

# 보안 액세스 및 Umbrella S3 버킷 키 회전 확인 (90일마다 필요)

## 목차

---

- [소개](#)
  - [배경 정보](#)
  - [문제](#)
  - [솔루션](#)
  - [S3 버킷에 대한 액세스 확인](#)
  - [관련 정보](#)
- 

## 소개

이 문서에서는 Cisco 보안 및 모범 사례 개선의 일환으로 S3 버킷 키를 회전하는 단계를 설명합니다.

## 배경 정보

Cisco 보안 및 모범 사례 개선의 일환으로 로그 스토리지용 Cisco 매니지드 S3 버킷을 사용하는 Cisco Umbrella 및 Cisco Secure Access 관리자는 이제 S3 버킷용 IAM 키를 90일마다 회전해야 합니다. 이전에는 이러한 키를 회전할 필요가 없었습니다. 이 요구 사항은 2025년 5월 15일부터 적용됩니다.

버킷의 데이터는 관리자에게 속하지만 버킷 자체는 Cisco 소유/관리됩니다. Cisco 사용자가 보안 모범 사례를 준수하도록 하기 위해 Cisco Secure Access 및 Umbrella에 앞으로 최소 90일마다 키를 돌리도록 요청하고 있습니다. 따라서 사용자가 데이터 유출 또는 정보 공개로 인한 위험이 없으며 선도적인 보안 회사로서 Cisco 보안 모범 사례를 준수할 수 있습니다.

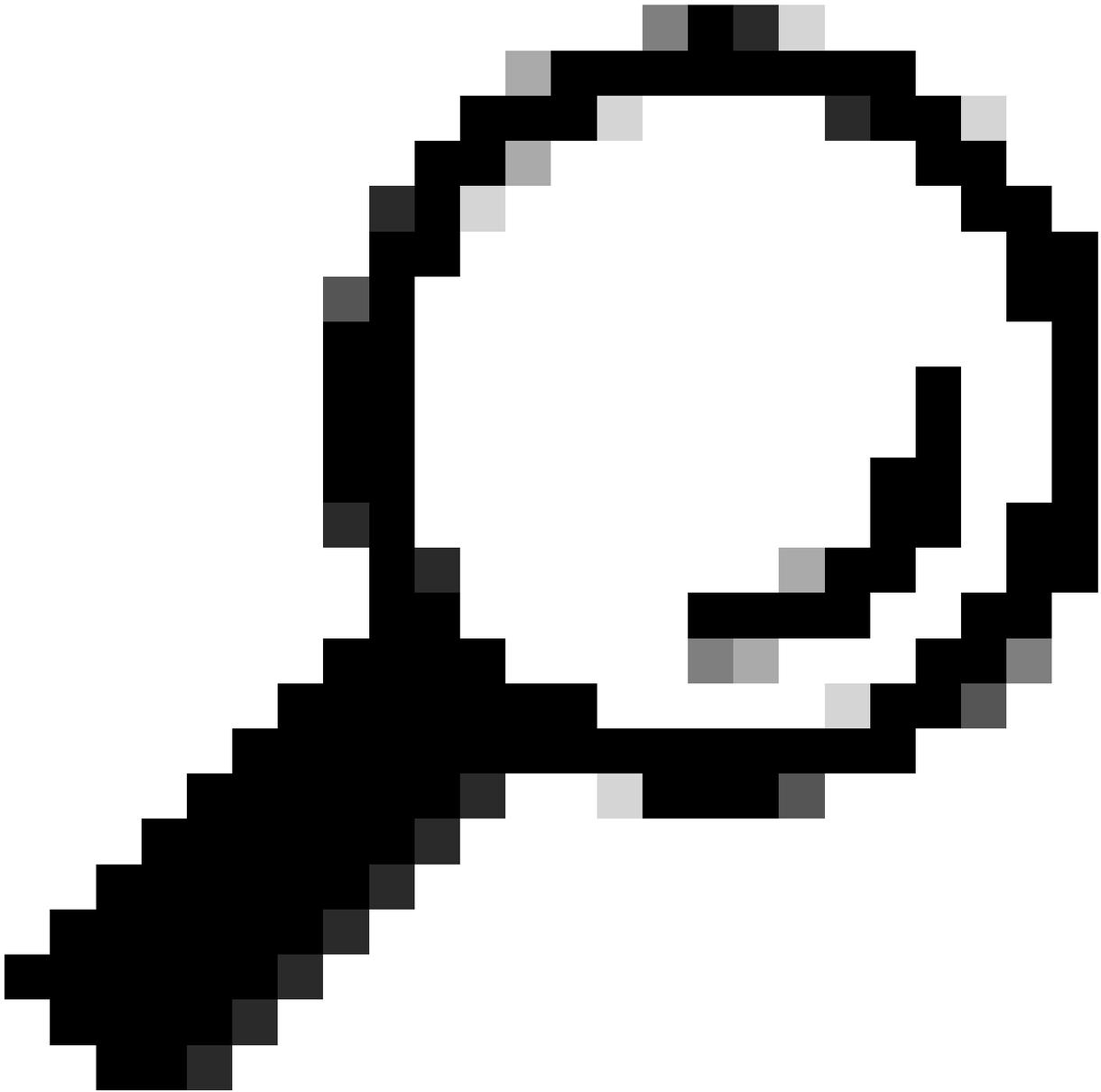
이 제한은 Cisco 이외의 관리 S3 버킷에는 적용되지 않으며, 이 보안 제한으로 인해 문제가 발생하는 경우 자체 관리 버킷으로 이동하는 것이 좋습니다.

## 문제

90일 이내에 키를 회전할 수 없는 사용자는 더 이상 Cisco에서 관리하는 S3 버킷에 액세스할 수 없습니다. 버킷의 데이터는 로깅된 정보로 계속 업데이트되지만 버킷 자체는 액세스할 수 없게 됩니다.

## 솔루션

1. Admin(관리) > Log Management(로그 관리)로 이동하고 Amazon S3 영역에서 Use a Cisco-managed Amazon S3 bucket(Cisco에서 관리하는 Amazon S3 버킷 사용)을 선택합니다



팁: 새 배너에는 S3 버킷 키 회전의 새로운 보안 요구 사항에 대한 경고 메시지가 표시됩니다.

---

✔ We're sending data to your Cisco-managed Amazon S3 storage

Cisco-managed Amazon S3 buckets require that you regenerate the keys every 90 days. Note that this would invalidate any existing keys. If you would like to avoid this, use your company-managed S3 bucket. You may also regenerate them if you forgot your existing keys. To learn more [view our guide](#).

⚠ **Your Cisco-managed Amazon S3 bucket keys expire in 30 days.**  
After this time, your logs will still be sent to your Amazon S3 bucket but you will no longer be able to access them. In order to avoid loss of access, click "Regenerate Keys".

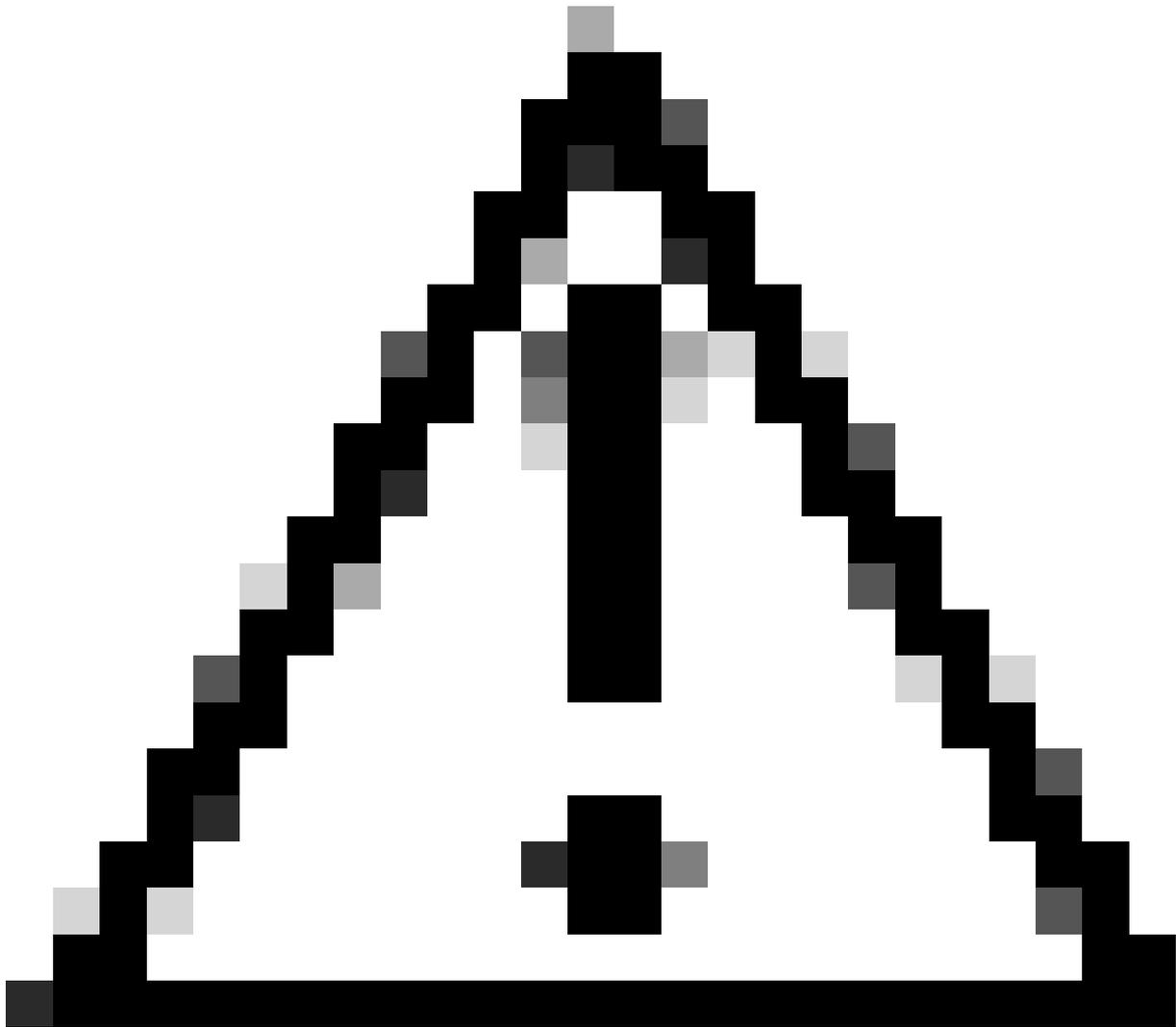
Storage Region	US West (N. California)
Retention Duration	30 days <a href="#">Edit</a>
Admin Audit Log	Include Admin Audit Log in S3 <input checked="" type="checkbox"/>
Data Path	s3://cisco-managed-us-west-1/
Last Sync	Feb 13, 2023 at 6:10 PM
Schema Version	v4 <a href="#">Upgrade</a>   <a href="#">View Details</a> <span>v6 Available</span>

STOP LOGGING

REGENERATE KEYS

2. 새 S3 버킷 키 생성

3. 새 키를 안전한 장소에 보관합니다.



주의: 키 및 암호는 한 번만 표시할 수 있으며 Cisco 지원 팀에 표시되지 않습니다.

---

## New keys have been generated

Your keys are ready. Please keep them in a safe place. If you need to regenerate keys, *old keys will immediately and permanently lose access.*

**Data Path** s3://cisco-managed-us-west-1/ [redacted] 

**Access Key** [redacted] 

**Secret Key** [redacted] 

Got it!

**CONTINUE**

4. Cisco Managed S3 버킷에서 로그를 수집하는 외부 시스템을 새 키와 암호로 업데이트합니다.

## S3 버킷에 대한 액세스 확인

S3 버킷에 대한 액세스를 확인하려면 이 예제나 Secure Access and Umbrella 설명서 가이드에 설명된 파일 형식을 사용할 수 있습니다.

1. 새로 생성된 키로 AWS CLI를 구성합니다.

```
$ aws configure
AWS Access Key ID [None]:
```

```
AWS Secret Access Key [None]:
```

```
Default region name [None]:
```

```
Default output format [None]:
```

2. S3 버킷에 저장된 로그 중 하나를 나열합니다.

```
$ aws s3 ls s3://cisco-managed-us-west-1/[org_id]_[s3-bucket-instance]/dnslogs  
PRE dnslogs/  
$ aws s3 ls s3://cisco-managed-us-west-1/[org_id]_[s3-bucket-instance]/auditlogs  
PRE auditlogs/
```

## 관련 정보

- [Cisco Secure Access 로깅 관리](#)
- [로그 형식 및 버전 관리](#)

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.