를 선택합니다.

- 기존 테넌트에 사용자 레코드가 이미 있는 경우 해당 테넌트에 로그인됩니다.
- 이미 여러 포털에 사용자 레코드가 있는 경우 연결할 포털을 선택할 수 있습니다.
- 여러 테넌트에 대한 사용자 레코드가 이미 있는 경우 연결할 Security Cloud Control 테넌트를 선택할 수 있습니다.
- 기존 테넌트에 대한 사용자 레코드가 아직 없는 경우 Security Cloud Control에 대해 자세히 알아보거나 평가판 테넌트를 요청할 수 있습니다.

포털 보기는 여러 테넌트에서 통합된 정보를 검색하고 표시합니다.

자세한 내용은 여러 Security Cloud Control 테넌트 관리를 참조하십시오.

테넌트 보기에는 사용자 레코드가 있는 여러 테넌트가 표시됩니다.



Security Cloud Control의 사용자 역할

Security Cloud Control에는 읽기 전용, 편집 전용, 구축 전용, 관리자, 슈퍼 관리자 등 다양한 사용자 역할이 있습니다. 사용자 역할은 각 테넌트의 각 사용자에 대해 구성됩니다. Security Cloud Control 사용자가 둘 이상의 테넌트에 액세스할 수 있는 경우, 사용자 ID는 동일하지만 테넌트마다 역할이 다를 수 있습니다. 사용자는 한 테넌트에 대해서는 읽기 전용 역할을, 다른 테넌트에서는 슈퍼 관리자 역할을 가질 수 있습니다. 인터페이스 또는 설명서에서 읽기 전용 사용자, Admin 사용자 또는 Super Admin 사용자를 언급하는 경우 특정 테넌트에 대한 사용자의 권한 수준을 의미합니다.

읽기 전용 역할

읽기 전용 역할이 할당된 사용자는 모든 페이지에서 이 파란색 배너를 볼 수 있습니다.

Read Only User. You cannot make configuration changes.

읽기 전용 역할의 사용자는 다음을 수행할 수 있습니다.

- Security Cloud Control의 모든 페이지 또는 설정을 봅니다.
- 모든 페이지의 콘텐츠를 검색하고 필터링합니다.

- 디바이스 구성을 비교하고 변경 로그를 보고 VPN 매핑을 확인합니다.
- 모든 페이지의 모든 설정 또는 개체에 관한 모든 경고를 봅니다.
- 자체 API 토큰을 생성, 새로 고침 및 취소합니다. 읽기 전용 사용자가 자신의 토큰을 취소하면 다시 생성할 수 없습니다.
- 인터페이스를 통해 지원팀에 문의하고 변경 로그를 내보낼 수 있습니다.

읽기 전용 사용자는 다음을 수행할 수 없습니다.

- 모든 페이지에서 무엇이든 생성, 업데이트, 구성 또는 삭제합니다.
- 디바이스를 온보딩합니다.
- 개체 또는 정책과 같은 항목을 만드는 데 필요한 작업을 단계별로 진행하지만 저장할 수는 없습니다.
- Security Cloud Control 사용자 레코드를 생성합니다.
- 사용자 역할을 변경합니다.
- 액세스 규칙을 정책에 연결하거나 분리합니다.

편집 전용 역할

편집 전용 역할이 있는 사용자는 다음을 수행할 수 있습니다.

- 개체, 정책, 규칙 세트, 인터페이스, VPN 등을 포함하되 이에 국한되지 않는 디바이스 구성을 편집하고 저장합니다.
- **Read Configuration(**구성 읽기**)** 작업을 통해 이루어진 구성 변경을 허용합니다.
- 변경 요청 관리 작업을 활용합니다.

편집 전용 사용자는 다음을 수행할 수 없습니다**.**

- 디바이스 또는 여러 디바이스에 변경 사항을 구축합니다.
- 단계적 변경 또는 OOB를 통해 감지된 변경을 폐기합니다.
- AnyConnect 패키지를 업로드하거나 이러한 설정을 구성합니다.
- 디바이스에 대한 이미지 업그레이드를 예약하거나 수동으로 시작합니다.
- 보안 데이터베이스 업그레이드를 예약하거나 수동으로 시작합니다.
- Snort 2와 Snort 3 버전 사이를 수동으로 전환합니다.
- 템플릿을 생성합니다.
- 기존 OOB 변경 설정을 변경합니다.
- 시스템 관리 설정을 수정합니다.

- 디바이스를 온보딩합니다.
- 디바이스를 삭제합니다.
- VPN 세션 또는 사용자 세션을 삭제합니다.
- Security Cloud Control 사용자 레코드를 생성합니다.
- 사용자 역할을 변경합니다.

구축 전용 역할

구축 전용 역할이 있는 사용자는 다음을 수행할 수 있습니다.

- 디바이스 또는 여러 디바이스에 단계적 변경 사항을 구축합니다.
- ASA 디바이스에 대한 구성 변경 사항을 되돌리거나 복원합니다.
- 디바이스에 대한 이미지 업그레이드를 예약하거나 수동으로 시작합니다.
- 보안 데이터베이스 업그레이드를 예약하거나 수동으로 시작합니다.
- 변경 요청 관리 작업을 활용합니다.

구축 전용 사용자는 다음을 수행할 수 없습니다**.**

- Snort 2와 Snort 3 버전 사이를 수동으로 전환합니다.
- 템플릿을 생성합니다.
- 기존 OOB 변경 설정을 변경합니다.
- 시스템 관리 설정을 수정합니다.
- 디바이스를 온보딩합니다.
- 디바이스를 삭제합니다.
- VPN 세션 또는 사용자 세션을 삭제합니다.
- 모든 페이지에서 무엇이든 생성, 업데이트, 구성 또는 삭제합니다.
- 디바이스를 온보딩합니다.
- 개체 또는 정책과 같은 항목을 만드는 데 필요한 작업을 단계별로 진행하지만 저장할 수는 없습니다.
- Security Cloud Control 사용자 레코드를 생성합니다.
- 사용자 역할을 변경합니다.
- 액세스 규칙을 정책에 연결하거나 분리합니다.

VPN 세션 관리자 역할

VPN 세션 관리자 역할은 사이트 간 VPN 연결이 아닌 원격 액세스 VPN 연결을 모니터링하는 관리자를 위해 설계되었습니다.

VPN 세션 관리자 역할이 있는 사용자는 다음을 수행할 수 있습니다.

- Security Cloud Control의 모든 페이지 또는 설정을 봅니다.
- 모든 페이지의 콘텐츠를 검색하고 필터링합니다.
- 디바이스 구성을 비교하고 변경 로그를 보고 RA VPN 매핑을 확인합니다.
- 모든 페이지의 모든 설정 또는 개체에 관한 모든 경고를 봅니다.
- 자체 API 토큰을 생성, 새로 고침 및 취소합니다. 참고로 VPN 세션 관리자 사용자가 자신의 토큰을 취소하면 토큰을 다시 만들 수 없습니다.
- 인터페이스를 통해 지원팀에 문의하고 변경 로그를 내보냅니다.
- 기존 RA VPN 세션을 종료합니다.

VPN 세션 관리자 사용자는 다음을 수행할 수 없습니다**.**

- 모든 페이지에서 무엇이든 생성, 업데이트, 구성 또는 삭제합니다.
- 디바이스를 온보딩합니다.
- 개체 또는 정책과 같은 항목을 만드는 데 필요한 작업을 단계별로 진행하지만 저장할 수는 없습니다.
- Security Cloud Control 사용자 레코드를 생성합니다.
- 사용자 역할을 변경합니다.
- 액세스 규칙을 정책에 연결하거나 분리합니다.

관리자 역할

관리자는 Security Cloud Control의 모든 측면에 대한 완전한 액세스 권한을 갖습니다. 관리 사용자는 다음을 수행할 수 있습니다.

- Security Cloud Control에서 개체 또는 정책을 생성, 읽기, 업데이트 및 삭제하고 설정을 구성합니다.
- 디바이스를 온보딩합니다.
- Security Cloud Control의 모든 페이지 또는 설정을 봅니다.
- 모든 페이지의 콘텐츠를 검색하고 필터링합니다.
- 디바이스 구성을 비교하고 변경 로그를 보고 VPN 매핑을 확인합니다.
- 모든 페이지의 모든 설정 또는 개체에 관한 모든 경고를 봅니다.

- 자체 API 토큰을 생성, 새로 고침 및 취소합니다. 토큰이 취소되면 인터페이스를 통해 지원팀에 문의하고 변경 로그를 내보낼 수 있습니다.

관리 사용자는 다음을 수행할 수 없습니다.

- Security Cloud Control 사용자 레코드를 생성합니다.
- 사용자 역할을 변경합니다.

슈퍼 관리자

슈퍼 관리자는 Security Cloud Control의 모든 측면에 대한 완전한 액세스 권한을 갖습니다. 슈퍼 관리자는 다음을 수행할 수 있습니다.

- 사용자 역할을 변경합니다.
- 사용자 레코드를 생성합니다.

Note 최고 관리자는 Security Cloud Control 사용자 레코드를 생성할 수 있지만 사용자가 테넌트에 로그인하는 데 필요한 모든 사용자 레코드는 아닙니다. 사용자는 테넌트에서 사용하는 ID 제공자의 어카운트도 필요합니다. 엔터프라이즈에 자체 SSO(Single Sign-On) ID 제공자가 없는 경우 ID 제공자는 Cisco Secure Cloud Sign-on입니다. 사용자는 Cisco Secure Cloud Sign-On 어카운트에 자가 등록할 수 있습니다. 자세한 내용은 새 Security Cloud Control 테넌트에 대한 초기 로그인를 참조하십시오.

- Security Cloud Control에서 개체 또는 정책을 생성, 읽기, 업데이트 및 삭제하고 설정을 구성합니다.
- 디바이스를 온보딩합니다.
- Security Cloud Control의 모든 페이지 또는 설정을 봅니다.
- 모든 페이지의 콘텐츠를 검색하고 필터링합니다.
- 디바이스 구성을 비교하고 변경 로그를 보고 VPN 매핑을 확인합니다.
- 모든 페이지의 모든 설정 또는 개체에 관한 모든 경고를 봅니다.
- 자체 API 토큰을 생성, 새로 고침 및 취소합니다. 토큰이 취소되면 다음을 수행할 수 있습니다.
- 인터페이스를 통해 지원팀에 문의하고 변경 로그를 내보낼 수 있습니다.

사용자 역할의 기록 변경

사용자 레코드는 사용자의 현재 역할이 기록된 것입니다. 테넌트와 연결된 사용자를 보면 레코드별로 각 사용자의 역할을 확인할 수 있습니다. 사용자 역할을 변경하면 사용자 레코드가 변경됩니다. 사용자의 역할은 사용자 관리 테이블에서 해당 역할로 식별됩니다. 자세한 내용은 User Management(사용자 관리)를 참조하십시오.

사용자 레코드를 변경하려면 슈퍼 관리자여야 합니다. 테넌트에 슈퍼 관리자가 없는 경우 Security Cloud Control 지원에 문의하십시오.

Security Cloud Control에 사용자 어카운트 추가

Security Cloud Control 사용자는 인증을 받고 Security Cloud Control 테넌트에 액세스할 수 있도록 Security Cloud Control 레코드 및 해당 IdP 어카운트가 필요합니다. 이 절차는 Cisco Secure Cloud Sign-On의 사용자 어카운트가 아니라 사용자의 Security Cloud Control 사용자 레코드를 생성합니다. 사용자가 Cisco Security Cloud Sign On에 어카운트가 없는 경우, https://sign-on.security.cisco.com로 이동하고 로그인 화면 하단에서 **Sign up(**등록**)**을 클릭하여 자가 등록할 수 있습니다.

Note 이 작업을 수행하려면 Security Cloud Control에서 슈퍼 관리자 역할이 있어야 합니다.

사용자 레코드 생성

적절한 사용자 역할이 있는 사용자 레코드를 생성하려면 다음 절차를 수행합니다.

Procedure

단계 **1** Security Cloud Control에 로그인합니다.

단계 **2** 왼쪽 창에서 **Administration(**관리**)** > **API User Management(**사용자 관리**)**를 클릭합니다.

단계 **3** 테넌트에 새 사용자를 추가하려면 파란색 플러스 버튼(+)을 클릭합니다.

단계 **4** 사용자의 이메일 주소를 입력합니다.

Note
사용자의 이메일 주소는 Cisco Secure Log-On 어카운트의 이메일 주소와 일치해야 합니다.

단계 **5** 드롭다운 메뉴에서 사용자 역할을 선택합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

Note
최고 관리자는 Security Cloud Control 사용자 레코드를 생성할 수 있지만 사용자가 테넌트에 로그인하는 데 필요한 모든 사용자 레코드는 아닙니다. 사용자는 테넌트에서 사용하는 ID 제공자의 어카운트도 필요합니다. 엔터프라이즈에 자체 SSO(Single Sign-On) ID 제공자가 없는 경우 ID 제공자는 Cisco Secure Sign-on입니다. 사용자는 Cisco Secure Sign-On 어카운트에 자가 등록할 수 있습니다. 자세한 내용은 새 Security Cloud Control 테넌트에 대한 초기 로그인를 참조하십시오.

사용자 역할에 대한 사용자 레코드 편집

이 작업을 수행하려면 슈퍼 관리자 역할이 있어야 합니다. 슈퍼 관리자가 로그인한 Security Cloud Control 사용자의 역할을 변경할 경우 역할이 변경되면 해당 사용자는 자동으로 세션에서 로그아웃됩니다. 사용자가 다시 로그인하면 새 역할을 맡게 됩니다.

Note 이 작업을 수행하려면 Security Cloud Control에서 슈퍼 관리자 역할이 있어야 합니다.

Caution 사용자 레코드의 역할을 변경하면 사용자 레코드와 연결된 API 토큰이 있는 경우 해당 토큰이 삭제됩니다. 사용자 역할이 변경되면 사용자는 새 API 토큰을 생성해야 합니다.

사용자 역할 편집

Note Security Cloud Control 사용자가 로그인되어 있고 슈퍼 관리자가 역할을 변경하는 경우, 변경 사항을 적용하려면 사용자가 로그아웃했다가 다시 로그인해야 합니다.

사용자 레코드에 정의된 역할을 편집하려면 다음 절차를 따르십시오.

Procedure

단계 **1** Security Cloud Control에 로그인합니다.

단계 **2** 왼쪽 창에서 **Administration(**관리**)** > **API User Management(**사용자 관리**)**를 클릭합니다.

단계 **3** 사용자 행에서 편집 아이콘을 클릭합니다.

단계 **4** 역할 드롭다운 메뉴에서 사용자의 새 역할을 선택합니다.

단계 **5** 사용자 레코드에 사용자와 연결된 API 토큰이 있는 것으로 표시되면 사용자의 역할을 변경하고 결과적으로 API 토큰을 삭제할 것임을 확인해야 합니다.

단계 **6** **v**를 클릭합니다.

단계 **7** Security Cloud Control가 API 토큰을 삭제한 경우 사용자에게 연락하여 새 API 토큰을 생성합니다.

Note
Dynamic Attributes Connector 서비스 어카운트(csdac-service@tenantname)의 API 전용 사용자에 대한 **Revoke(**취소**)**, **Refresh(**새로고침**)**, **Delete(**삭제**)**및 **Edit(**편집**)** 옵션이 비활성됩니다. 이는 고객이 이 API 어카운트의 API 토큰을 삭제, 편집 또는 취소하지 않도록 하기 위한 것으로, Dynamic Attributes Connector 기능에 필요합니다.

사용자 역할에 대한 사용자 레코드 삭제

Security Cloud Control에서 사용자 레코드를 삭제하면 Cisco Secure Cloud Sign-On 어카운트과 사용자 레코드의 매핑이 끊어져 연결된 사용자가 Security Cloud Control에 로그인할 수 없습니다. 사용자 레코드를 삭제하면 해당 사용자 레코드와 연결된 API 토큰도 삭제됩니다. Security Cloud Control에서 사용자 레코드를 삭제해도 Cisco Secure Cloud Sign-On에서 사용자의 IdP 어카운트는 삭제되지 않습니다.

Note 이 작업을 수행하려면 Security Cloud Control에서 슈퍼 관리자 역할이 있어야 합니다.

사용자 레코드 삭제

사용자 레코드에 정의된 역할을 삭제하려면 다음 절차를 참조하십시오.

Procedure

단계 **1** Security Cloud Control에 로그인합니다.

단계 **2** 왼쪽 창에서 **Administration(**관리**)** > **API User Management(**사용자 관리**)**를 클릭합니다.

단계 **3** 삭제할 사용자 행에서 휴지통 아이콘를 클릭합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** 확인을 클릭하여 테넌트에서 어카운트를 제거할 것임을 확인합니다.

Note
Dynamic Attributes Connector 서비스 어카운트(csdac-service@tenantname)의 API 전용 사용자에 대한 **Revoke(**취소**)**, **Refresh(**새로고침**)**, **Delete(**삭제**)**및 **Edit(**편집**)** 옵션이 비활성됩니다. 이는 고객이 이 API 어카운트의 API 토큰을 삭제, 편집 또는 취소하지 않도록 하기 위한 것으로, Dynamic Attributes Connector 기능에 필요합니다.

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.