Policy Analyzer and Optimizer

Security Cloud Control는 정책 분석기 및 옵티마이저를 제공합니다. 이 지능형 클라우드 서비스는 보안 정책을 분석하고, 변칙을 탐지하며, 정책을 최적화하기 위해 수행할 수 있는 교정에 대한 권장 사항을 제공합니다.

- 정책 분석기 및 옵티마이저 정보, 1 페이지
- 정책 분석기 및 옵티마이저 이용하기 위한 사전 요건, 3 페이지
- 정책 분석기 및 옵티마이저 라이선싱 요건, 4 페이지
- 클라우드 제공 Firewall Management Center에 대해 정책 분석기 및 옵티마이저 활성화, 4 페이지
- Security Cloud Control 매니지드 온프레미스 방화벽 Management Center에 대해 정책 분석기 및 옵티마이저 활성화, 4 페이지
- 정책 분석, 5 페이지
- 정책 보고, 7 페이지
- 정책 교정, 12 페이지
- 정책 분석기 및 옵티마이저 문제 해결, 14 페이지
- Policy Analyzer and Optimizer에 대한 FAQ(자주 묻는 질문), 15 페이지

정책 분석기 및 옵티마이저 정보

방화벽용 AIOps는 인공 지능(AI)과 머신러닝(ML)을 활용하여 네트워크 방화벽의 관리 및 보안을 간소화하고 강화합니다. 동적 기준선과 고급 예측 모델을 활용하여 AIOps는 정책 변칙을 감지하고 잠재적 문제가 확대되기 전에 예측함으로써 사전 예방적 유지보수와 안정성을 보장합니다. AIOps의 주요 기능 중 하나는 정책 분석기 및 옵티마이저입니다. AIOps 인사이트를 참조하여 AIOps가 제공하는 다양한 기타 기능에 대해 자세히 알아보십시오.

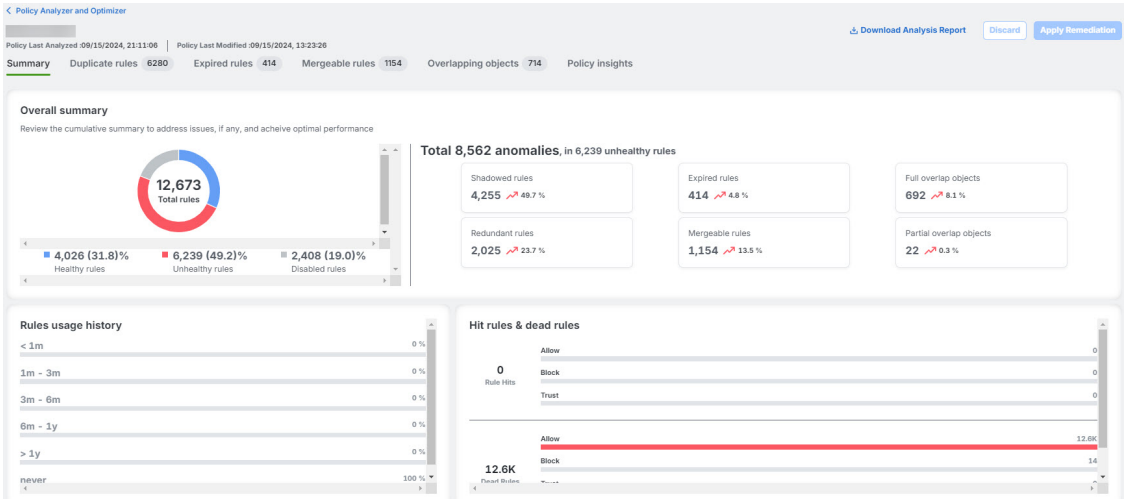
광범위한 액세스 제어 정책을 사용하는 Secure Firewall Threat Defense 디바이스에는 중복되거나 섀도잉된 규칙이 많이 있을 수 있습니다. 최적화되지 않은 규칙 집합으로 인해 비대해진 디바이스 메모리 과다 사용, 규칙 로딩 지연, 검색 시간 증가로 이어져 보안 정책 적용 효율성 저하, 네트워크 속도 감소, 구축 기간 연장을 초래할 수 있습니다.

이러한 상황을 처리하기 위해 Security Cloud Control는 정책 분석기 및 옵티마이저를 제공합니다. 이 지능형 클라우드 서비스는 보안 정책을 분석하고, 변칙을 탐지하며, 정책을 최적화하기 위해 수행할 수 있는 교정에 대한 권장 사항을 제공하여 방화벽 성능을 개선합니다. 정책 분석기 및 옵티마이저는

Security Cloud Control에 온보딩된 클라우드 제공 Firewall Management Center 및 온프레미스 방화벽 Management Center 모두의 정책을 분석할 수 있습니다. 이 기능은 다음 작업도 수행할 수 있습니다.

- 적중 횟수를 기반으로 하는 분석 개요 및 정책 인사이트를 포함하여 정책 상태 정보의 포괄적인 시각화를 제공합니다.
- 예약된 간격으로 또는 원하는 경우 언제든지 정기적으로 정책을 분석합니다.
- 중복 규칙, 규칙에서의 개체 중복 및 만료된 규칙과 같은 규칙 변칙을 탐지합니다.

그림 *1:* 분석 요약



정책 분석기 및 옵티마이저는 Security Cloud Control의 **Services(**서비스**)** 페이지, 왼쪽 창의 **Monitor(**모니터링**)** > **Insights & Reports(**인사이트 및 보고서**)** > **AIOps Insights(**인사이트**)** > **Policy Analyzer and Optimizer(**정책 분석기 및 옵티마이저**)**, 관리자 편의를 위한 및 온프레미스 방화벽 Management Center의 **Access Control(**액세스 제어**)** 정책 페이지에서 실행할 수 있습니다.

분석, 교정 및 보고

정책 분석기 및 옵티마이저는 분석, 교정 및 보고 서비스를 수행합니다.

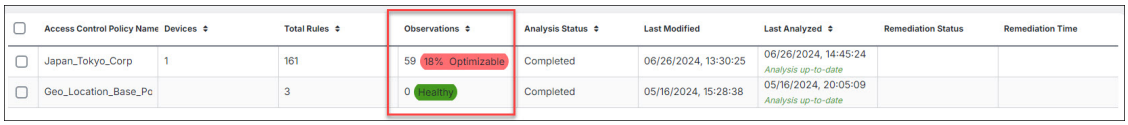
분석

정책 분석기 및 옵티마이저는 정책에 대한 클라우드 제공 Firewall Management Center 및 온프레미스 방화벽 Management Center를 폴링하고 정책 분석기 및 옵티마이저 페이지에 표시합니다. **Policy Analyzer and Optimizer(**정책 분석기 및 옵티마이저**)** 페이지를 열려면 왼쪽 창에서 **Administration(**관리**)** > **Integration(**통합**)** > **Firewall Management Center**를 클릭하고 클라우드 제공 **FMC** 또는 임의 온프레미스 방화벽 Management Center를 선택하고 오른쪽 창에서 **Policy Analyzer and Optimizer(**정책 분석기 및 옵티마이저**)**를 선택합니다. 또는 Security Cloud Control 왼쪽 창에서 **Monitor(**모니터링**)** > **Insights & Reports(**인사이트 및 보고서**)** > **AIOps Insights(**인사이트**)** > **Policy Analyzer and Optimizer(**정책 분석기 및 옵티마이저**)**를 선택합니다. 클라우드 제공 **FMC**를 선택하거나 왼쪽 상단의 **Data Source(**데이터 소스**)** 탭에서 온프레미스 방화벽 Management Center를 선택합니다.

새 액세스 제어 정책을 생성하거나 가져온 정책을 정책 분석기 및 옵티마이저에서 식별하는 데 다소 시간이 걸립니다. 그 후에는 정책 분석을 수동으로 트리거할 수 있습니다. 24시간마다 제공되는 자동 분석을 기다릴 수도 있습니다.

참고 온프레미스 방화벽 Management Center를 Security Cloud Control에 온보딩할 수 없는 경우, 정책을 SFO 파일로 내보내고 클라우드 제공 Firewall Management Center로 가져와 분석을 트리거할 수 있습니다.

분석이 완료되면 정책 분석기 및 옵티마이저는 정책의 규칙 수, 최적화할 수 있는 정책의 비율, 그리고 규칙 상태 요약, 규칙 마지막 사용, 규칙 적중 및 사용 불능 규칙 등의 정보가 포함된 상세 요약을 제공합니다.



참고 **Observations(**관찰**)** 열 아래의 **Optimizable(**최적화 가능**)** 비율은 제안된 교정이 적용되는 경우 최적화할 수 있는 정책 수의 근사치입니다.

보안정책 교정

정책 분석 요약은 보안 정책의 상태를 설명하며, 정책 분석기 및 옵티마이저이 제안한 교정 중 정책에 적용할 항목을 선택할 수 있도록 합니다. 제안된 교정을 사용하여 중복 규칙, 중복 개체, 만료된 규칙을 비활성화하거나 삭제할 수 있으며, 허용 및 차단 설정이 유사한 규칙은 하나의 규칙으로 병합할 수 있습니다. 적중 횟수 데이터는 **Policy Insights(**정책 인사이트**)** 탭 아래에 나열됩니다. **Apply Remediation(**교정 적용**)**을 선택하여 선택한 교정을 정책에 적용할 수 있습니다.

보고

분석이 완료되면 자세한 분석 보고서를 사용할 수 있습니다. 정책에 교정이 적용된 후에는 교정 보고서도 사용할 수 있습니다. 교정 보고서에는 존재하는 정책 변칙 및 적용된 교정의 통합 목록이 포함되며 PDF로 다운로드할 수 있습니다.

정책 분석기 및 옵티마이저 이용하기 위한 사전 요건

- 온프레미스 방화벽 Management Center는 버전 7.2 이상이어야 하며 Security Cloud Control에 온보딩되어야 합니다. 분석하려는 정책이 최소한 하나의 디바이스와 연결되어 있는지 확인합니다.
- 온프레미스 방화벽 Management Center 버전 7.6 이상은 Cisco Security Cloud와 통합되어야 합니다. 온프레미스 방화벽 Management Center는 Security Cloud 통합의 일부로 선택한 Security Cloud Control 테넌트에 온보딩됩니다.

정책 분석기 및 옵티마이저 라이선싱 요건

정책 분석기 및 옵티마이저는 추가 라이선싱이 필요하지 않습니다. Security Cloud Control 기본 구독의 일부로 제공됩니다.

클라우드 제공 **Firewall Management Center**에 대해 정책 분석기 및 옵티마이저 활성화

정책 분석기 및 옵티마이저는 기본적으로 클라우드 제공 Firewall Management Center에 대해 활성화되어 있습니다. 이를 클라우드 제공 Firewall Management Center의 액세스 정책을 분석하는 데 사용하려면 다음 단계를 수행합니다.

프로시저

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

단계 **2** 기본적으로 클라우드 제공 Firewall Management Center가 선택되어 있는 **Services(**서비스**)** 페이지가 열립니다.

단계 **3** 오른쪽 창 **System(**시스템**)** 아래에서 **Policy Analyzer and Optimizer(**정책 분석기 및 옵티마이저**)**를 클릭합니다.

이제 클라우드 제공 Firewall Management Center의 액세스 제어 정책이 나열된 것을 볼 수 있습니다. 하나를 선택하여 분석하거나 이미 분석된 정책의 세부 정보를 볼 수 있습니다.

Security Cloud Control 매니지드 온프레미스 방화벽 **Management Center**에 대해 정책 분석기 및 옵티마이저 활성화

온프레미스 방화벽 Management Center 버전 7.2 이상을 사용하는 경우, 이를 SecureX 와 통합하고 온프레미스 방화벽 Management Center를 Security Cloud Control에 온보딩하고, **Administration(**관리**)** > **Integration(**통합**)** > **Firewall Management Center**로 이동하여 온프레미스 방화벽 Management Center를 선택하고, 오른쪽 창에 **System(**시스템**)**에서 **Policy Analyzer and Optimizer(**정책 분석기 및 옵티마이저**)**를 선택합니다. 자세한 내용은 온프레미스 방화벽 Management Center 온보딩을 참조하십시오.

온프레미스 방화벽 Management Center 버전 7.6이 있고 정책 분석기 및 옵티마이저를 사용하려는 경우 아래 단계를 따르십시오.

프로시저

단계 **1** 온프레미스 방화벽 Management Center에서 **Integration(**통합**)** > **Cisco Security Cloud**로 이동합니다.

단계 **2** 온프레미스 방화벽 Management Center를 Cisco Security Cloud 와 통합하지 않은 경우 **Cisco Security Cloud** 활성화를 클릭하고 단계를 수행합니다. 클라우드 통합을 인증하려면 기존 Security Cloud Control 테넌트를 선택하거나 새 테넌트를 프로비저닝해야 합니다. 클라우드 통합이 성공한 후 온프레미스 방화벽 Management Center가 온보딩됩니다.

단계 **3** 온프레미스 방화벽 Management Center을 Cisco Security Cloud 와 통합한 후 **Enable Policy Analyzer and Optimizer(**정책 분석기 및 옵티마이저 활성화**)** 체크 박스를 선택하고 **Save(**저장**)**를 클릭합니다.

단계 **4** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동합니다.

단계 **5** 정책을 선택하고 **Analyze Policy(**정책 적용**)**를 클릭합니다. **Anomaly(**변칙**)** 열에 **In Progress(**진행 중**)**가 표시되고 분석이 완료되면 변칙의 수와 정책을 최적화할 수 있는 비율이 표시됩니다.

단계 **6** 비율을 클릭하면 온프레미스 방화벽 Management Center이 등록된 Security Cloud Control 테넌트의 **Policy Analyzer and Optimizer(**정책 분석기 및 옵티 마이저**)** 페이지로 교차 실행됩니다.

정책 분석

클라우드 제공 Firewall Management Center를 프로비저닝하거나 온프레미스 방화벽 Management Center를 Security Cloud Control 테넌트에 온보딩하고 정책을 생성한 후 정책 분석기 및 옵티마이저를 사용하여 분석을 시작할 수 있습니다. 자세한 내용은 온프레미스 방화벽 Management Center 온보딩 및 Security Cloud Control 테넌트에서 클라우드 제공 Firewall Management Center 활성화를 참조하십시오.

이 섹션에서는 정책을 분석할 수 있는 다양한 방법을 설명합니다.

클라우드 제공 **Firewall Management Center** 정책 분석

클라우드 제공 Firewall Management Center가 Security Cloud Control 테넌트에 이미 프로비저닝되어 있는 경우 정책 분석을 즉시 시작할 수 있습니다. Security Cloud Control에서 클라우드 제공 Firewall Management Center를 프로비저닝하려면 Security Cloud Control에서 클라우드 제공 Firewall Management Center 활성화를 참조하십시오.

참고 새 정책을 생성하면 정책 분석기 및 옵티마이저가 정책 세부 정보를 가져와서 **Policy Analyzer and Optimizer(**정책 분석기 및 옵티마이저**)**에 표시되기까지 데 다소 시간이 걸릴 수 있습니다. 새로 고침 ( ) 버튼을 클릭하여 페이지를 수동으로 새로 고침하여 새 정책을 확인합니다.

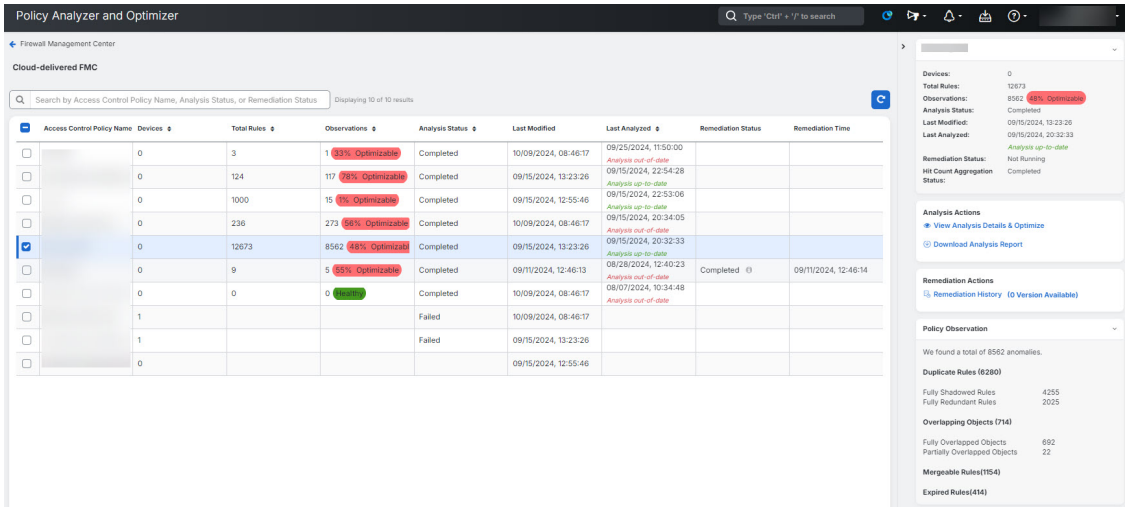
프로시저

단계 **1** **Administration(**관리**)** > **Integration(**통합**)** > **Firewall Management Center**로 이동 - 클라우드제공 사용 **FMC**가 기본적으로 선택되어 있는 **Services(**서비스**)** 페이지가 나타납니다.

단계 **2** 오른쪽 창 **System(**시스템**)** 아래에서 **Policy Analyzer and Optimizer(**정책 분석기 및 옵티마이저**)**를 클릭합니다.

왼쪽 창에서 **Monitor(**모니터링**)** > **Insights & Reports(**인사이트 및 보고서**)** > **AIOps Insights(**인사이트**)** > **Policy Analyzer and Optimizer(**정책 분석기 및 옵티마이저**)**를 선택합니다. 왼쪽 상단 모서리의 **Showing policy for(**정책 표시 대상**)** 옵션에는 표시되는 디바이스의 정책이 표시됩니다. 클릭하여 클라우드 제공 Firewall Management Center 및 기타 온프레미스 방화벽 Management Center간에 전환할 수 있습니다.

단계 **3** 분석된 정책의 경우 정책 분석기 및 옵티마이저는 분석의 개요를 제공하며 여기에는 **Total Rules(**전체 규칙**)**, **Observations(**관찰**)**, **Anaysis Status(**분석 상태**)**, **Last Modified(**마지막 수정**)** 및 **Last Analyzed(**마지막 분석**)** 타임스탬프가 포함됩니다. 정책을 선택하면 오른쪽 창에서 추가 세부 정보를 확인할 수도 있습니다.



단계 **4** 분석 세부 정보를 보거나 재분석할 정책을 선택합니다.

정책 분석기 및 옵티마이저은 24시간마다 모든 정책을 자동으로 분석하며, 모든 정책이 이미 분석되어 세부 정보를 검토할 준비가 되어 있을 가능성이 높습니다.

단계 **5** 다른 분석을 수동으로 트리거하려면 **Re-analyze Policy(**정책 다시 분석**)**를 클릭합니다.

온프레미스 방화벽 **Management Center** 정책 분석

온프레미스 방화벽 Management Center 버전 7.2 이상에서 정책 분석기 및 옵티마이저을 사용하여 정책을 분석하려면 **Cisco Security Cloud** 에서 자동 검색 또는 온보딩 방법으로 **Use Credentials(**자격증명 사용**)**을 사용하여 Security Cloud Control에 온보딩해야 합니다. 온프레미스 방화벽 Management Center 버전 7.6의 경우 Cisco Security Cloud에 통합해야 합니다. 그러면 온프레미스 방화벽 Management Center가 Security Cloud Control 테넌트에 온보딩됩니다. 시작하기 전에 다음을 수행합니다.

- 온프레미스 방화벽 Management Center를 온보딩한 후 **Administration(**관리**)** > **Integration(**통합**)** > **Firewall Management Center**에서 **Active(**활성**)** 상태인지 확인합니다.
- Cisco Security Cloud와 통합한 후, **Integration(**통합**)** > **Cisco Security Cloud**로 이동하여 **Enable Policy Analysis & Optimization(**정책 분석 및 최적화 활성화**)** 체크 박스를 선택합니다.
- 온프레미스 방화벽 Management Center를 방금 온보딩했거나 이미 온보딩된 온프레미스 방화벽 Management Center에서 새 정책을 생성하거나 가져온 경우, 정책 분석기 및 옵티마이저가 정책을 가져올 때까지 기다립니다.
- 정책 분석은 수동으로 실행할 수도 있고, 예약된 자동 분석의 일부로 자동 실행될 수도 있습니다.

프로시저

단계 **1** **Administration(**관리**)** > **Integration(**통합**)** > **Firewall Management Center**로 이동 - 클라우드제공 사용 **FMC**가 기본적으로 선택되어 있는 **Services(**서비스**)** 페이지가 나타납니다.

단계 **2** 분석할 정책이 있는 온프레미스 방화벽 Management Center를 선택합니다.

단계 **3** 오른쪽 창 **System(**시스템**)** 아래에서 **Policy Analyzer and Optimizer(**정책 분석기 및 옵티마이저**)**를 클릭합니다.

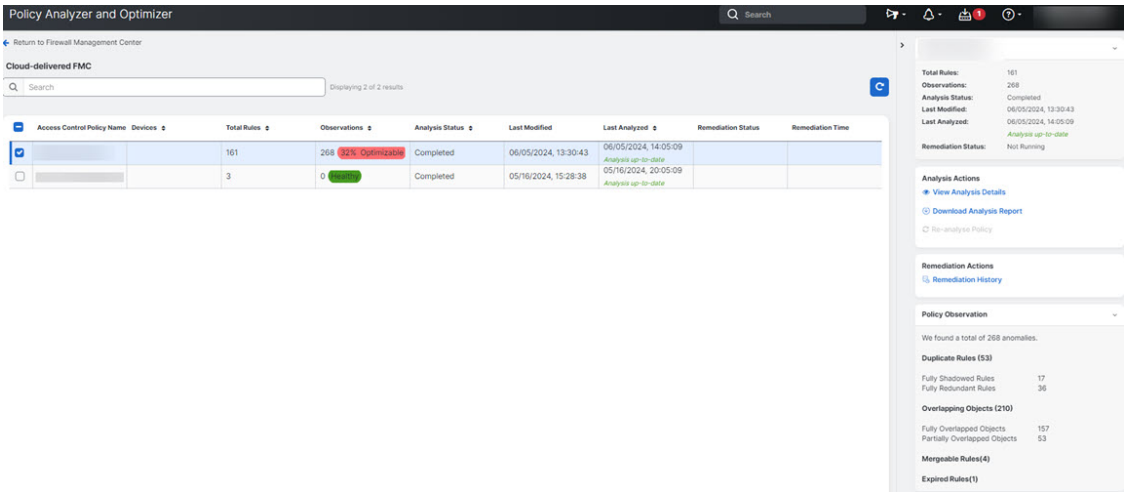
왼쪽 창에서 **Monitor(**모니터링**)** > **Insights & Reports(**인사이트 및 보고서**)** > **AIOps Insights(**인사이트**)** > **Policy Analyzer and Optimizer(**정책 분석기 및 옵티마이저**)**를 선택합니다. 왼쪽 상단 모서리의 **Showing policy for(**정책 표시 대상**)** 옵션에는 표시되는 디바이스의 정책이 표시됩니다. 클릭하여 클라우드 제공 Firewall Management Center 및 기타 온프레미스 방화벽 Management Center간에 전환할 수 있습니다.

참고
온프레미스 방화벽 Management Center 인터페이스에서 정책 분석을 트리거할 수도 있습니다. 자세한 내용은 Security Cloud Control 매니지드 온프레미스 방화벽 Management Center에 대해 정책 분석기 및 옵티마이저 활성화, 4 페이지를 참조하십시오.

단계 **4** 분석된 정책의 경우 정책 분석기 및 옵티마이저는 분석의 개요를 제공하며 여기에는 **Total Rules(**전체 규칙**)**, **Observations(**관찰**)**, **Anaysis Status(**분석 상태**)**, **Last Modified(**마지막 수정**)** 및 **Last Analyzed(**마지막 분석**)** 타임스탬프가 포함됩니다. 정책을 선택하면 오른쪽 창에서 추가 세부 정보를 확인할 수도 있습니다.

정책 보고

정책이 분석되고 준비되면 **Policy Analyzer and Optimizer(**정책 분석기 및 옵티마이저**)** 페이지에서 **Analysis Status(**분석 상태**)**가 **Completed(**완료**)**이고 **Observations(**관찰**)** 열에 정책이 정상 상태이거나 최적화할 수 있는 경우 표시됩니다.

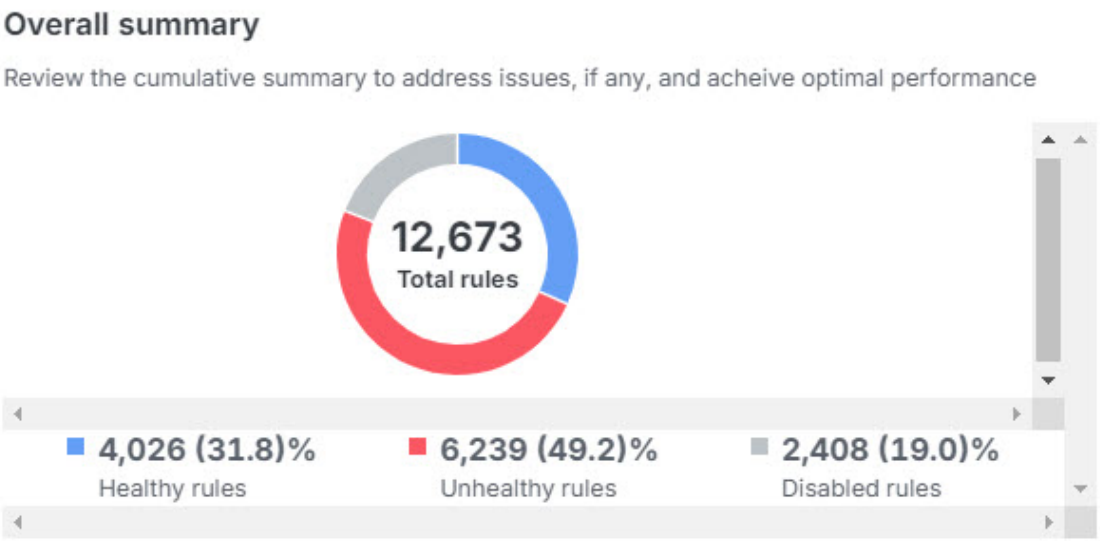


오른쪽 창에 분석에 대한 세부 정보를 보려면 정책을 선택합니다. **View Analysis Details(**분석 세부 정보 보기**)**, **Download Analysis Report Download(**분석 보고서 다운로드**)**, **Remediation History(**교정 기록**)** 보기 등의 작업을 수행할 수 있습니다.

정책 분석 요약

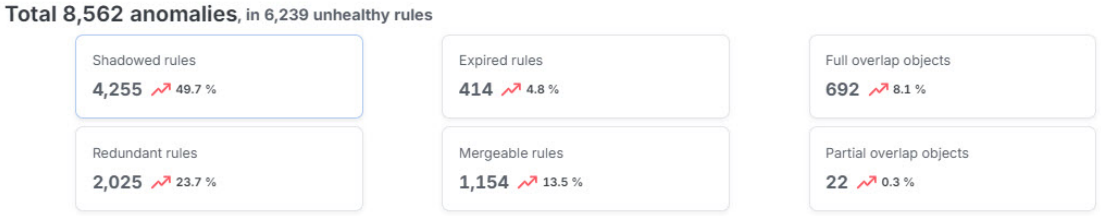
Summary(요약**)** 탭에는 pie chart와 막대 그래프로 표시되는 다음 규칙 정보가 포함되어 있습니다.

Overall summary(전체 요약**)** - pie chart를 사용하여 정상, 비활성화, 만료 및 변칙을 포함하는 규칙의 수에 대한 인사이트를 제공합니다. pie의 일부로 마우스를 가져가면 규칙의 백분율을 볼 수 있습니다.

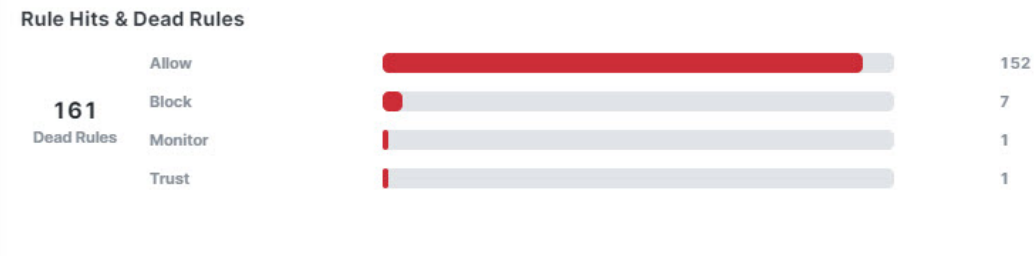


Rule usage history(규칙 사용 기록**)** - 규칙 사용의 최신성에 대한 인사이트를 기간별로 제공합니다.

Rules with Anomalies(변칙이 있는 규칙**)** - 변칙이 있는 규칙 수에 대한 인사이트를 막대 그래프로 제공합니다. 막대 위에 마우스를 올려놓으면 변칙이 있는 규칙의 수를 확인할 수 있습니다.



Hits rules & dead rules(적중 규칙 및 사용 불능 규칙**)** - 허용, 차단, 모니터링 및 신뢰를 비롯한 규칙 유형별로 만료된 규칙의 적중 횟수에 대한 인사이트를 제공합니다.



중복 규칙

Duplicate Rules(중복 규칙**)** 탭에 변칙이 있는 섀도잉 및 중복 규칙이 나열됩니다.

- **Fully Shadowed Rule(**완전하게 섀도잉된 규칙**)**은 그 앞에 위치한 다른 규칙이 이 규칙을 가리기 때문에 네트워크 트래픽을 절대 평가하지 않는 규칙입니다.
- **Fully Redundant Rule(**완전 중복 규칙**)**은 더 큰 또 다른 규칙의 일부인 규칙으로, 이 중복 규칙을 제거해도 네트워크 트래픽에 영향을 주지 않습니다. 이 규칙에서 수행해야 하는 트래픽 평가를 다른 규칙에서 이미 수행되기 때문입니다.

모든 완전하게 섀도잉된 규칙 또는 완전 이중화 이중화된 규칙을 비활성화하거나 삭제하도록 선택할 수 있습니다.

참고 각 관찰 항목을 확장하면 상위 규칙으로 인해 중복되는 규칙 목록을 확인할 수 있습니다. 목록의 각 규칙은 속성 집합과 함께 표시됩니다. 규칙과 함께 표시할 규칙 속성을 선택하려면 오른쪽 상단의 설정 버튼을 클릭합니다.

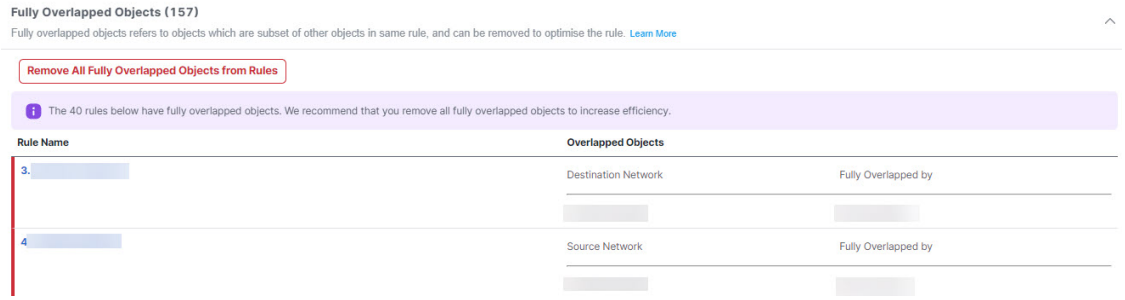
섀도우 규칙 또는 중복 규칙을 비활성화한 후에도 변경 사항을 적용하기 전에 작업을 **Undo(**실행 취소**)** 할 수 있습니다. 규칙의 영향을 측정하려면 먼저 규칙을 비활성화한 후 삭제하는 것이 좋습니다. 나중에 삭제하면 규칙이 영구적으로 삭제되기 때문입니다.

규칙이 있는 클라우드 제공 Firewall Management Center 또는 온프레미스 방화벽 Management Center로 이동하여 언제든지 비활성화된 규칙을 활성화할 수 있습니다.

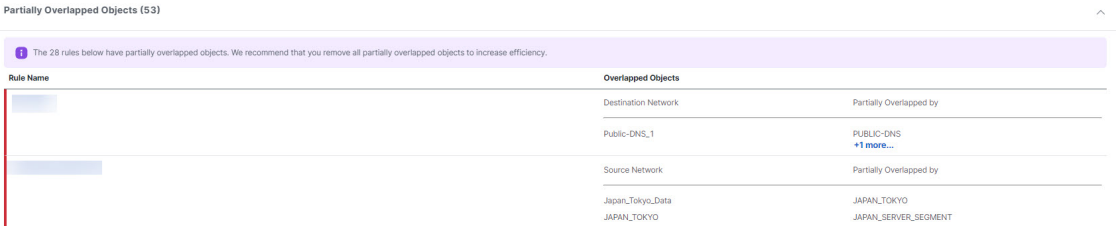
중복 개체

Overlapping Objects(중복 개체**)** 탭은 완전히 중복되거나(IP 주소 또는 포트 번호가 동일하거나 완전한 하위 집합) 부분적으로 중복되는 개체(IP 주소의 일부 하위 집합은 반복되지만 전체 하위 집합은 반복되지 않음)를 나열합니다.

예를 들어 규칙에 192.168.1.1의 개체와 192.168.1.0/24에 대한 개체가 포함된 경우, 192.168.1.1 개체는 다른 개체에 의해 완전히 중복되며 규칙에서 필요하지 않습니다. **Remove All Fully Overlapped Objects from Rules(**규칙에서 완전히 중복되는 개체 제거**)** 옵션을 클릭할 수 있습니다.



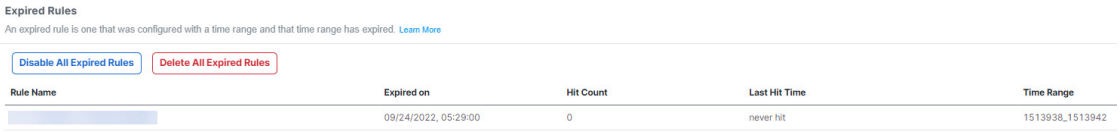
부분적 중복의 경우 각 어커런스를 평가하고, 변경이 가능한지 결정하고, 개체를 편집하여 해당 변경 사항을 직접 구현해야 합니다.



만료된 규칙

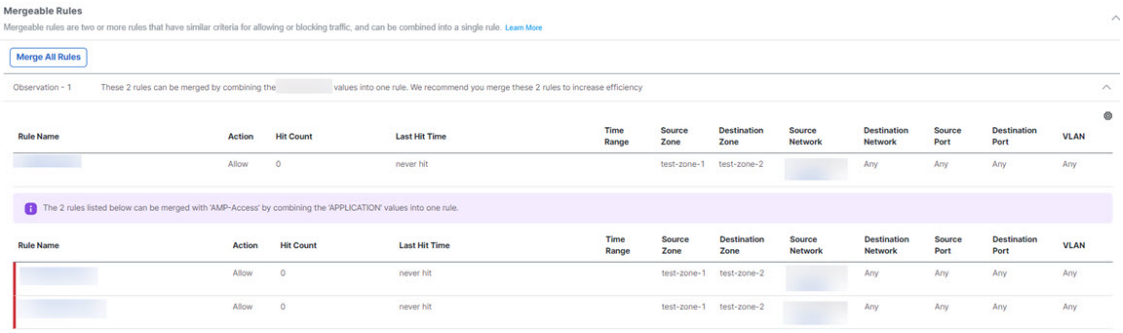
Expired Rules(만료된 규칙**)** 탭에는 기간이 설정되었으나 해당 기간이 만료된 규칙이 나열됩니다. 규칙이 만료된 날짜, 적중 횟수, 마지막 적중 시간 및 시간 범위와 같은 규칙 정보도 확인할 수 있습니다.

Disable All Expired Rules(모든 만료된 규칙 비활성화**)** 또는 **Delete All Expired Rules(**만료된 모든 규칙 삭제**)**를 선택할 수 있습니다.



병합 가능한 규칙

Mergeable Rules(병합 가능한 규칙**)** 탭에는 허용 및 차단 설정이 유사하고 단일 규칙으로 병합할 수 있는 규칙이 나열됩니다. 관찰을 읽고 한번에 **Merge All Rules(**모든 규칙 병합**)**를 클릭하여 해당 규칙의 개체를 병합하여 관리하는 규칙 수를 줄일 수 있습니다.



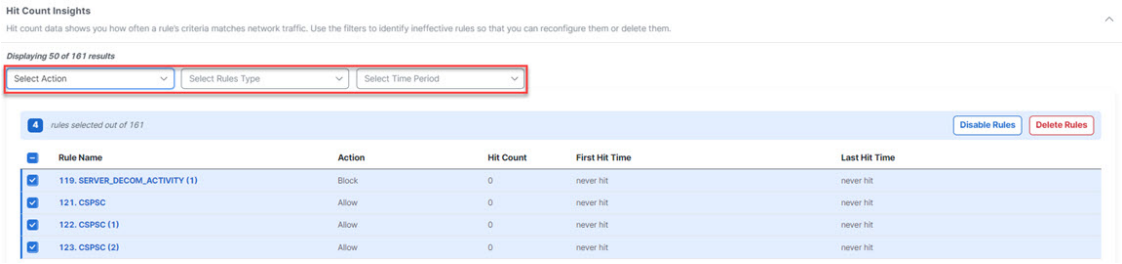
참고 두 규칙을 병합할 때, 첫 번째 규칙의 로깅 설정이 병합 대상 규칙에 적용됩니다. 따라서 병합된 규칙의 로깅 동작은 첫 번째 규칙에 구성된 설정을 따르며, 다른 규칙의 고유한 로깅 구성을 덮어쓰게 됩니다.

정책 인사이트

Policy Insights(정책 인사이트**)** 탭에는 트리거되지 않은 규칙(**Never Hit Rules(**적중되지 않음 규칙**)**이 처음에 나열되는 **Hit Count(**적중 횟수**)** 섹션이 있습니다. 적중 횟수 정보는 정책에 할당된 모든 디바이스에서 가져옵니다. 기준을 변경하고 다른 적중 횟수 정보(예: 지난 6개월 동안의 적중하지 않은 규칙) 또는 선택한 기간의 적중 규칙을 확인할 수 있습니다. 규칙에 설정된 작업, 적중 정보 및 기간을 사용하여 규칙을 필터링할 수 있습니다.

- **Never Hit Rules(**적중된 적 없는 규칙**)** - 생성 당시부터 적중되지 않은 규칙.
- **Hit Rules(**적중 규칙**)** - 선택한 기간에 적중된 규칙.
- **Not Hit Rules(**적중하지 않은 규칙**)** - 선택한 기간 동안 적중되지 않은 규칙.

비활성화하거나 삭제할 규칙을 선택하고 **Disable Rules(**규칙 비활성화**)** 또는 **Delete Rules(**규칙 삭제를 클릭합니다. 먼저 규칙을 비활성화하여 비활성화가 미치는 영향을 측정한 다음 삭제하는 것이 좋습니다.



정책 교정

분석 요약에서 변칙이 있는 규칙을 삭제하거나 비활성화하도록 선택하는 경우, 정책 분석기 및 옵티마이저는 해당 변경 사항을 즉시 적용하지 않습니다. 원하는 변경 사항은 스테이징되며 **Apply Remediation(**교정 적용**)**을 클릭하는 경우에만 적용됩니다.

Apply Remediation(교정 적용**)**을 한 번 클릭하면 동일한 보고서를 기반으로 교정을 다시 적용할 수 없습니다. 정책 설정에서 정책 분석을 다시 실행하고 새 보고서를 사용하여 변칙 항목을 해결해야 합니다.

정책 교정 적용

시작하기 전에

- 교정을 적용하기 전에 모든 정책을 백업해야 합니다.
- 적용될 수 있도록 준비된 몇 가지 정책 교정을 확인합니다. 준비된 변경 사항이 없는 경우 **Apply Remediation(**교정 적용**)** 버튼이 비활성화됩니다.

- 적용 중인 정책 버전을 확인할 수 있도록 오른쪽 상단에서 **Policy Last Modified(**마지막으로 수정한 정책**)**, **Policy Last Analyzed(**마지막으로 분석된 정책**)** 날짜 및 타임스탬프, 교정하도록 표시한 규칙 수를 확인해야 합니다.

프로시저

단계 **1** **Policy Analyzer and Optimizer(**정책 분석기 및 옵티마이저**)** 페이지에서 **Apply Remediation(**교정 적용**)**을 클릭합니다.

단계 **2** 적용할 모든 교정의 요지가 포함된 확인 팝업을 자세히 읽고 교정을 원하지 않는 정책에 교정을 적용하고 있지 않은지 확인합니다.

단계 **3** **Apply(**적용**)**를 클릭합니다.

참고
Apply(적용**)**를 클릭하면 **Remediations are are deployed(**교정 구축 중**)** 및 **The policy is locked for remediation(**정책이 교정을 위해 잠김**)**과 같은 팝업 메시지가 표시됩니다.

단계 **4** 교정이 성공적으로 완료되면, **Download Optimization Report(**최적화 보고서 다운로드**)**를 클릭합니다.

교정이 적용될 때 방금 정책을 수정했으므로, 다른 분석 요약을 얻으려면 새로 수정된 정책 집합을 다시 분석해야 합니다. 이 요약을 사용하여 남은 정책 변칙을 교정할 수 있습니다.

교정 보고서에는 적용된 모든 교정 및 적용된 규칙의 통합 데이터가 포함됩니다. **Policy Analyzer and Optimizer(**정책 분석기 및 옵티마이저**)** 페이지에서 정책을 선택하면 오른쪽 창에서 교정 날짜 및 시간, 교정을 시작한 사용자 및 교정 상태에 대한 데이터를 포함하는 **Remediation History(**교정 기록**)**를 볼 수 있습니다. 동일한 팝업에서 교정 보고서를 다운로드할 수도 있습니다.

교정은 모두 기록되며 **Remediation History(**교정 기록**)**에서 교정 날짜 및 시간, 교정을 수행한 사용자 등의 정보와 함께 볼 수 있습니다.

참고
관리 워크플로우가 활성화된 온프레미스 방화벽 Management Center의 경우 정책 교정이 적용되면 내부 워크플로우 티켓이 생성되고 변경 사항이 준비됩니다. 변경 사항은 티켓이 제출되거나 승인될 때만 적용됩니다. *Cisco Secure Firewall Management Center* 관리 가이드에서 변경 관리를 참고하십시오.

정책 교정 보고서에는 어떤 내용이 포함되나요?

정책 교정 보고서는 완료된 교정의 모든 부분을 통합하며 PDF로 다운로드할 수 있습니다. 이 보고서에는 정책에 대해 수행한 교정을 기반으로 하는 다음 섹션이 포함되어 있습니다. 각 섹션은 규칙 이름, 취한 교정 작업 및 모든 관련 코멘트에 대한 정보를 전달합니다. 예를 들어 중복 규칙을 교정하지 않은 경우 보고서에 중복 규칙 교정과 관련된 섹션이 포함되지 않습니다.

- 교정 요약
- 적중 횟수 교정

- 만료된 규칙 교정
- 중복 규칙 교정
- 병합 가능한 규칙 교정

참고 정책이 정책 분석기 및 옵티마이저에 의해 교정되었는지 확인하려면 **Policies(**정책**)** > **Access Policies(**액세스 정책**)**로 이동하여 **Policy Editor(**정책 편집기**)**에서 규칙을 확인하도록 정책을 편집합니다. 정책 분석기 및 옵티마이저에 의해 정책이 교정되면 최적화된 규칙에 코멘트가 추가됩니다. 또한 "updated by 정책 분석기 및 옵티마이저"를 사용하여 정책 분석기 및 옵티마이저에 의해 최적화된 모든 규칙을 필터링하여 정책 분석기 및 옵티마이저에 의해 교정된 모든 규칙을 볼 수 있습니다.

정책 분석기 및 옵티마이저 문제 해결

정책 분석기 및 옵티마이저와 관련된 문제를 문제를 해결 하려면 다음 섹션을 읽어보십시오.

Policy Analyzer and Optimizer가 정책을 분석하지 않음

Analyze Policy(정책 분석**)**를 클릭했음에도 불구하고 정책 분석기 및 옵티마이저에서 정책을 분석하지 않는 경우 다음을 시도합니다.

프로시저

단계 **1** **Administration(**관리**)** > **Integration(**통합**)** > **Firewall Management Center**로 이동합니다.

단계 **2** 정책 분석이 발생하지 않는 온프레미스 방화벽 Management Center 또는 클라우드 제공 **FMC**를 선택하고 오른쪽 창 **Actions(**작업**)**에서 **Workflows(**워크플로우**)**를 선택합니다.

단계 **3** 워크플로우의 **Current State(**현재 상태**)**가 **Error(**오류**)**로 표시되는 경우 워크플로우를 확장하고 **END STATE(**종료 상태**)**가 **ERROR(**오류**)**인 마지막 작업으로 스크롤합니다.

단계 **4** **RESULT(**결과**)** 아래의 **Error Message(**오류 메시지**)**를 클릭하여 자세한 오류 메시지를 확인하거나 **Stack Trace(**스택 추적**)**를 클릭하여 오류를 일으킨 발생한 일련의 예외를 확인합니다.

단계 **5** 오류를 해결하거나 Cisco TAC에 지원을 요청하십시오.

Policy Analyzer and Optimizer가 정책을 가져오지 않음

온프레미스 방화벽 Management Center의 정책이 Security Cloud Control의 정책 분석기 및 옵티마이저 페이지에 표시되지 않는 경우 다음을 수행합니다.

프로시저

단계 **1** 온프레미스 방화벽 Management Center에서 **Integration(**통합**)** > **Cisco Security Cloud**를 선택합니다.

단계 **2** **Enable Policy Analyzer and Optimizer(**정책 분석기 및 옵티마이저 활성화**)** 체크 박스가 선택되어 있는지 확인합니다.

단계 **3** (선택 사항) Security Cloud Control 테넌트의 왼쪽 탐색창에서 **Administration(**관리**)** > **Integration(**통합**)** > **Firewall Management Center**로 이동하여 온프레미스 방화벽 Management Center이 활성 상태이고 연결 가능한지 확인합니다.

Policy Analyzer and Optimizer에 대한 FAQ(자주 묻는 질문)

Cisco AI Assistant이 정책 분석기 및 옵티마이저를 사용하여 수동으로 수행하는 대신 정책을 분석하고 교정할 수 있습니까**?**

Cisco AI Assistant는 정책 분석기 및 옵티마이저와 협업하여 변칙이 있는 정책을 조사하고 사용자에게 알립니다. 그러나 AI Assistant는 정책을 자동으로 분석하고 교정할 수 없습니다.

정책 분석기 및 옵티마이저이 이미 분석된 정책에 대한 새 변경 사항을 탐지하고 동일한 정책에 대해 다시 분석을 실행할 수 있습니까**?**

정책 분석기 및 옵티마이저은 수동으로 트리거된 경우 또는 24시간 예약된 정책 분석 실행으로만 정책을 분석할 수 있습니다.

공유 정책의 경우 정책 분석기 및 옵티마이저이 개별 디바이스 기반 보고서를 제공합니까**?**

아니요. 정책 분석기 및 옵티마이저는 액세스 정책 분석 데이터를 기반으로만 보고서를 제공합니다.

온프레미스 방화벽 **Management Center** 사용자입니다**.** 정책 분석기 및 옵티마이저를 사용하려면 **Security Cloud Control** 기본 라이선스를 구매해야 합니까**?**

아니요. 정책 분석기 및 옵티마이저는 Cisco Security Cloud 통합 중에 기존 또는 새로 생성된 Security Cloud Control 테넌트의 일부로 제공됩니다.

Cisco Security Cloud와 온프레미스 방화벽 **Management Center**를 통합할 때 **Security Cloud Control** 테넌트를 프로비저닝했습니다**. Security Cloud Control**에서 정책 분석기 및 옵티마이저 이외의 어떤 다른 기능을 활용할 수 있습니까**?**

Security Cloud Control 테넌트의 정책 분석기 및 옵티마이저 기능만 활용할 수 있습니다. Security Cloud Control의 다른 기능을 사용하려면 Security Cloud Control 기본 라이선스 및 기타 디바이스별 라이선스를 구매해야 합니다.

변경 관리 워크플로우가 활성화되어 있고 승인받아야 할 보류 중인 변경 사항이 있는 정책이 있는 온프레미스 방화벽 **Management Center**의 경우에도 정책 분석기 및 옵티마이저가 여전히 교정을 해당 정책에 적용할 수 있습니까**?**

아니요. 정책이 사용을 위해 잠겨 있다는 오류로 인해 복구 작업이 방해받을 것입니다.

정책 분석기 및 옵티마이저이 정책에서 분석할 수 있는 최대 규칙 수가 있습니까**?**

제한은 없습니다. 정책 분석기 및 옵티마이저는 원하는 수의 정책 및 규칙을 분석할 수 있습니다. 그러나 정책에 규칙 수가 더 많은 경우에는 분석도 시간이 오래 걸립니다.

규칙 비활성화와 규칙 삭제의 차이점은 무엇입니까**?** 더 나은 옵션은 무엇입니까**?**

규칙을 삭제하면 디바이스 메모리에서 규칙이 완전히 제거됩니다. 그러나 규칙을 비활성화하면 해당 규칙이 디바이스 메모리에 백업으로 유지되며 디바이스에 구축되지 않습니다.

정책 교정이 부분적으로 수행된 데 실패하면 변경 사항이 정책 분석기 및 옵티마이저에 의해 자동으로 취소됩니까**?**

아니요. 이러한 경우 실패 알림 및 교정 보고서를 받게 됩니다. 보고서를 확인하여 절반만 진행된 교정에 의해 영향을 받은 규칙이 무엇인지 파악할 수 있습니다. 이후 변경 사항을 수동으로 되돌린 다음, 교정을 처음부터 다시 시작할 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.