Verify Secure Access and Umbrella S3 Bucket Keys Rotation (Required Every 90 Days)

Contents

Introduction

This document describes the steps of rotating the S3 Bucket keys as part of Cisco Security and best practices improvements.

Background Information

As part of Cisco Security and best practices improvements, Cisco Umbrella and Cisco Secure Access administrators with Cisco-managed S3 buckets for log storage are now required to be rotated the IAM Keys for the S3 bucket every 90 days. Previously, there was no requirement to rotate these keys. This requirement taking effect beginning on May 15, 2025.

While the data in the bucket belongs to the administrator, the bucket itself is Cisco-owned/managed. In order to have Cisco users comply with security best practice, we are asking our Cisco Secure Access and Umbrella to rotate their keys at least every 90 days going forward. This helps to insure that our users are not at risk of data leakage or information disclosure and adhere to our security best practices as a leading security company.

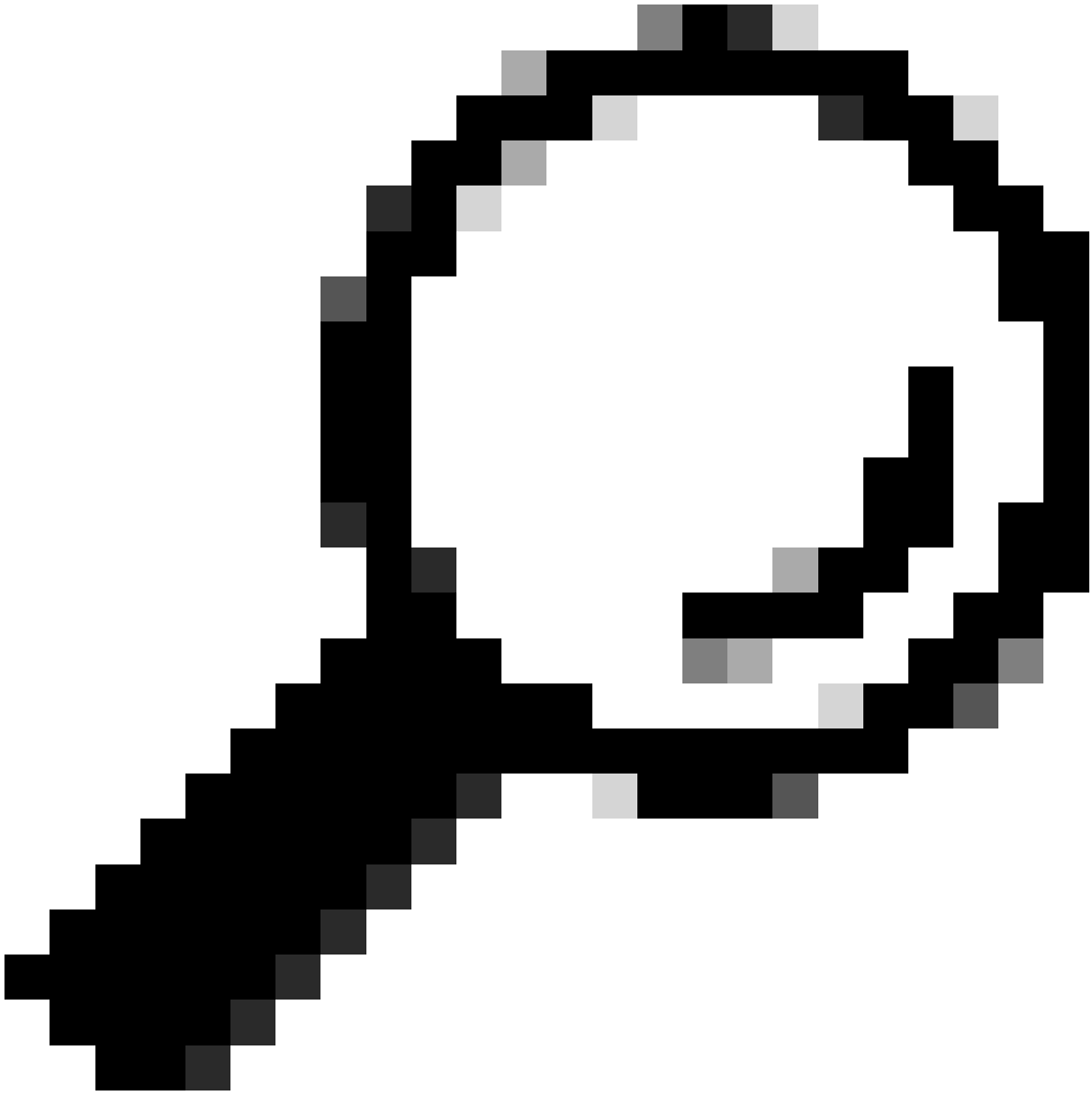
This restriction does not apply to non-Cisco managed S3 buckets and we recommend you move to your own managed bucket is this security restriction creates a problem for you.

Problem

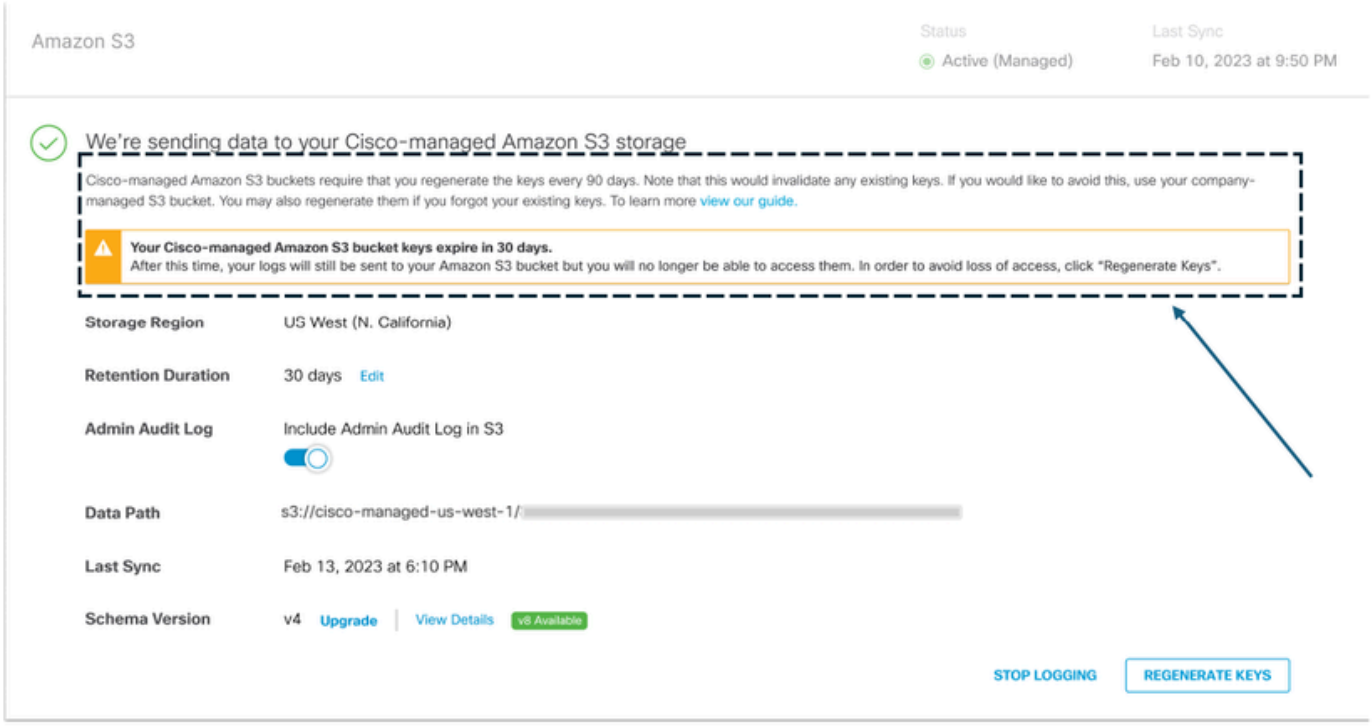
Users who are not able to rotate their keys within 90 days, are no longer have access to their Cisco-managed S3 buckets. The data in the bucket continue to be updated with logged information but the bucket itself becomes inaccessible.

Solution

1. Navigate to **Admin** > **Log Management** and in the Amazon S3 area select Use a **Cisco-managed Amazon S3 bucket**

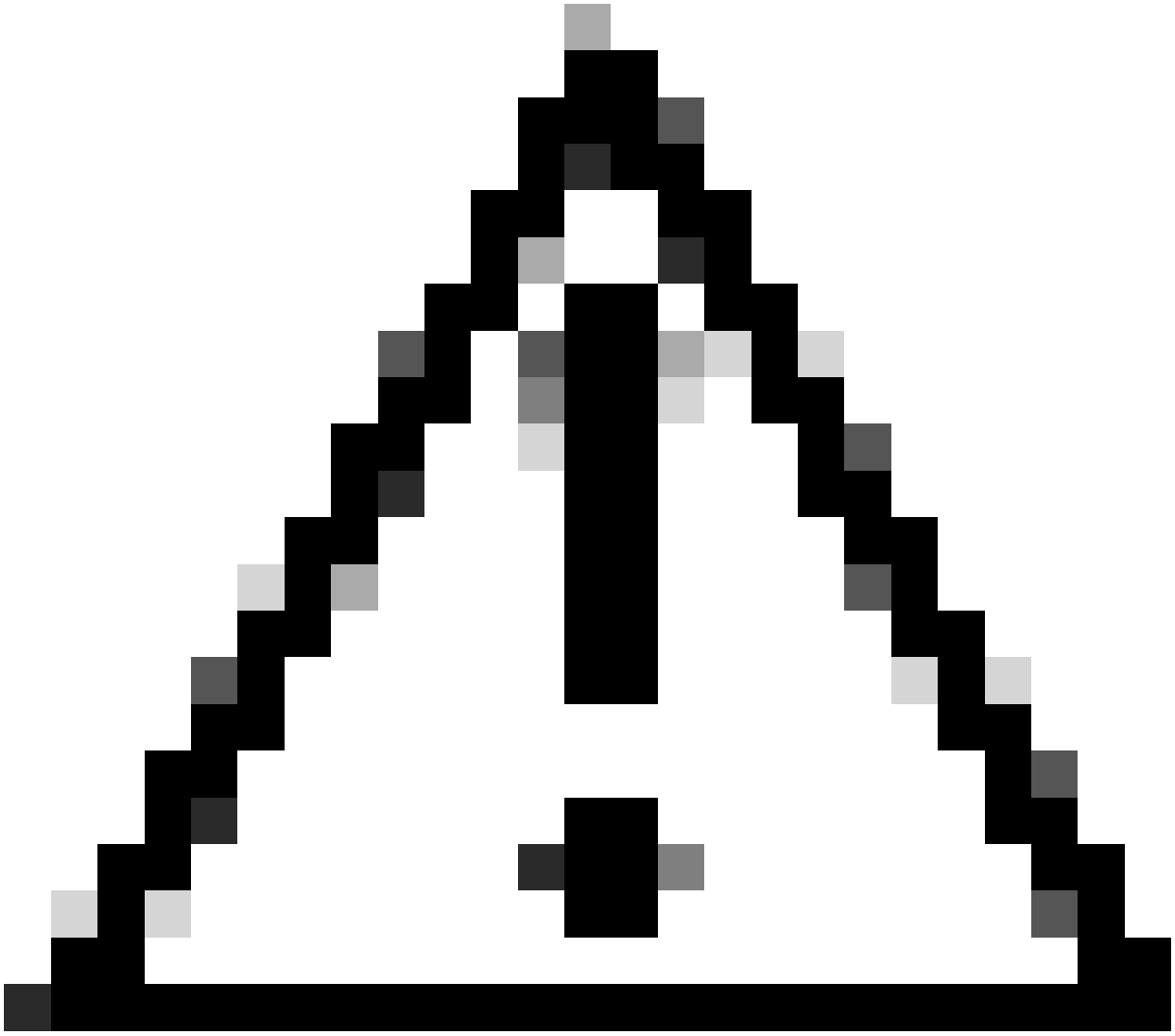


Tip: New banner is presented with warning message regarding the new security requirements of rotating the S3 Bucket keys.

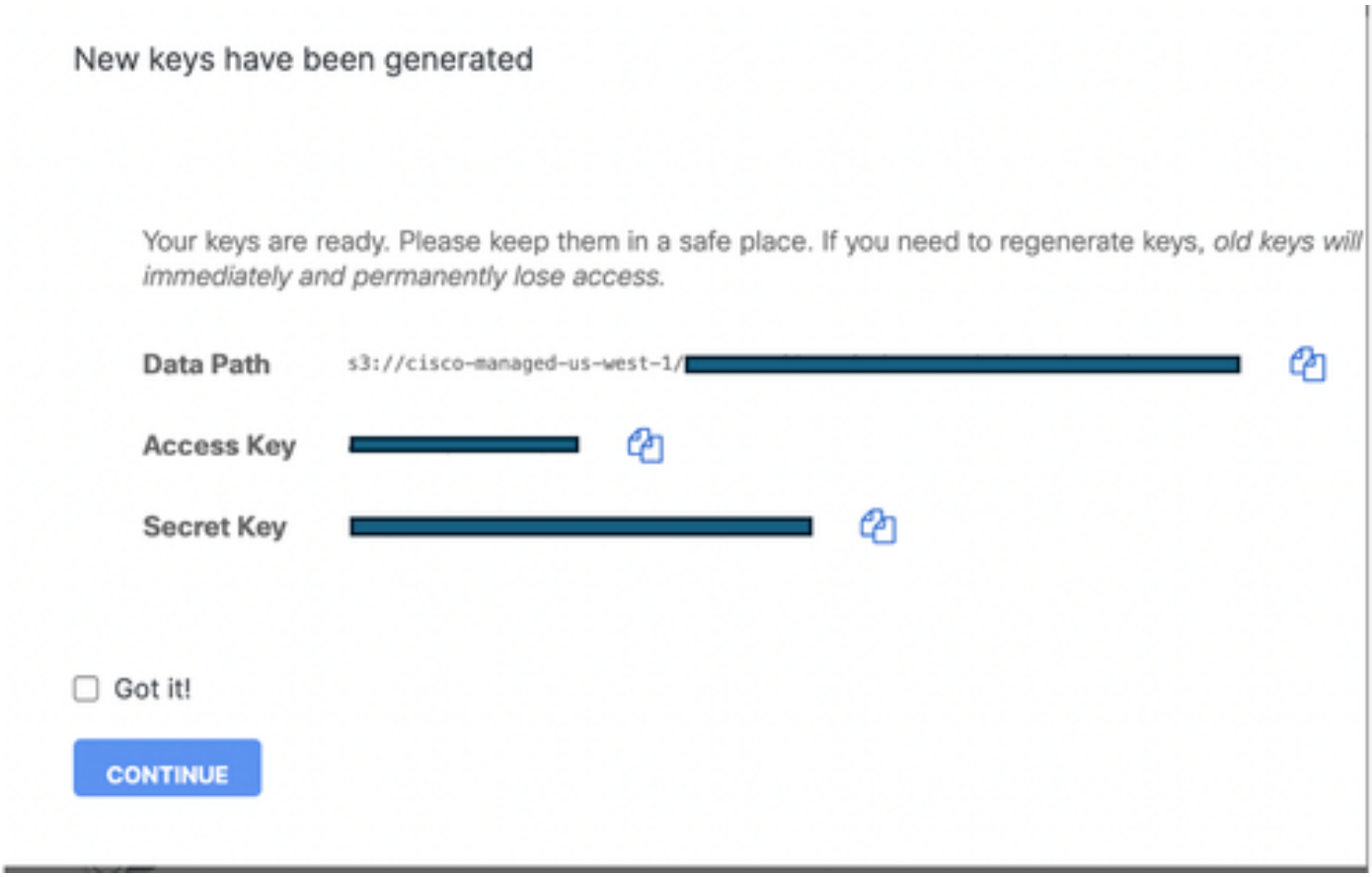


2. Generate your new S3 Bucket keys

3. Store your new key in safe place.



Caution: They Key and secret can only be displayed once and is not visible to Cisco support team.



4. Update any external system ingesting logs from Cisco-Managed S3 bucket with the new key and secret.

Verify Access To S3 Bucket

To verify Access to your S3 Bucket you can use the files format as clarified in this example or in Secure Access and Umbrella documentation guide.

1. Configure your **AWS CLI** with new generated keys.

```
$ aws configure
AWS Access Key ID [None]: <Enter Your Generated Access Key>
AWS Secret Access Key [None]: <Enter Your Generated Secret Key>
Default region name [None]: <Enter Your S3-Bucket Region>
Default output format [None]:
```

2. List one of the saved logs in your S3-Bucket.

```
$ 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/
```

Related Information

- Manage Cisco Secure Access Logging
- Log Formats and Versioning