CLOUD STORAGE SECURITY

Antivirus for Amazon S3

End-User Deployment and Configuration Guide

aws PARTNER

- Public Sector
- Security Software Competency

Overview

In this document you will learn how to deploy Antivirus for Amazon S3 into your AWS environment and scan your first file to ensure it's not infected.

We'll cover the following:

- Subscribe, Deploy, and Configure in your Primary Account
- Protecting Additional Account(s)
- Day 1 Activities
- Frequently Asked Questions
- Advanced Considerations

> **We needed to migrate our existing AV solution to a solution that could accommodate API-integrated scanning. To our surprise, we were able to start scanning our files in 2 weeks instead of the expected 2 months because Antivirus for Amazon S3 was so easy to install, setup and configure. And it met our performance expectations from the get-go.**
>
> Lead Cloud Security Architect at
> Major Healthcare Company

Subscribe to Antivirus for Amazon S3

Antivirus for Amazon S3 is available in AWS Marketplace with a 30 day free trial for testing and usage. The software is self-hosted and no data will leave or be processed outside of your environment. Pricing is consumption based and publicly available within the AWS Marketplace listing. Users also have the option to purchase a custom license through AWS Marketplace Private Offers or Cloud Storage Security directly.

Step 1 - Subscribe and deploy Antivirus for Amazon S3 via the AWS Marketplace

To subscribe, go to the Cloud Storage Security Antivirus for Amazon S3 listing in AWS Marketplace. After selecting the configuration you can start deploying Antivirus for Amazon S3 using our CloudFormation Template.

AWS Marketplace listing

Step 2 - Deploy Antivirus for Amazon S3 using a CloudFormation Template

Deployment of the app is accomplished using a CloudFormation Template that installs all necessary infrastructure and software components as well as all required permissions and roles. Review full details of setting up the CloudFormation Template by visiting the **How to Deploy** section of the Cloud Storage Security Help Docs.

The CloudFormation Template will create the following resources:

- ECS Fargate Cluster with 1 Service and Task
- DynamoDB; AppConfig
- IAM Roles and Policies
- Cognito UserPool
- SNS Topic and CloudWatch Log Groups
- Load Balancer (Optional)

While executing the CloudFormation Template you'll need to fill in 6 required fields all other fields are optional:

- Stack Name
- The VPC for the Management Console to run in
- Select Subnet A ID
- Select Subnet B ID
- Specify a Console Security Group CIDR Block
- Set a valid email address that will be used for your account login

You can scroll down to find Agent Configuration, particularly, Agent Scanning Engine and change the engine from ClamAV to Sophos if you want to use a specific scanning engine. You can also set the multi-engine scanning option to be disabled, enabled for all files or only for large files that ClamAV can't scan.

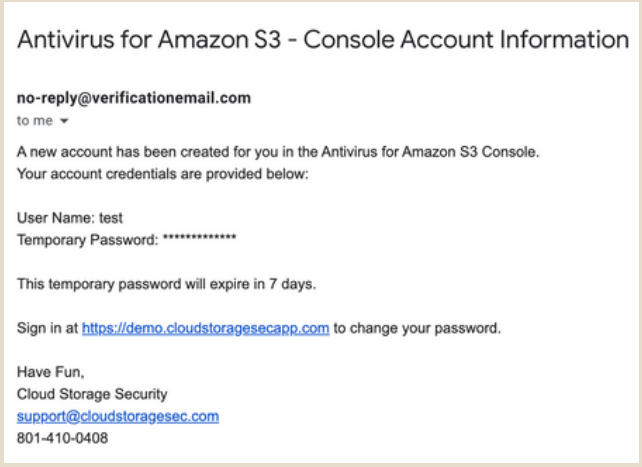
After you bypass the stack configuration options and review your stack you can click the Create Stack button. You'll need to wait until the stack status has changed to CREATE_COMPLETE for the app to be fully deployed.

Step 3 - Launch the Antivirus for Amazon S3 Management Console

Once the stack is created, you will have a running Console task that provides the GUI management.

You'll receive an invitation email with login credentials that you can use to access your console.

Once you've accessed your console, you'll be able to review all discovered buckets, connect additional AWS accounts (if you have any) and enable any/all aspects of scanning.


Antivirus for Amazon S3 - Console Account Information

no-reply@verificationemail.com
to me

A new account has been created for you in the Antivirus for Amazon S3 Console.
Your account credentials are provided below:

User Name: test
Temporary Password: **********

This temporary password will expire in 7 days.

Sign in at https://demo.cloudstoragesecapp.com to change your password.

Have Fun,
Cloud Storage Security
support@cloudstoragesec.com
801-410-0408

Sample email with login credentials

Protecting Additional Accounts

Because most AWS users today have multiple AWS accounts it is imperative a security tool allows you to centrally manage the data protection for these accounts. Linking "remote accounts" (non-deployment accounts) through the console will allow you to manage the Amazon S3 buckets from each account enabling the right scan protection for each account and/or each bucket. All that is required is to deploy a cross-account role (provided by the linking process) within each remote account.

Step 1 - Link an account

You can link an account by clicking the Link Another Account button and filling in the *Account Number*, the *Nickname* and specifying which group the account will belong to. Then click the *Link Account* button.

Step 2 - Deploy the Cross Account Role

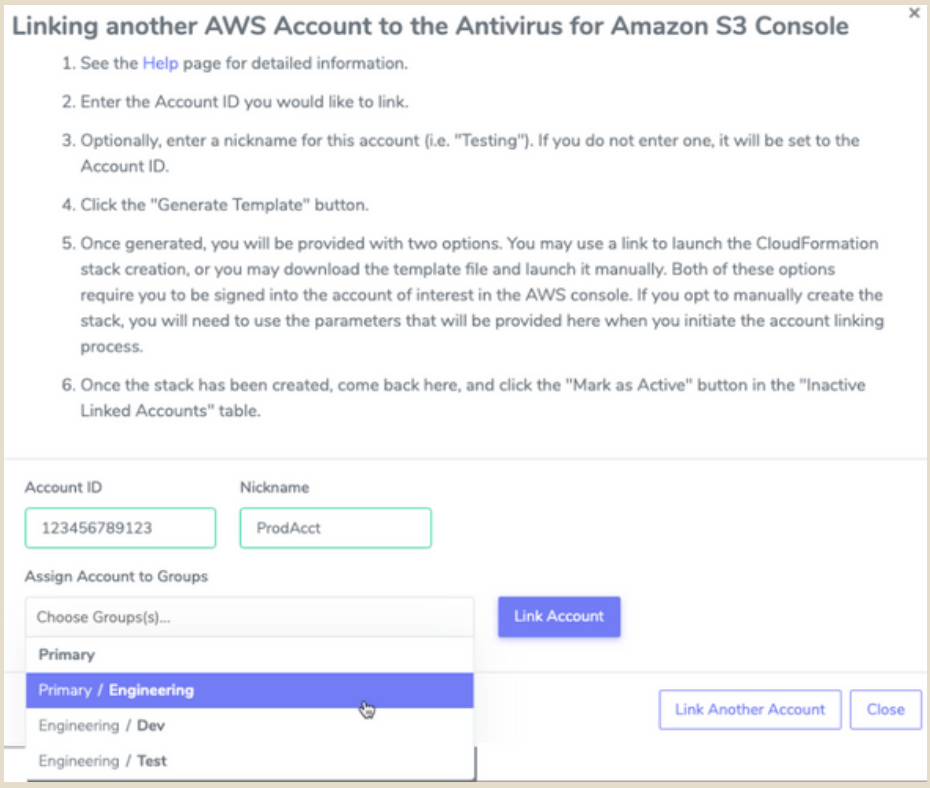
After you click the *Link Account* button, the fields will be replaced with a link to directly launch the CloudFormation Template to create the cross-account role.

Once the role is created, head back to the Antivirus for Amazon S3 console and mark the account active from the action ellipses button.

Step 3 - Verify the Account(s) is Linked

If you see the bucket count update, you can feel confident the role is working appropriately.

Once complete, the account will be shown as active and a bucket count provided. Accounts can be linked and then added in stages so feel free to link all of your remote accounts and then activate them singularly or in groups. You can always deactivate / reactivate accounts later on as needed.



Linking an AWS account as shown in Cloud Storage Security Help Docs

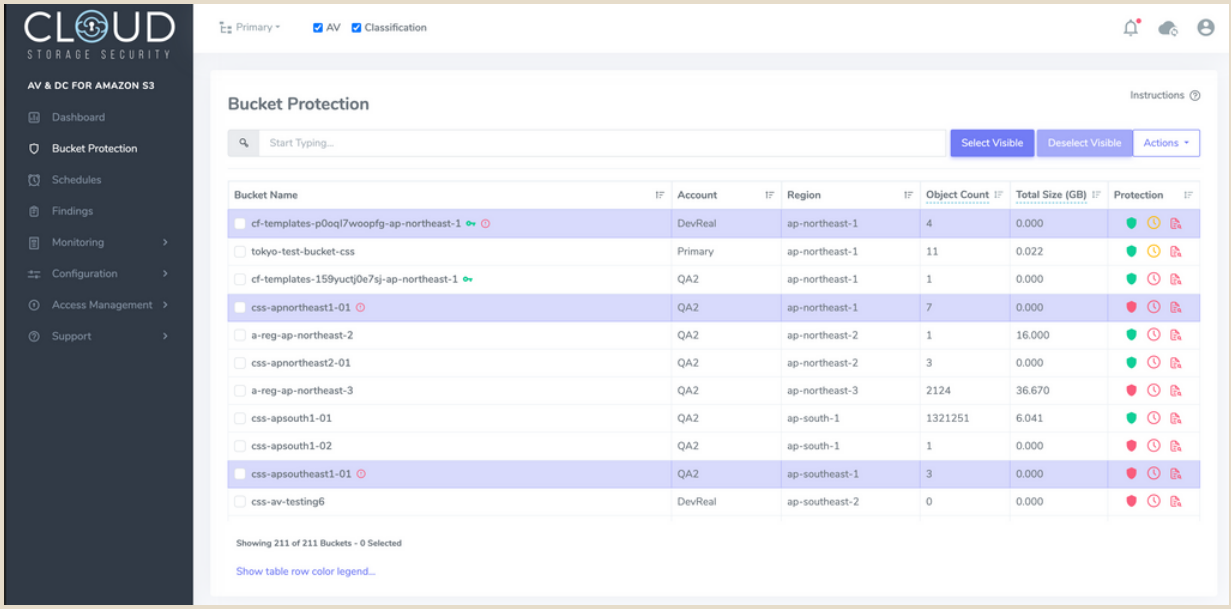
Day 1 Activities for Setup and Protection

There are two main “day 1” activities you should complete right away: enable protection for buckets and setup of notifications to stay aware of file scanning. Additional tasks can be performed as required, please review the Advanced Considerations section in this document.

Enabling Event-Driven Bucket Protection

Antivirus for Amazon S3 accomplishes the scanning of files through three main interaction mechanisms: event driven scanning, retro driven scanning, and API driven scanning.

Once buckets are discovered, you can choose to turn on protection for buckets by clicking the red shield associated with each bucket in your **Bucket Protection** list. Enabling bucket protection allows the app to scan all incoming files in real time. Event Driven scanning requires the least amount of changes to application code, which means you can implement it very quickly as part of your application workflow with little to no impact.



Bucket protection dashboard

Baseline Existing Data and Enabling Scheduled Scanning

You may choose to scan your existing data (files/objects that were already in your buckets at the time of install) to baseline the data and ensure all of your data is clean and safe to use. You can trigger this baseline to occur at the time you activate protection (as described in Event Based Scanning above) or by selecting the bucket(s) and clicking *Scan Existing Files...* in the actions menu within the bucket protection section of your console.

Alternatively, you have the option to enable **scanning on a scheduled basis** of your choosing which will scan new and/or existing files within a bucket on a set schedule.

API Driven Scanning

You can use the **API driven scanning model** to determine how you want to handle clean and infected files programmatically based on the result of the virus scanning. Please review Application Integrated Scanning within the Advanced Considerations section of this document for more information.

Setup Proactive Notifications

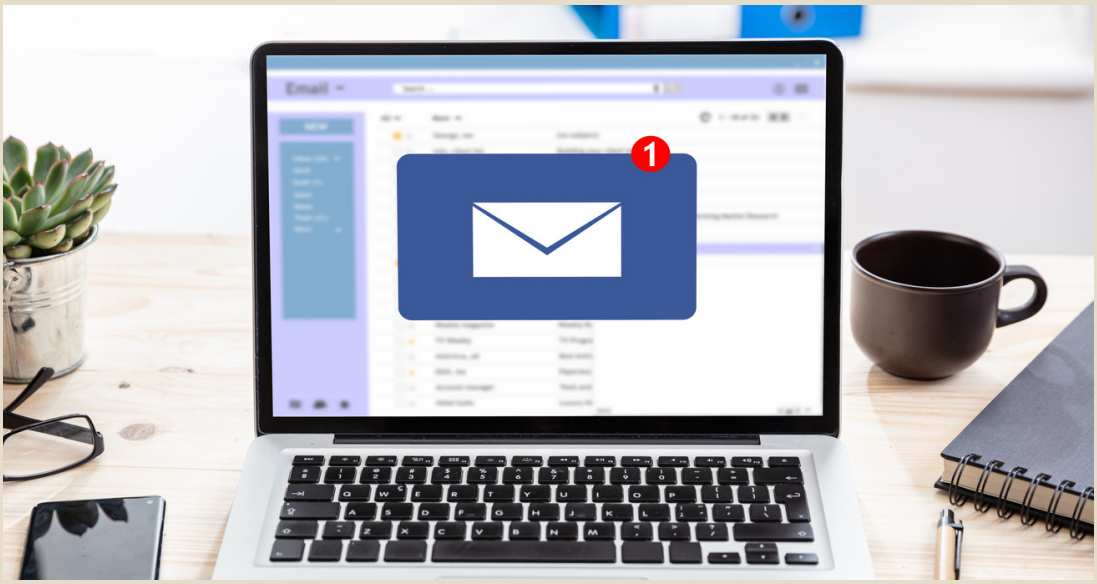
The Dashboard is a great resource to monitor your environment while you are using the console. For all the times you are not in front of the console, we provide **Proactive Notifications**. A Notifications SNS Topic is provided where Antivirus for Amazon S3 publishes useful messages. You can simply subscribe to the Topic with the protocol (HTTP, HTTPS, Email, Email-JSON, Amazon SQS, AWS Lambda, Platform Application Endpoint, SMS) of your choice.

Let's set up an email notification for each time that an infected file is added to our protected bucket:

- From the left menu choose Configuration -> Proactive Notifications and click on Add Subscription
- In the Notification Type box select "Scan Result" and choose your bucket(s) you want notifications for (leaving this empty will receive messages for all protected buckets)
- For the Scan Results and Protocol, enter Infected and Email, and then enter your email address
- Click Add Subscription. The Status is "Pending" so you'll need to confirm your subscription using the confirmation email sent to the email address you entered to receive notifications
- Once confirmed you should start receiving notifications anytime infected files are found

We also recommend subscribing to Product Update notifications:

- From the left menu choose Configuration -> Proactive Notifications and click on Add Subscription
- In the Notification Type box select "UpdatesAvailable" and choose your bucket(s) you want notifications for (leaving this empty will receive messages for all protected buckets)
- For the Protocol, enter Email, and then enter your email address
- Click Add Subscription. The Status is "Pending" so you'll need to confirm your subscription using the confirmation email sent to the email address you entered to receive notifications
- Once confirmed you will receive an email anytime there is a product update



Frequently Asked Questions

How am I charged?

Once your trial expires you'll automatically start to be charged on a pay as you go (PAYGO) basis whenever you scan data. If you're expecting to scan large amounts of data, we have licenses that are negotiable as well. However, if you stick to PAYGO, you'll be charged a minimum monthly subscription fee of $49 per month for the first 100 GB scanned. After that, you will be charged a per GB fee.

Do objects ever leave my account?

No. Antivirus for Amazon S3 is designed and deployed in such a way that neither your Amazon S3 objects nor any copies ever leave your account(s). The solution is deployed in your own AWS environment and we do not have access to your objects.

Which scanning engines are used?

We offer maximum flexibility. You have the option to use the open source ClamAV engine or use our proprietary scanning engine provided by Sophos, which allows you to scan files larger than 2GB with much better performance than the ClamAV engine. Additionally, you have the option to enable scanning using **multiple engines** at once.

Find additional detailed deployment instructions in Cloud Storage Security Help Docs

Who do I contact for support?

Email our support team at support@cloudstoragesec.com or call us at 385-376-3838.

How large of a file can I scan?

We support files up to 5TB in size, which is the maximum file size allowed by Amazon S3, through our **extra large file scanning** capability.

How can I test scanning with a real virus?

The European Institute for Computer Antivirus Research (EICAR) has developed an inert test virus to test your antivirus appliance. You can download the EICAR test virus from the following URL:
http://www.eicar.org/download/eicar.com.txt

Please note: we do not recommend you ever use real virus files for testing purposes.

Do I always have to have scanning agents running?

No. The solution has the flexibility to allow you to schedule both its usage and what data is scanned. **Smart Scan** is a set of agent configurations that allow you to optimize the cost of your infrastructure so you don't always have to keep scanning agents running 24/7. **Scheduled scanning** crawls selected Amazon S3 buckets and scans the pre-existing files in those buckets. You have the flexibility when leveraging this option to specify all files or files within a specific time window.

Advanced Considerations

Application Integrated Scanning

Cloud Storage Security has an accessible API that you can use to submit files for scanning to Antivirus for Amazon S3 in real time. API driven scanning allows you to **scan files as they are uploaded to ensure their security even before the files enter an S3 bucket**. You can use the API driven scanning model to determine how you want to handle clean and infected files programmatically based on the result of the virus scanning. You can use the following APIs:

- Authentication
- Scan File, Return Verdict
- Scan File, Upload to Bucket
- Scan File by S3 Path

Most customers will implement API driven scanning within an application that allows end users to directly upload files. Once the user submits a file the process to scan the file programmatically begins by authenticating with our API and scanning the uploaded file. Once a file is scanned and a verdict is returned, the application workflow can respond accordingly. If the file is found to be clean, you can write the file to the destination of choice. If the file is found to be infected, you can notify the user immediately that their file was rejected because of malware infection.

2 Bucket System Document Flow

The 2 Bucket System flow allows you to create a physical separation between the ingestion of files and your production bucket(s). This allows you to separate incoming objects from your production buckets until they are scanned so they cannot be accessed by your end-users until they are guaranteed to be safe. This approach requires you to create a staging/dirty bucket as the landing area for all uploads and then to leverage the real-time scan result notifications we write to a “notifications” SNS Topic to then copy/move the files to the production bucket(s) as seen below. For detailed steps on how to set this up please visit the **Cloud Storage Security Help Docs**.

Data Classification for Amazon S3

Additional data protection can be achieved through Data Classification for Amazon S3. Identify and protect sensitive data within your cloud infrastructure to ensure proper security posture for sensitive data stored in and shared through Amazon S3. Utilizing **Sophos’ DLP engine**, you can classify files within protected S3 buckets using retro and scheduled classification scans to create a baseline for your pre-existing data in S3.

About Cloud Storage Security

Cloud Storage Security (CSS) is an AWS Public Sector Partner with Security Software Competency and an AWS Qualified Software offering. Organizations throughout the world turn to CSS to ensure their data is clean and protected. Its flagship product, Antivirus for Amazon S3, complements and extends AWS-native security services by preventing organizations from sharing malware via their cloud-based applications and data lakes. Data classification for Amazon S3 advances data privacy practices and regulatory compliance. CSS is a startup founded by a team of expert software developers and cloud professionals with more than 50 years of experience building and running security solutions. Take advantage of a 30 day free trial in AWS Marketplace.

CLOUD STORAGE SECURITY

aws Qualified Software

https://CloudStorageSec.com