IBM QRadar용 클라우드 보안 앱 구성

목차

소개

이 문서에서는 로그 분석을 위해 IBM QRadar를 사용하는 Cisco Cloud Security 앱을 구성하는 방법에 대해 설명합니다.

개요

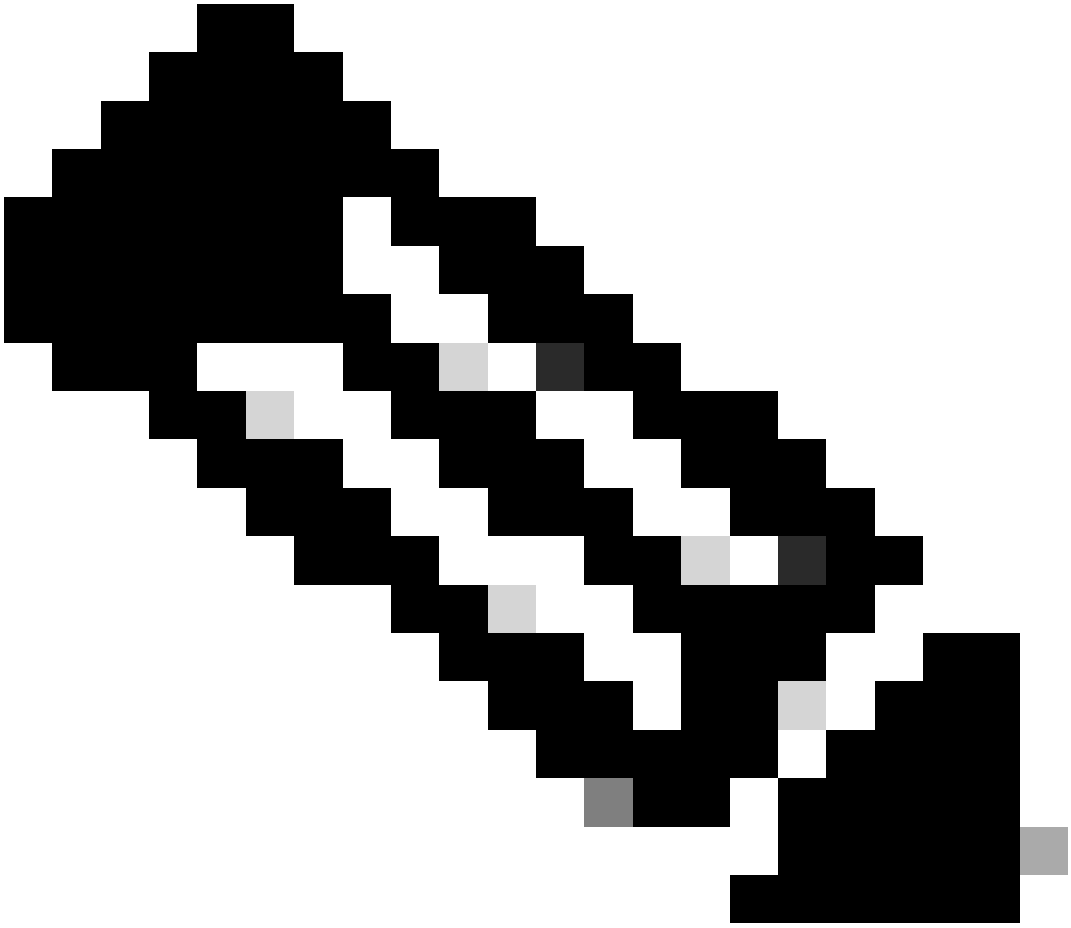
IBM의 QRadar는 로그 분석을 위해 널리 사용되는 SIEM입니다. Cisco Umbrella는 조직의 DNS 트래픽을 위해 Cisco Umbrella에서 제공하는 로그와 같은 대량의 데이터를 분석할 수 있는 강력한 인터페이스를 제공합니다. IBM QRadar용 Cisco Cloud Security App은 여러 보안 제품(Investigate, Enforcement, CloudLock)의 통찰력을 제공하고 QRadar와 통합합니다. 또한 사용자가 보안을 자동화하고 QRadar에서 직접 위협을 더 빠르게 억제할 수 있습니다.

QRadar용 Cisco Cloud Security 앱을 설치하면 Cisco Cloud Security 플랫폼의 모든 데이터가 통합되며 QRadar 콘솔에서 데이터를 그래픽 형태로 볼 수 있습니다. 분석가는 이 애플리케이션을 통해 다음을 수행할 수 있습니다.

- 도메인, IP 주소, 이메일 주소 조사
- 도메인 차단 및 차단 해제(적용)
- 네트워크의 모든 인시던트에 대한 정보를 봅니다.

이 문서에서는 QRadar가 S3 버킷에서 로그를 가져와 사용할 수 있도록 QRadar를 설정하고 실행하는 기본적인 방법에 대해 설명합니다.

요구 사항



참고: QRadar에 대한 지원은 IBM에서 제공되어야 합니다. Cisco에서는 타사 하드웨어 또는 소프트웨어를 직접 지원할 수 없기 때문입니다. Umbrella 대시보드를 S3 버킷에 연결하는 데 문제가 있을 경우 지원을 제공할 수 있습니다. 여기에서 대부분의 정보는 IBM 웹 사이트에서도 확인할 수 있습니다.
https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/c_dsm_guide_microsoft_Cisco_Umb

Cisco Umbrella 요건

이 문서에서는 Amazon AWS S3 버킷이 Umbrella(Settings(설정) > Log Management(로그 관리))에서 구성되었으며 최근 로그가 업로드된 상태에서 녹색으로 표시된다고 가정합니다.

이 기능을 구성하는 방법에 대한 자세한 내용은 여기: 로그 관리를 참조하십시오.

IBM Security QRadar SIEM 요구 사항

관리자는 QRadar 어플라이언스, Amazon S3 컨피그레이션 및 Umbrella 대시보드에 대한 관리 권한이 있어야 합니다. 이러한 지침에서는 QRadar 관리자가 LSX(Log source Extension) 파일을 생성

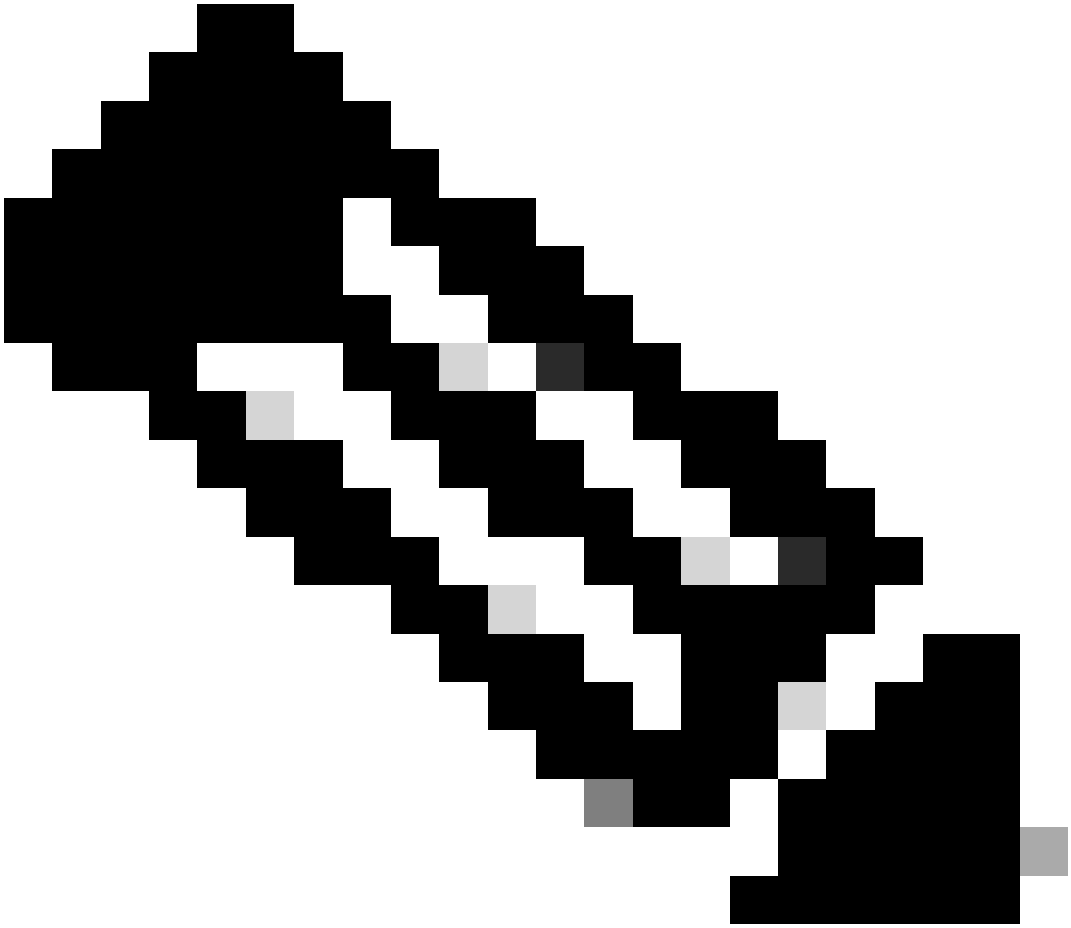
하는 데 익숙하다고 가정합니다.

Cisco Cloud Security App v1.0.3은 IBM QRadar 7.2.8까지만 작동합니다. 새 버전 v1.0.6은 7.4.2 이상에서 현재 QRadar 버전으로 작동합니다.

IBM QRadar용 Cisco Cloud Security 앱 설치

1. 다음 위치에서 IBM QRadar용 Cisco Cloud Security 앱을 다운로드하고 설치합니다. Cisco Cloud Security App v1.0.3(IBM QRadar v7.2.8의 경우) 또는 Cisco Cloud Security App v1.0.6(IBM QRadar v7.4.8의 경우)
2. 설치 후 QRadar에서 변경 사항을 배포합니다.

Cisco Cloud Security 앱 컨피그레이션: 로그 소스 추가

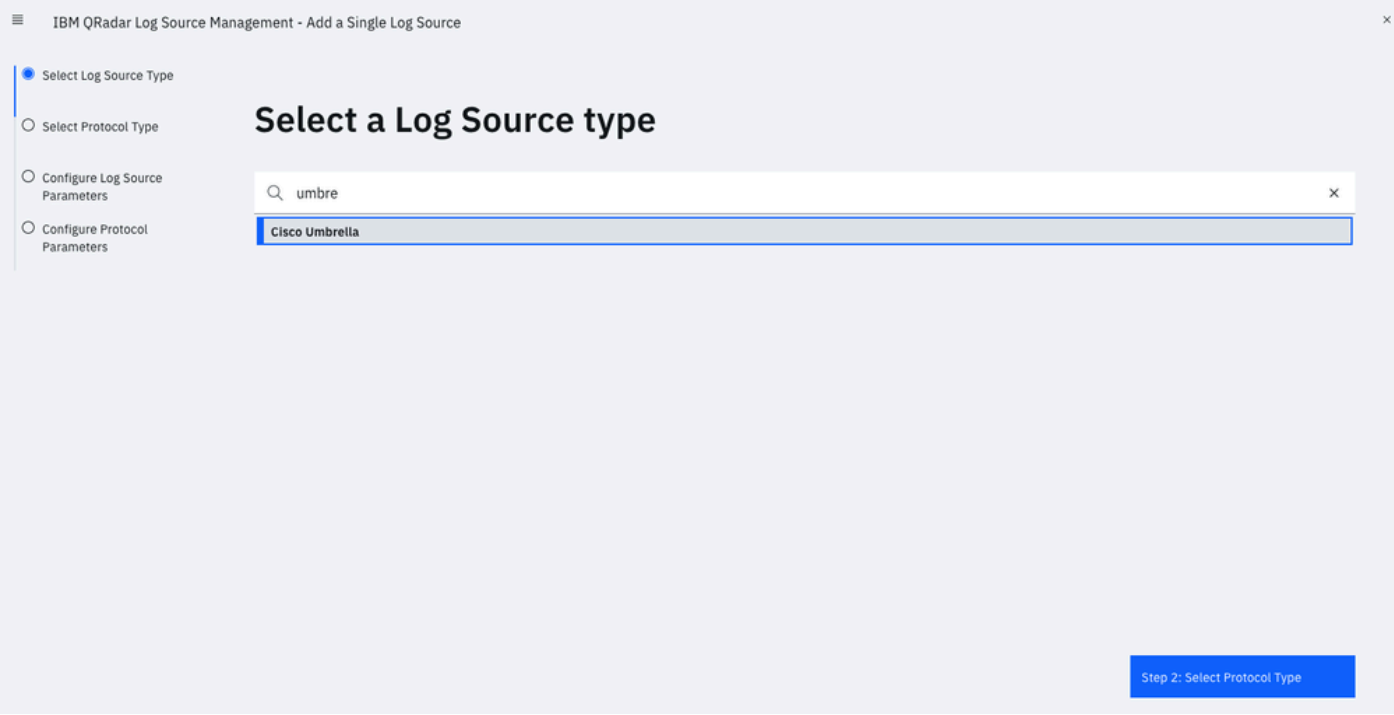


참고: S3에서 Audit 및 Firewall과 같은 다른 로그를 볼 수 있지만 지원되지 않습니다. 여기에 나열된 3개만 설정합니다. 이러한 다른 로그를 구성하려고 하면 오류가 발생합니다.

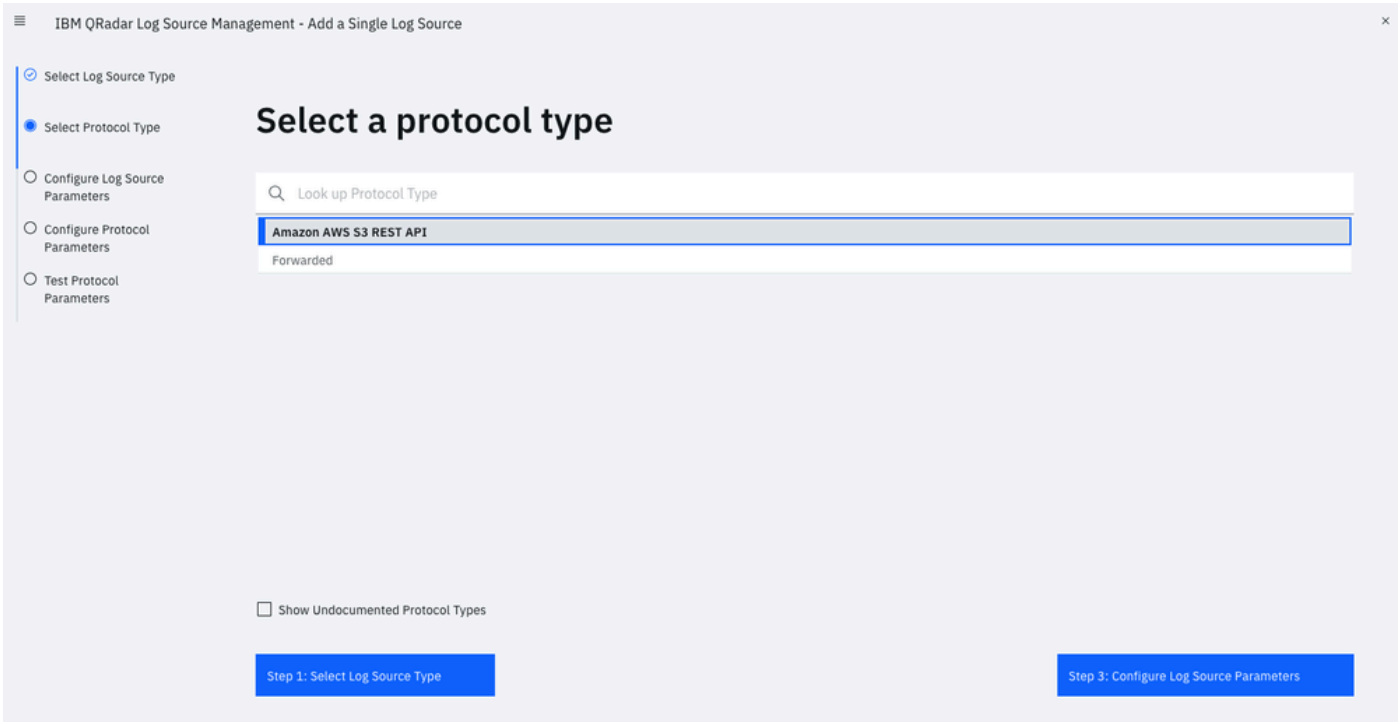
로그 소스를 추가하려면 QRadar 탐색 모음의 Admin(관리) 탭을 클릭하고 아래로 스크롤하여 QRadar Log Source Management(QRadar 로그 소스 관리)를 클릭한 다음 +New Log Source(새 로그 소스) 버튼을 클릭합니다.

- 로그 소스 이름(항목 이름은 나열된 것과 정확히 일치해야 함):
  - Cisco DNS 로그: cisco_umbrella_dns_logs
  - Cisco Umbrella IP 로그 cisco_umbrella_ip_logs
  - Cisco Umbrella Proxy 로그: cisco_umbrella_proxy_logs
- 이벤트 형식: Cisco Umbrella CSV
- 로그 원본 유형: Cisco Umbrella
- 프로토콜 구성: Amazon AWS S3 REST API
- 파일 패턴: .*?\.csv\.gz
- 로그 원본 확장: CiscoUmbrella_ext **
- 이 로그 원본을 구성원으로 설정할 그룹을 선택하십시오. cisco_umbrella_logsource_group

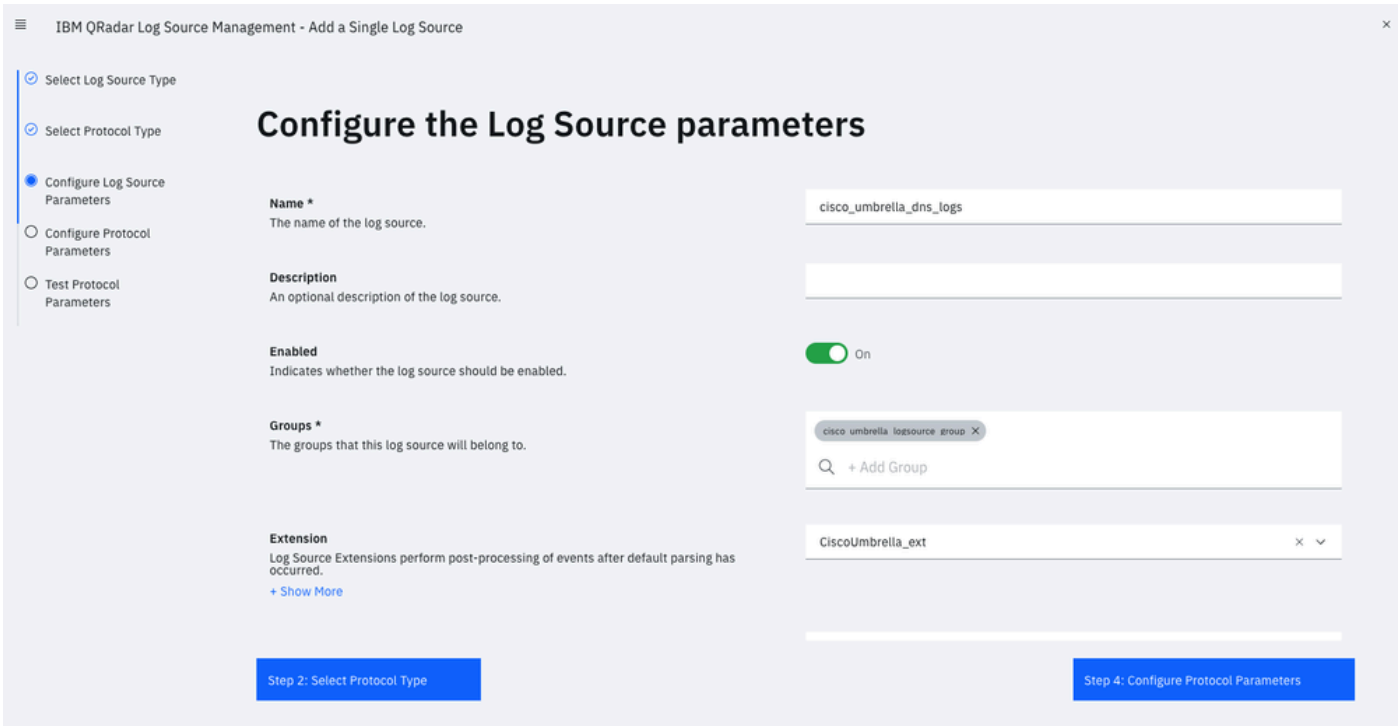
Add a Single Log Source(단일 로그 소스 추가) 마법사를 진행합니다.



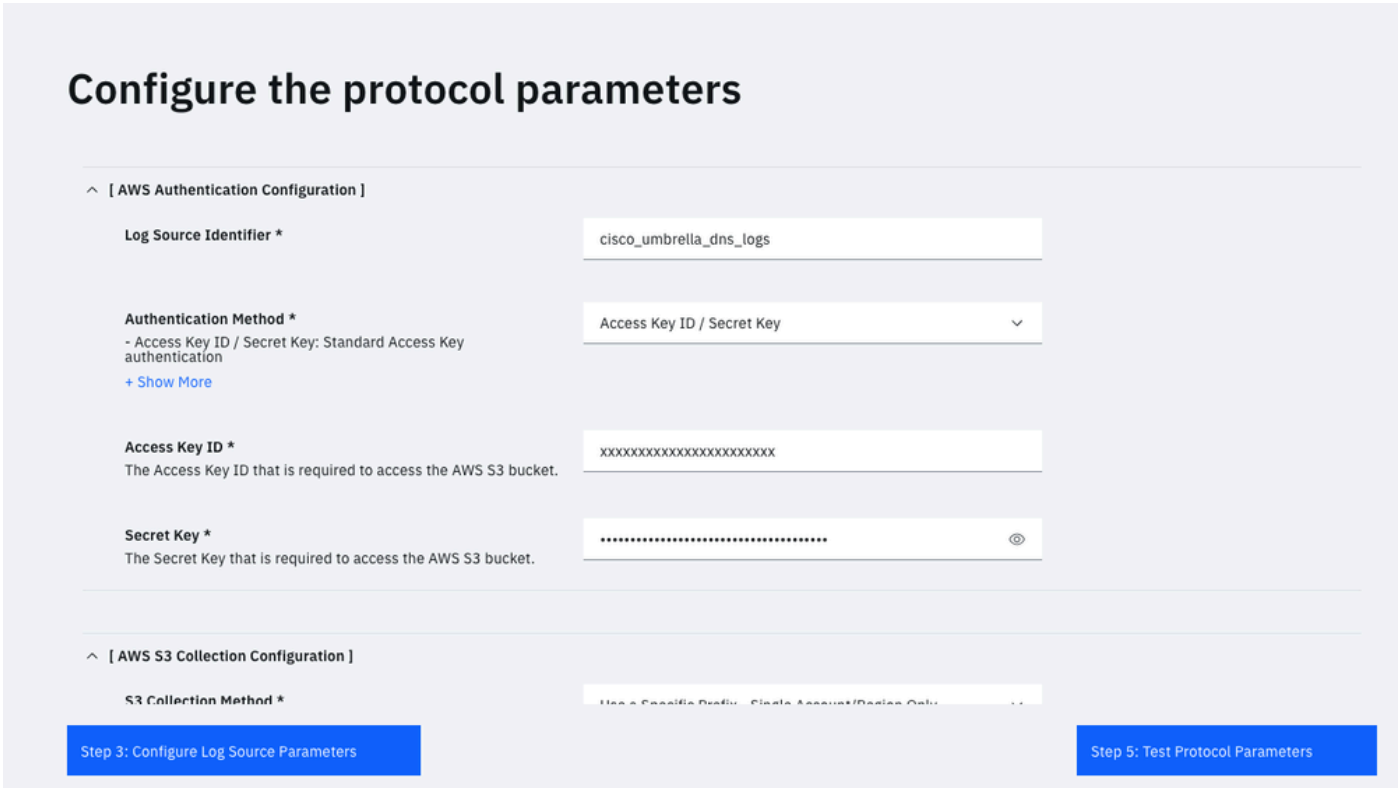
4404306773524



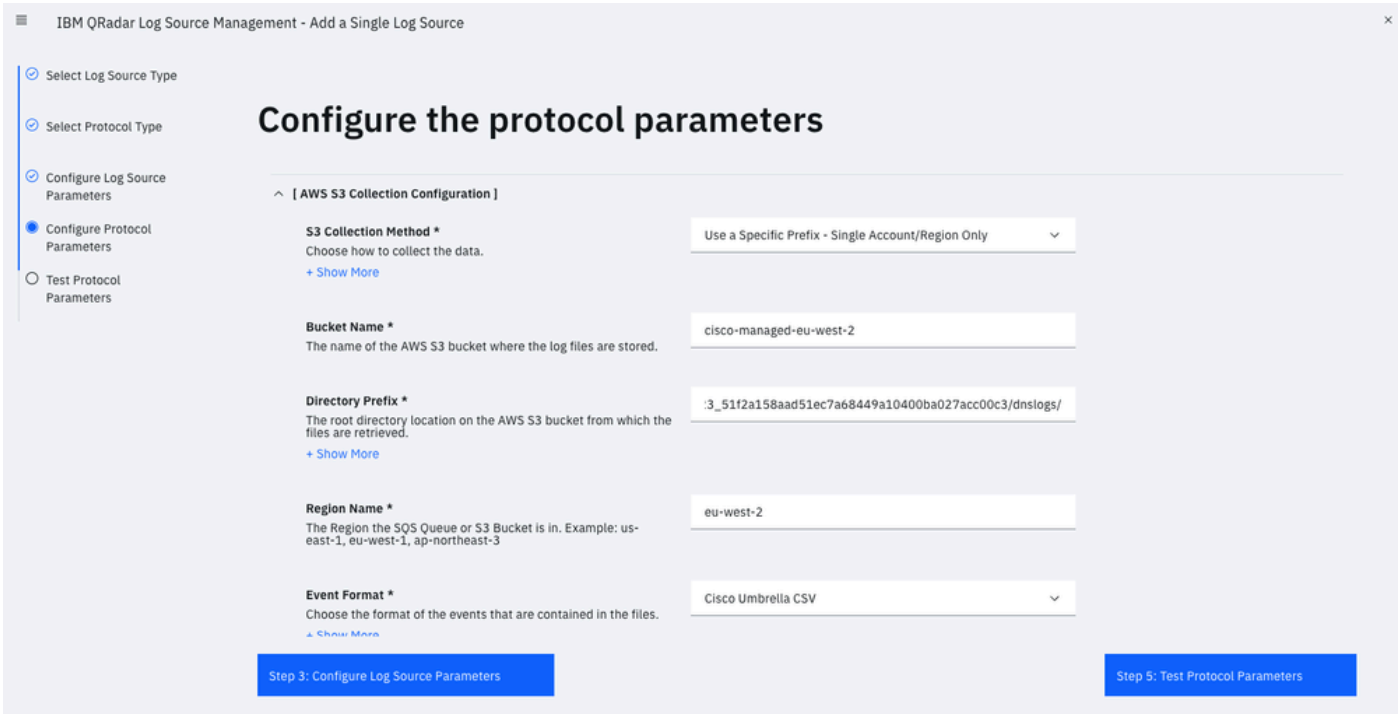
4404306773268



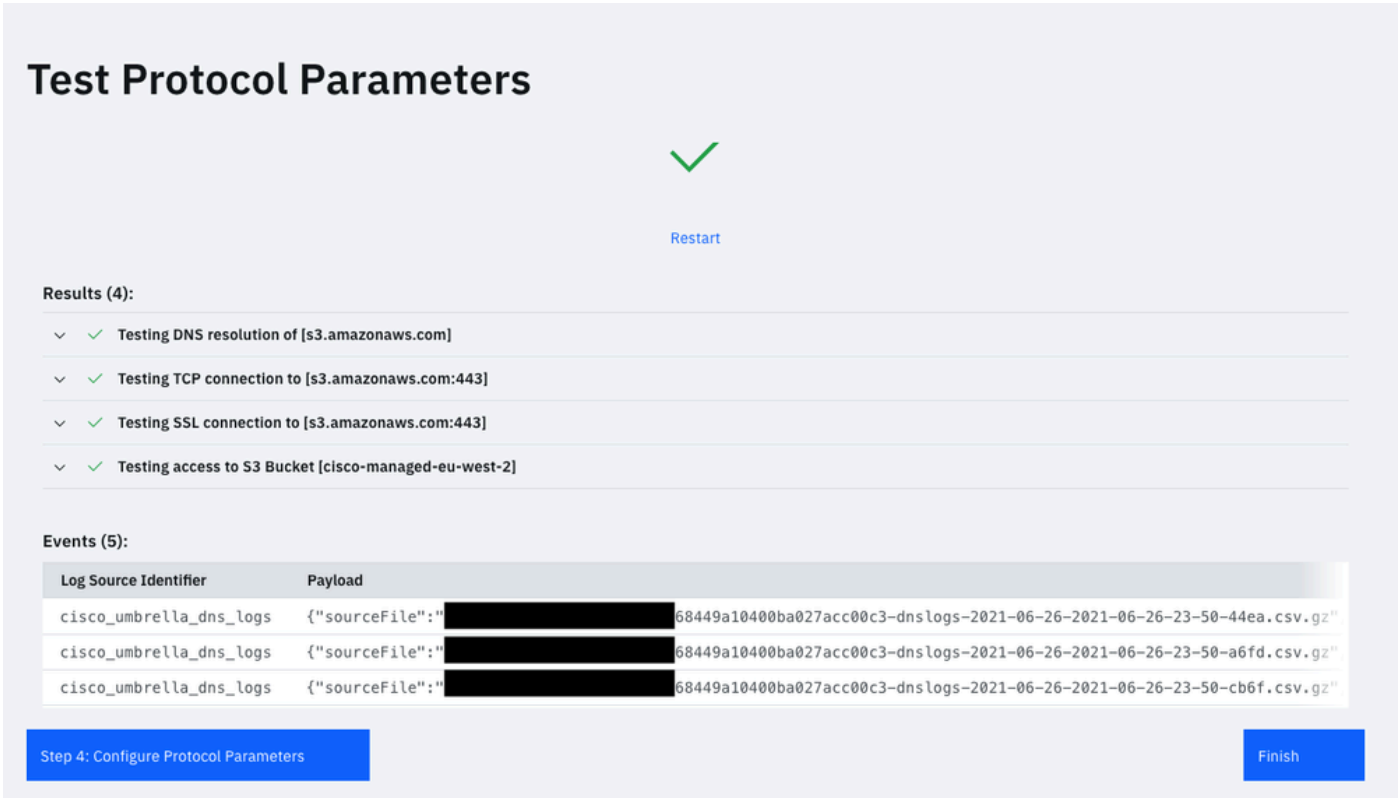
4404313505300



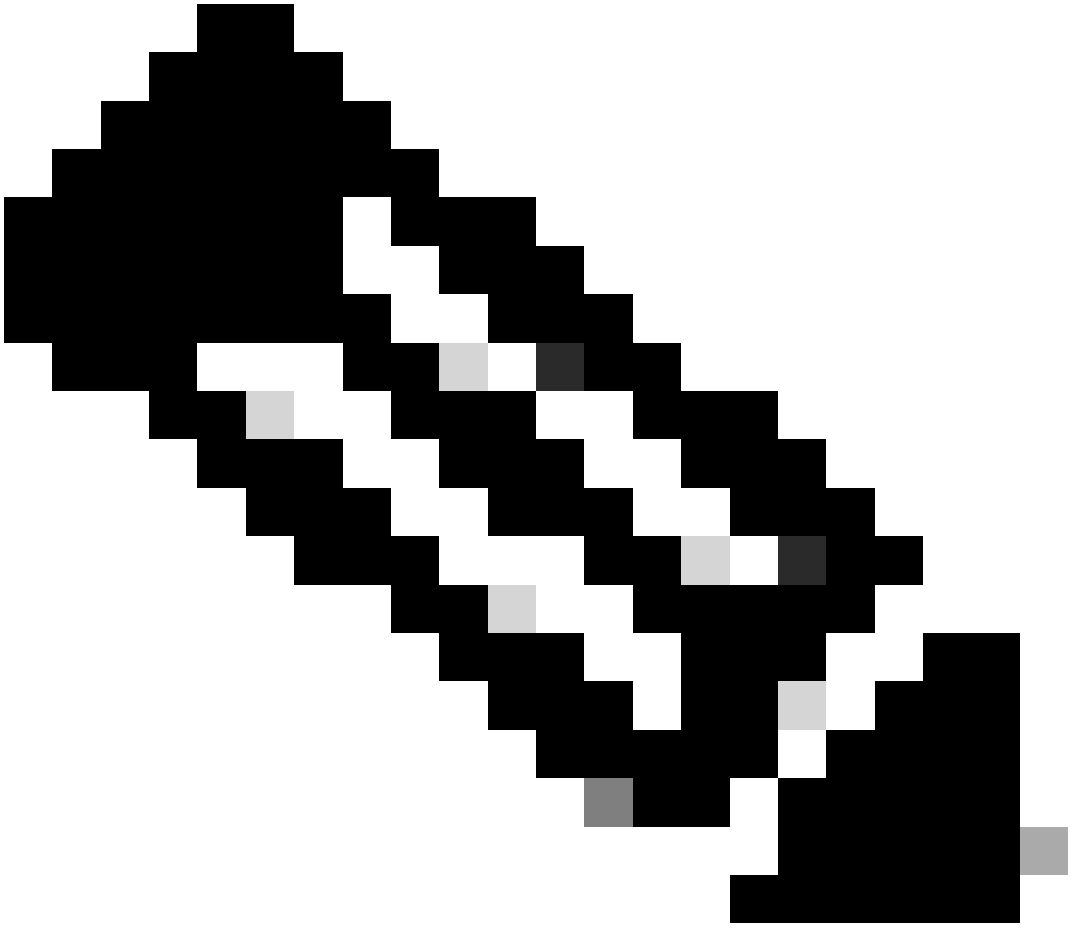
4404306774164



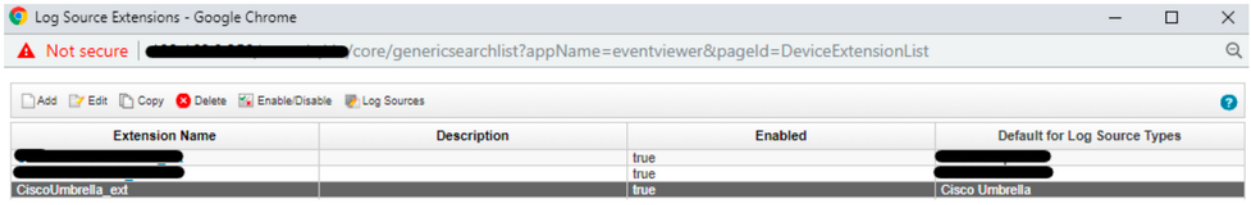
4404306897556



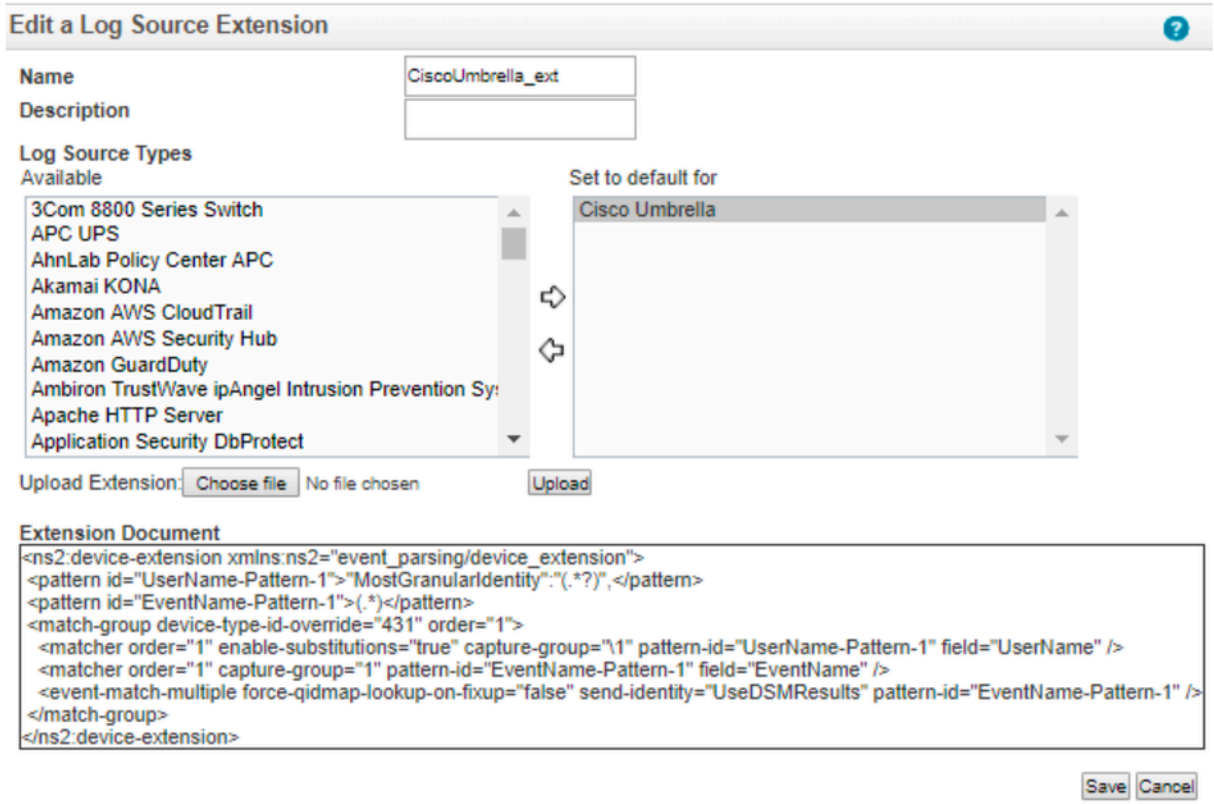
4404306881812



참고: 로그 소스 확장이 "CiscoUmbrella_ext"에 매핑되지 않은 경우 목록에서 로그 소스 이름을 선택하십시오.



360071157752



360071326791

다음은 Cisco Managed Bucket의 예입니다.

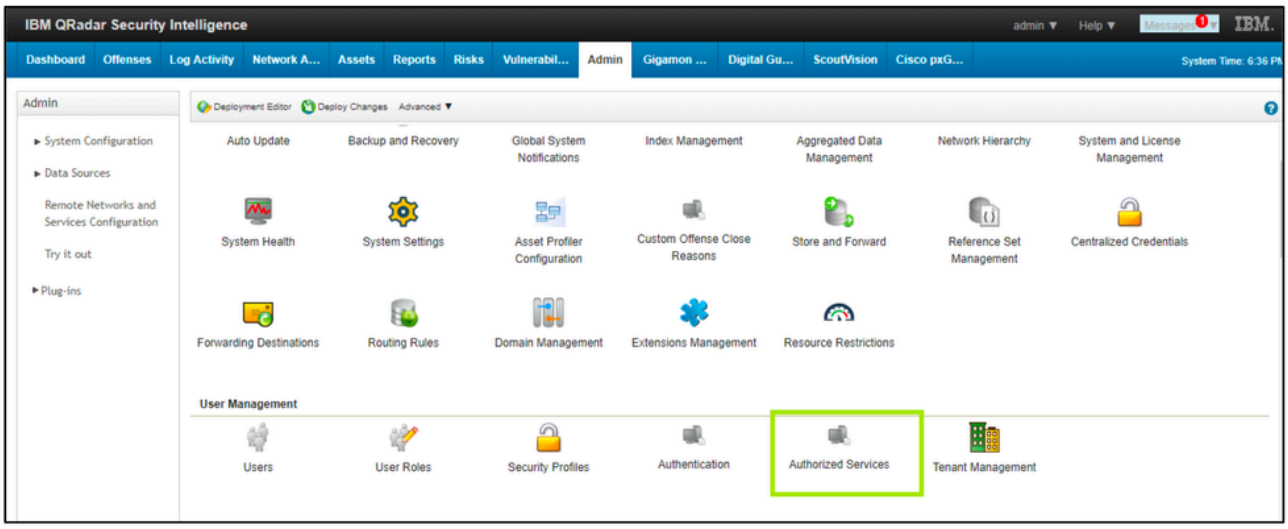
```
Bucket name: cisco-managed-us-west-1
ACCESS_KEY_ID: xxxxxxxxxxxxxx
SECRET_ACCESS_KEY: xxxxxxxxxxxxxx
Region: us-west-1
Your Directory Prefix is the key part of this. This is the customers folder,
followed by the appropriate log folder.
For example: xxxxxxx_cfa37bd906xxxxxx3aff94e205db7bxxxxxxx/dnslogs
```

다시 Cisco Cloud Security App Settings(Cisco Cloud Security 앱 설정)로 이동하고 그래프에서 데이터를 표시할 수 있도록 Panel refresh rate in hours(패널 새로 고침 비율(시간)를 최소값인 "1"로 설정합니다.

인증 토큰 생성

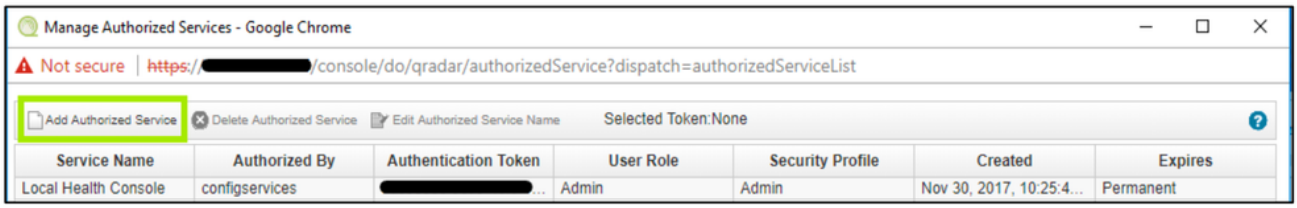
관리자가 Cisco Security App에 추가할 서비스 토큰을 생성해야 합니다. 모범 사례로서, 90일마다 Authorized Service Token을 다시 생성했습니다.

1. QRadar > Admin Tab(관리 탭) > Authorized Services(인증된 서비스)에 로그인합니다.



360071965571

2. Authorized Services를 추가합니다.

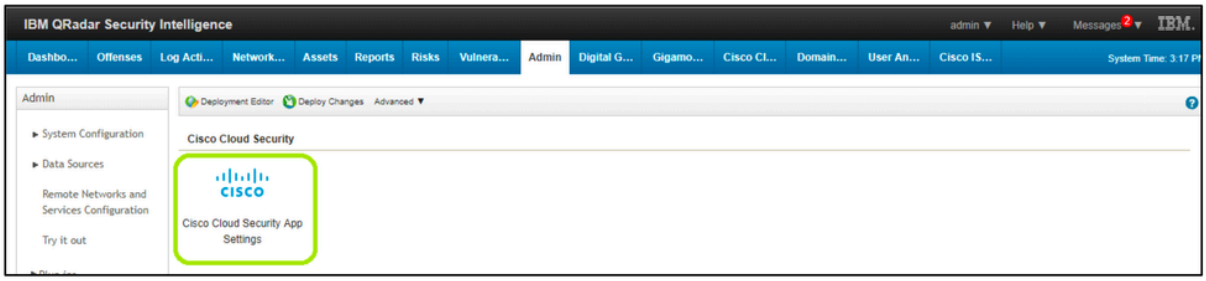


360071965551

3. 세부 정보를 입력하고 인증 토큰을 생성합니다.
4. 토큰을 생성한 후 "Deploy Changes"를 클릭합니다.

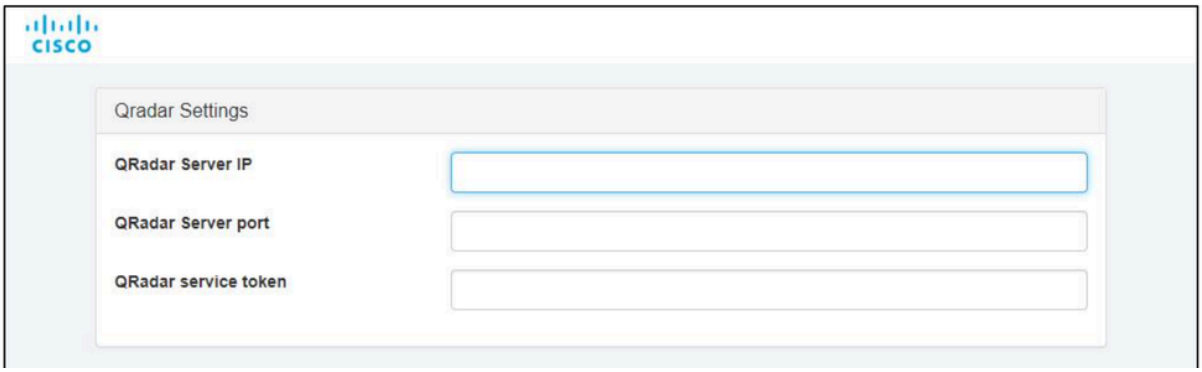
Cisco Cloud Security 앱 구성

1. QRadar 탐색 막대의 Admin(관리) 탭에서 아래로 스크롤하여 Cisco Cloud Security App Settings(Cisco Cloud Security 앱 설정)를 엽니다.



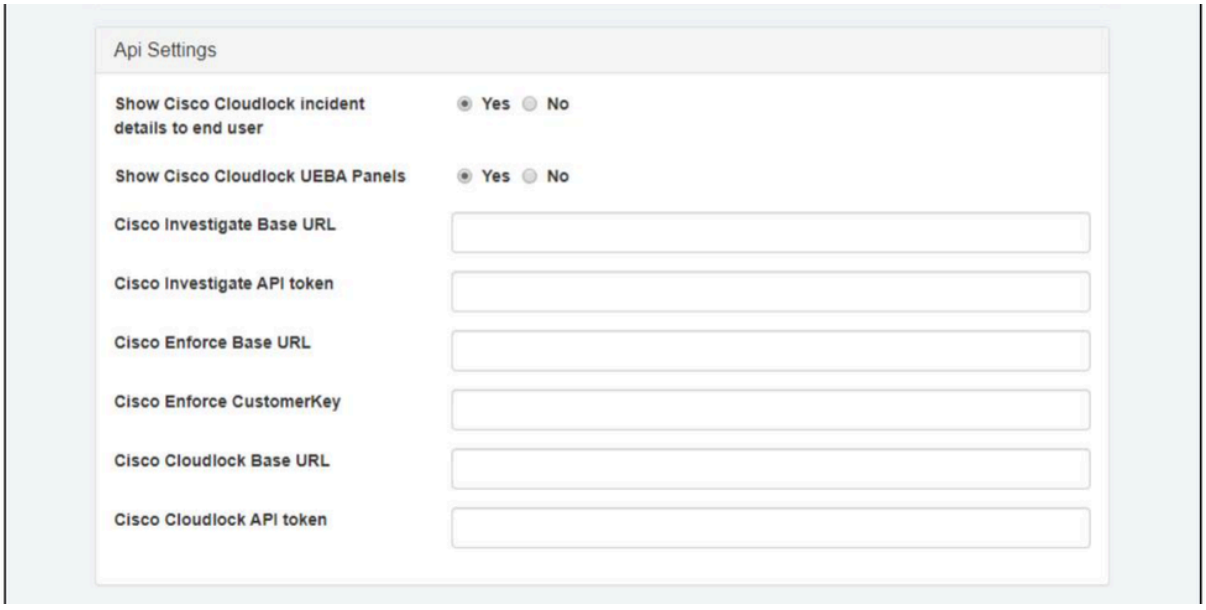
360071754732

2. 이전 단계에서 생성 된 인증 토큰을 입력 합니다.



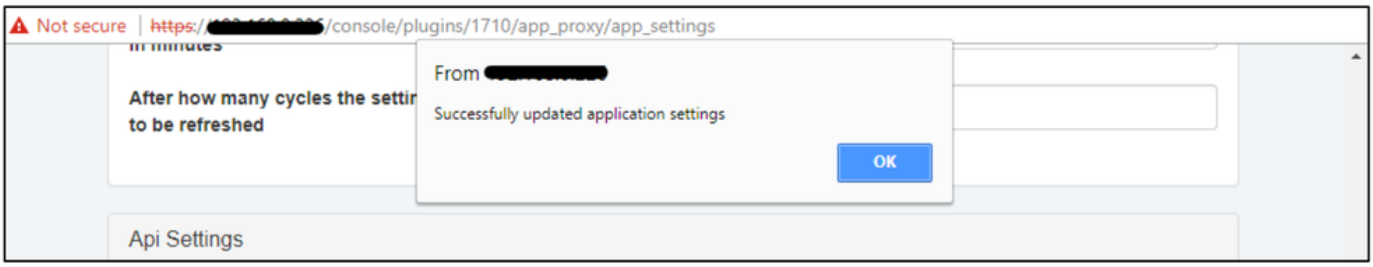
360072462992

3. 다음과 같이 Api 설정을 수정합니다.
    - Cisco Investigate 기본 URL: https://investigate.api.umbrella.com/
    - Cisco Investigate API 토큰 umbrella 대시보드를 통해 생성 -> Investigate -> API Keys -> Create New Token; 자세한 내용은 https://docs.umbrella.com/deployment-umbrella/docs/create-investigate-api-key을 참조하십시오.
    - Cisco Enforce 기본 URL: https://s-platform.api.opendns.com/1.0/
    - Cisco Enforce CustomerKey: umbrella 대시보드 -> 정책 구성 요소 -> 통합 -> 추가, 자세한 내용은 https://docs.umbrella.com/umbrella-user-guide/docs/set-up-custom-integrations을 참조하십시오.
    - Cisco Cloudlock 기본 URL: https://{YourCloudlockAPIServer}/api/v2(예: https://api-demo.cloudlock.com/api/v2/. support@cloudlock.com으로 이메일을 보내 Cloudlock Base URL(Cloudlock Enterprise API URL)을 확인하십시오.)
    - Cisco Cloudlock API 토큰: cloudlock을 통해 생성 -> 설정 -> 인증 및 API -> 생성; 자세한 내용은 https://developer.cisco.com/docs/cloud-security/cloudlock-api-getting-started/#authentication을 참조하십시오.



360072703611

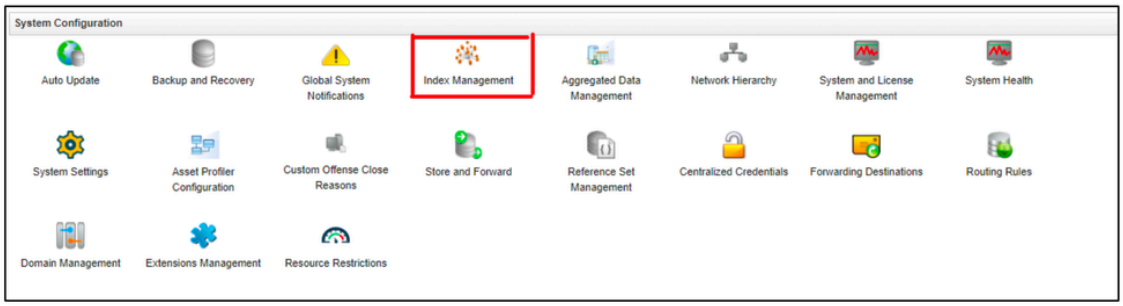
팝업은 애플리케이션 설정이 성공적으로 업데이트되었음을 나타냅니다.



360071986151

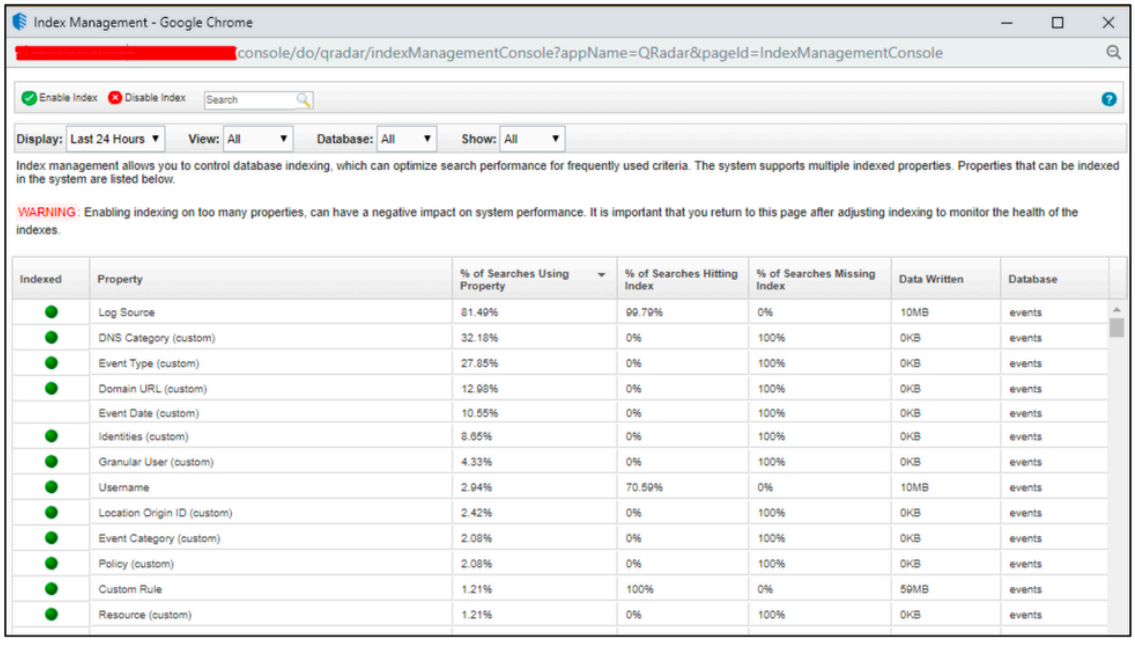
QRadar에서 인덱싱

1. Admin(관리) 탭으로 이동한 다음 Index Management(인덱스 관리)를 클릭합니다.



360071780112

2. 앱과 함께 패키지된 CEP를 인덱스화합니다.



360071988811

인덱싱할 권장 CEP는 다음과 같습니다.

1. 로그 소스
2. DNS 범주

3. 이벤트 유형
4. 도메인 URL
5. ID
6. 세분화된 사용자
7. 사용자 이름
8. 위치 출처 ID
9. 이벤트 범주
10. 정책
11. 리소스

이제 QRadar를 사용하여 Cisco Umbrella, Investigate 및 CloudLock 세부 정보에 대한 모니터링 활동을 시작할 준비가 되었습니다. QRadar를 탐색하는 방법에 대한 자세한 지침은 여기에서 확인할 수 있습니다. Cisco Cloud Security 앱 탐색.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.