**Antivirus – PYPG**

Contents

[Problem statement that we are trying to solve: 2](#_Toc115349164)

[Scope: 2](#_Toc115349165)

[Introduction: 2](#_Toc115349166)

[WHY THIS SOLUTION IS DIFFERENT 2](#_Toc115349167)

[Engines 3](#_Toc115349168)

[Scanning Models 3](#_Toc115349169)

[XL Files 3](#_Toc115349170)

[Analysis 3](#_Toc115349171)

[Configurations 3](#_Toc115349172)

[How to Subscribe: 4](#_Toc115349173)

[How to Deploy: 7](#_Toc115349174)

[How to Configure: 14](#_Toc115349175)

**Document Name: Antivirus - PYPG**

**Owner: Pooja Sawat**

# Problem statement that we are trying to solve:

How to subscribe, deploy, configure antivirus-pypg on aws.

# Scope:

Cloud Storage Security solutions, Antivirus for Amazon S3 and Data Classification for Amazon S3, are available via the Aws Marketplace. To install the software and get it running, you will have to complete three tasks.

* How to Subscribe
* How to Deploy
* How to Configure

# Introduction:

Ensure the data in your Amazon S3 data lakes and application workflows are free of viruses, ransomware, trojans and other payloads by scanning it with Antivirus for Amazon S3 by Cloud Storage Security.

## WHY THIS SOLUTION IS DIFFERENT

* Dual Engine Technology
* 4 Scanning Models
* XL File Scanning
* Static, Dynamic & Forensic Analysis
* Configuration Intelligence
* Simplified Setup
* Security First Approach with In Tenant Scanning

## Engines

Identify malware at petabyte scale across all buckets by leveraging the power of the Sophos Antivirus Dynamic Interface . These engines may be used simultaneously to optimize accuracy and performance.

## Scanning Models

Integrate the method that fits your needs to minimize process interruptions and eliminate service disruptions. Choose from:

* Event - scan new/modified objects in real time when they are dropped into Amazon S3 (great for data lake scanning and integrating into existing application workflows as minimal code changes are needed)
* Retro - scan existing objects on demand or via schedule (useful for compliance audits)
* API - scan objects inside or outside of AWS in real time via a REST-based API before they are written to Amazon S3 (useful if you are migrating to/building a new app on AWS and want inline scanning before the file is written or if you initiate a workflow where the scan dictates whether the object should be stored in Amazon S3)
* Amazon S3 Proxy - scan objects on intake before they are written or on access when they are retrieved by leveraging the Amazon S3 APIs you are already using (PUT, POST, GET)

## XL Files

Never skip scanning a file again due to size. Scan objects as large as 5 TB (the max file size permitted by Amazon S3).

## Analysis

Analyze files in real time when it is unclear whether they are truly a problem without having to execute them or by detonating them in a sandbox using the latest analysis techniques; Static and Dynamic Analysis is powered by the SophosLabs Intelix™ Platform. Antivirus for Amazon S3 also assists with Forensic Analysis as files are segmented by bucket and account enabling you to trace where the file entered and into which account it was added.

## Configurations

Gain visibility into misconfigurations - quickly identify all buckets with secure and insecure permission policies via a single unified dashboard.

# How to Subscribe:

Cloud Storage Security solutions are available via the AWS Marketplace. It is a simple, click-through process within your AWS account. You can subscribe to both products and run them independently or as a unified solution.

Step 1 - Find the listing on the Amazon Marketplace

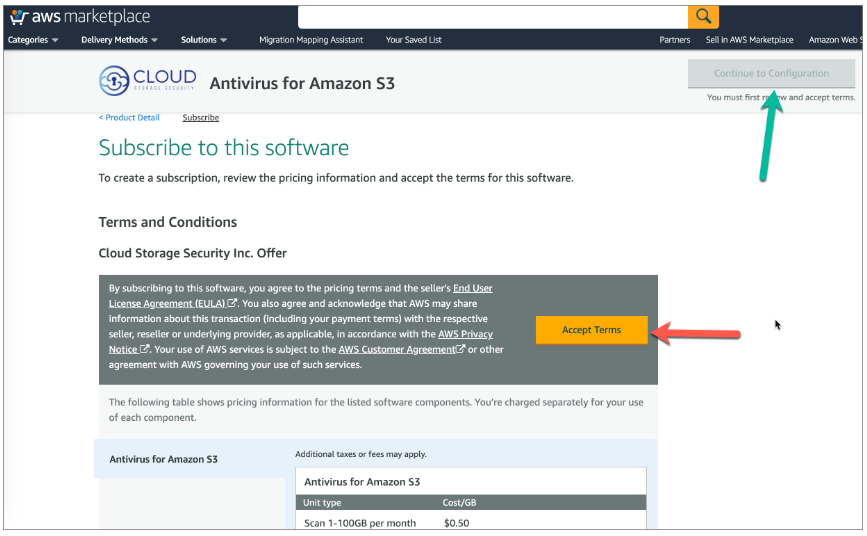
Go to the Cloud Storage Security antivirus for amazon S3 listing on Marketplace



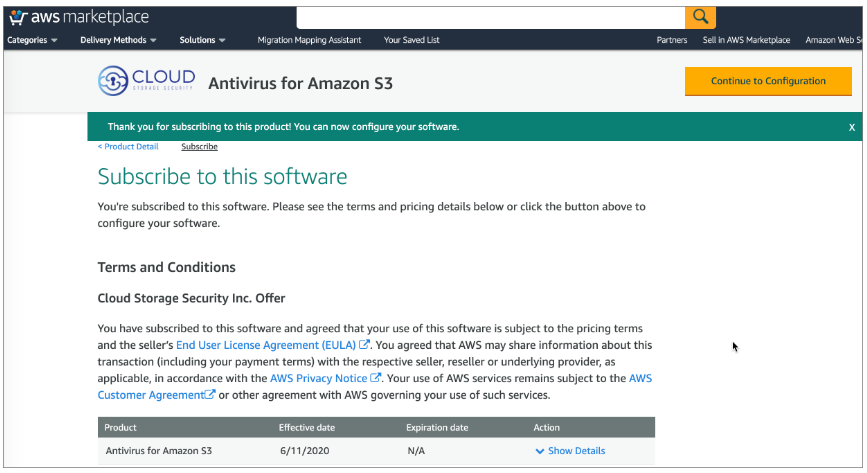
Step 2 - Subscribe to Antivirus for Amazon S3

Click on the Continue to Subscribe button within the AWS Marketplace listing.

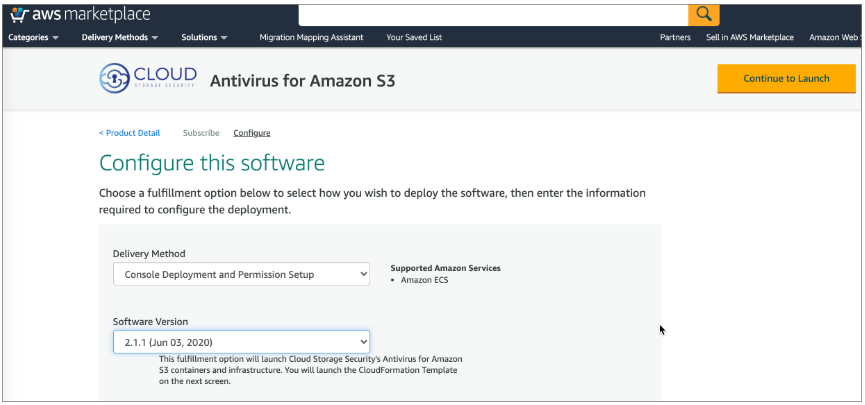
Below you will be asked to accept the terms. Before clicking, review the EULA.



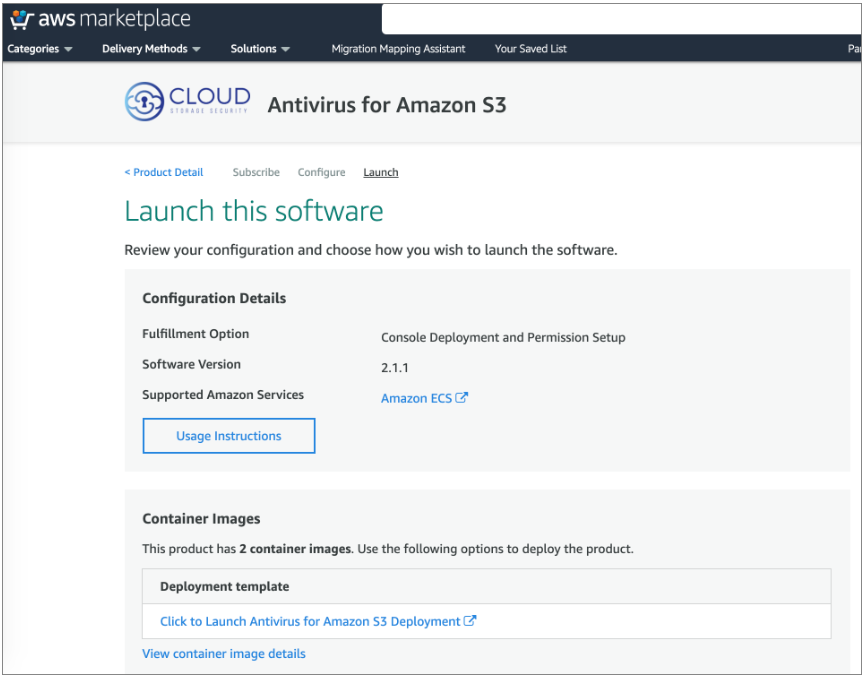
The Effective Date and Expiration Date will change to Pending for a few seconds. Once they are approved, click the Continue to Configuration button. You are now officially subscribed to the product.



Step 3 - Launch Antivirus for S3 For the next screen, you must select the Delivery Method and Software Version to continue. We recommend you leave the default options and click the Continue to Launch button.



The final task is to launch the software. Scroll down under Container Images, under Deployment Templates, click the link Click to Launch Antivirus for Amazon S3 Deployment. This will open the AWS Console CloudFormation service in a different tab. Leave this tab open just in case you need to restart the Stack again.

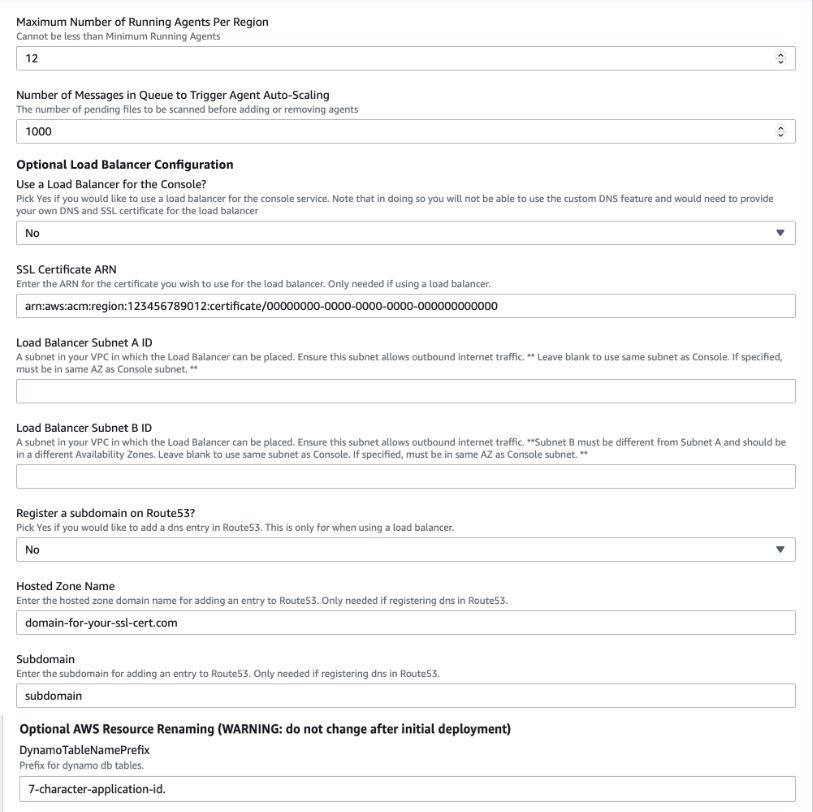
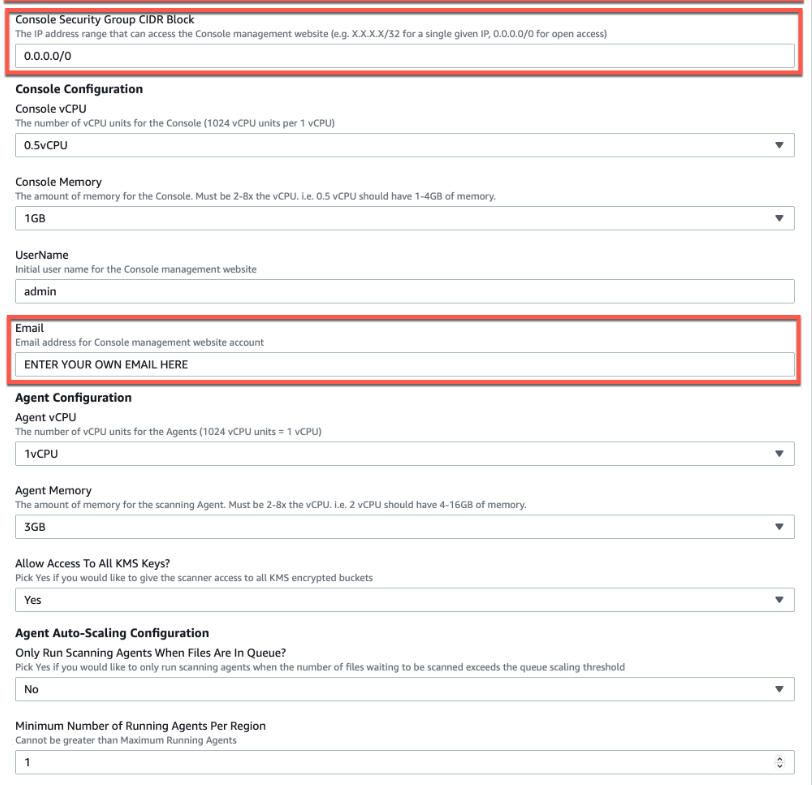
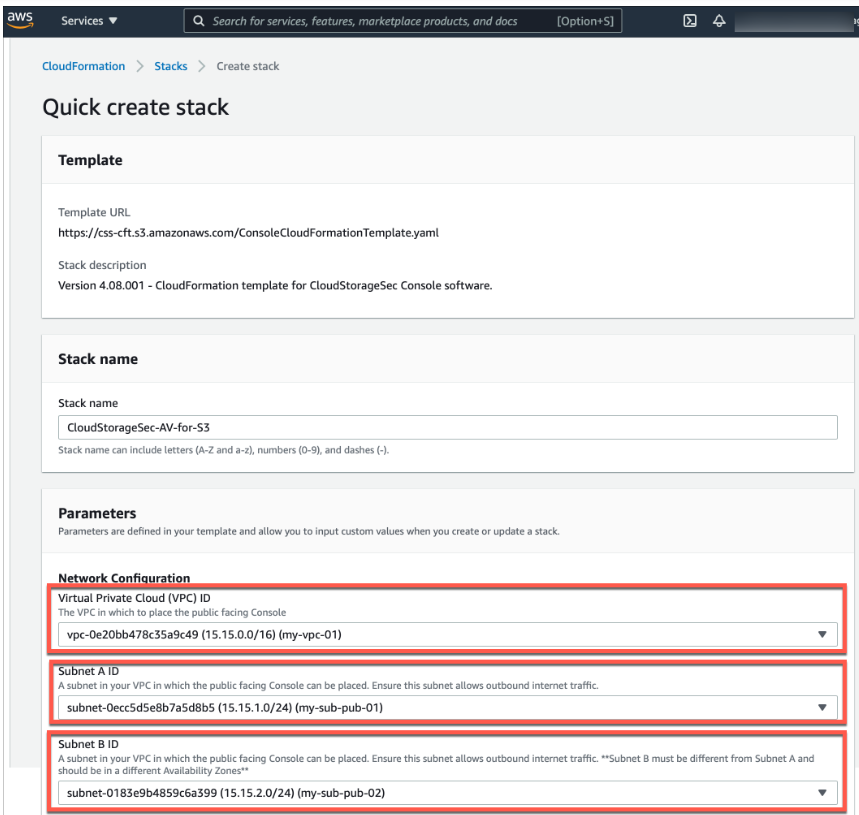


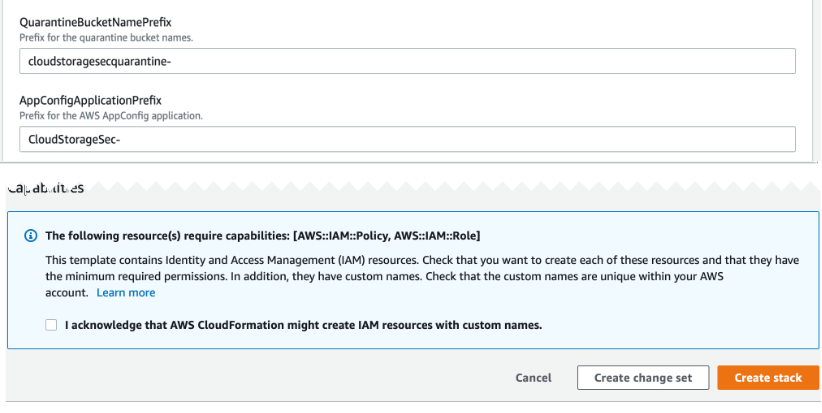
You have completed subscribing to Cloud Storage Security Antivirus for Amazon S3.

# How to Deploy:

Deploying Antivirus for Amazon S3 is accomplished by using a CloudFormation Template that will install the necessary infrastructure components as well as the required roles and permissions.

Step 1 - Quick Create Stack and Specify the Parameters

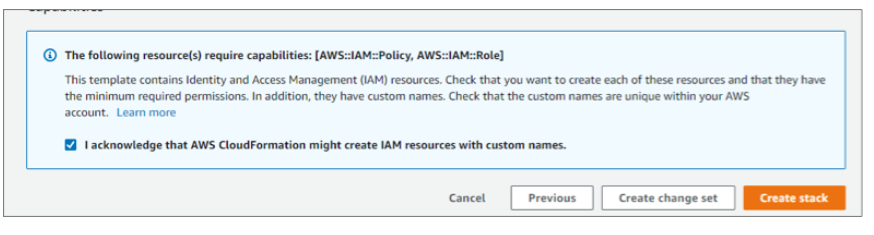




You must provide values for the fields in red boxes above. You can leave all the default settings in the rest of the fields.

1. You must select a VPC from the drop down list for the Management Console to run in.
2. You must select a Subnet A ID from the drop down list contained in the selected VPC.
3. You must select a different Subnet B ID from the drop down list contained in the selected VPC.
4. You must select a Console Security Group CIDR Block. Specify your network access or set to "0.0.0.0/0" to access the Antivirus for Amazon S3 Management Console from anywhere.
5. You must set a valid Email address.

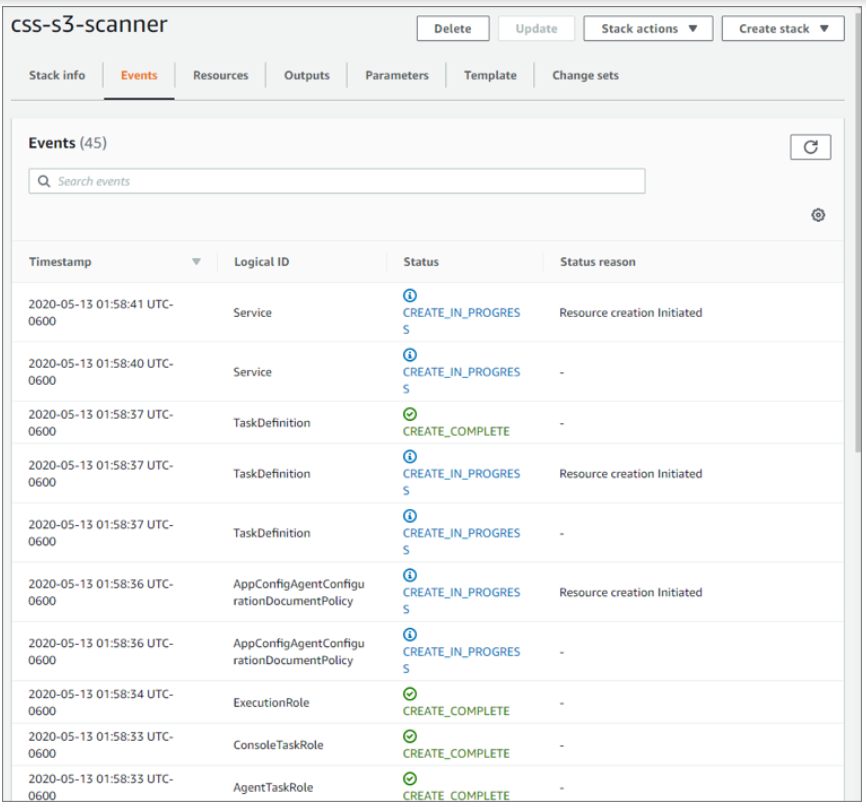
Step 2 - Review CloudStorageSec-AV-for-S3



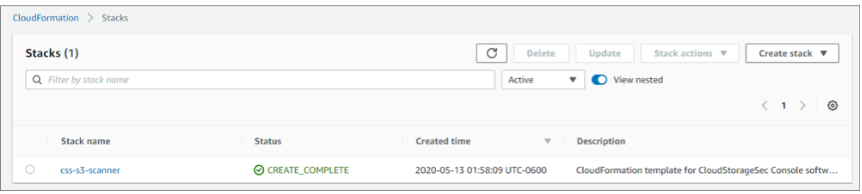
Check I acknowledge that AWS CloudFormation might create IAM resources with custom names. under Capabilities. Click Create Stack at the bottom of the screen.

Step 3 - Troubleshoot if needed

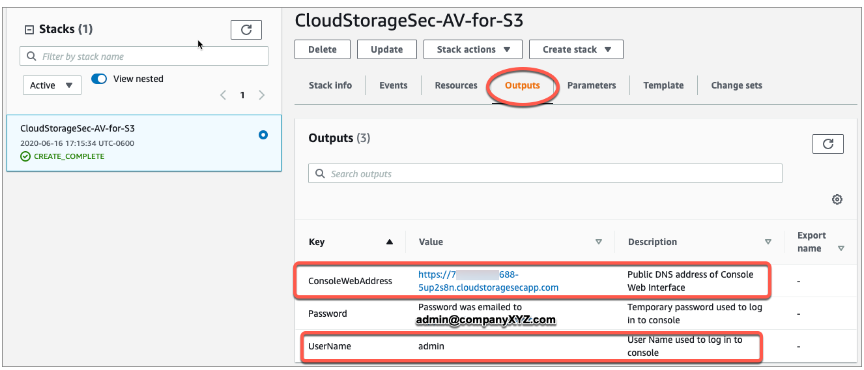
The stack you just created, CloudStorageSec-AV-for-S3 will have a status of CREATE\_IN\_PROGRESS. Wait for this to change to CREATE\_COMPLETE.



When finished:



Step 4 - Console Access



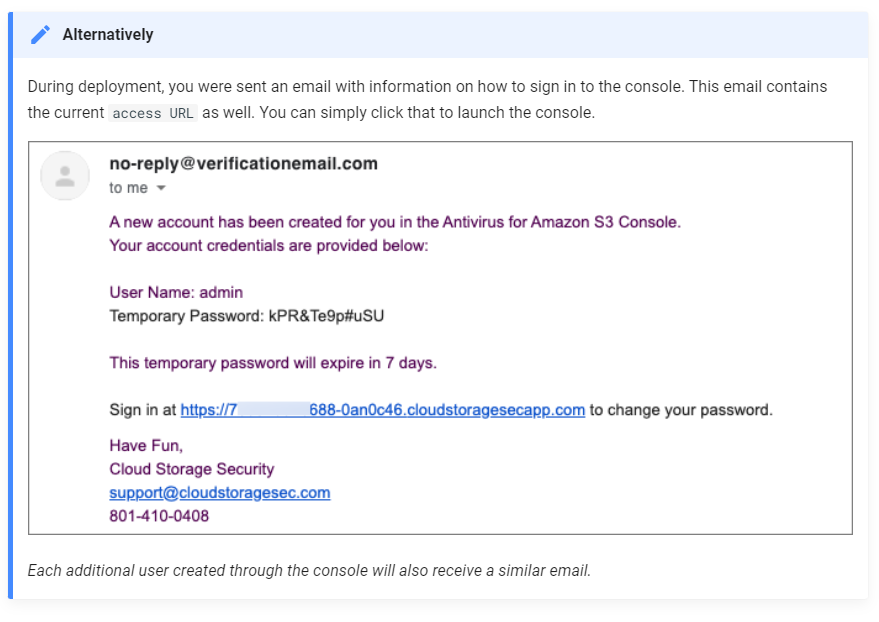
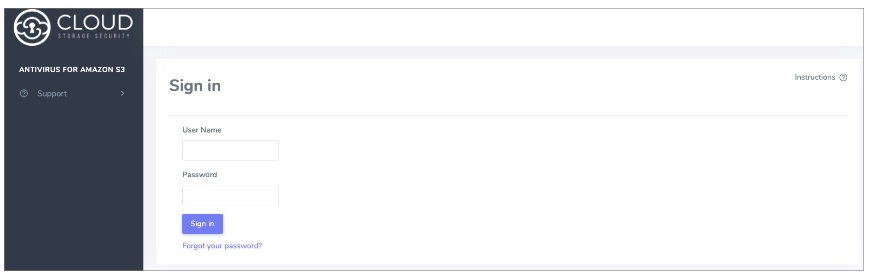
Once the stack creation completes, click the Output tab. The top row in the table will have the URL for the Antivirus for Amazon S3 Management Console. It will be in the format of https://<accountID-appID>.cloudstoragesecapp.com.

You have completed creating the stack for Cloud Storage Security Antivirus for Amazon S3.

# How to Configure:

Step 1 - Launch the Console

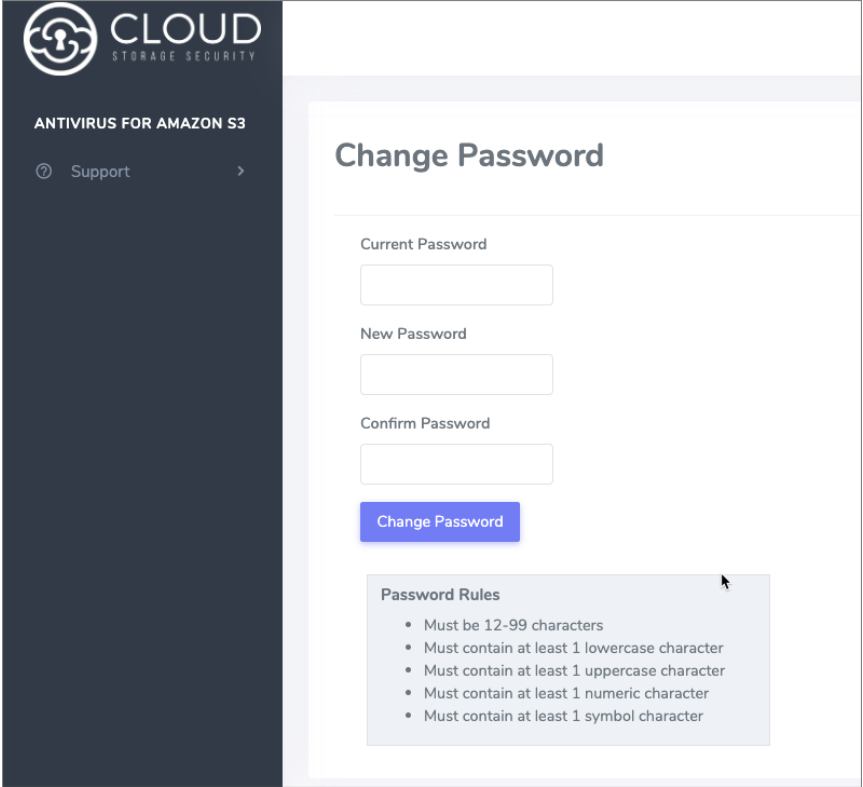
Open your modern browser of choice (chrome, firefox, edge, safari) and place the access URL you retrieved in the [previous step](https://help.cloudstoragesec.com/getting-started/how-to-deploy/#step-4-console-access) into the address bar and hit Enter. You will be taken to the Console Login page as seen below.



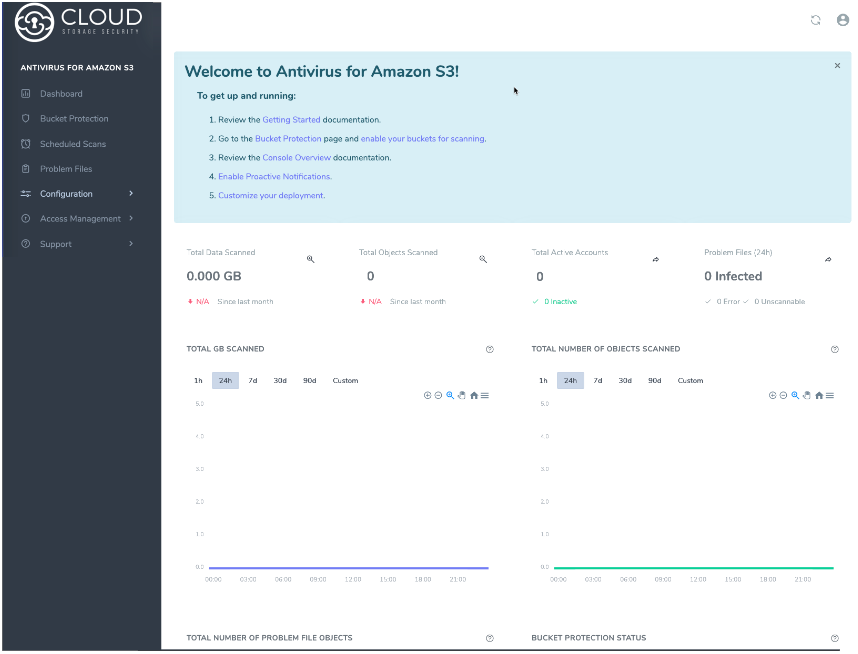
Sign in to the Console:

As seen above, an email is sent to you to provide your User Name and Temporary Password. Place the username and temporary password into the appropriate fields and click Log in.

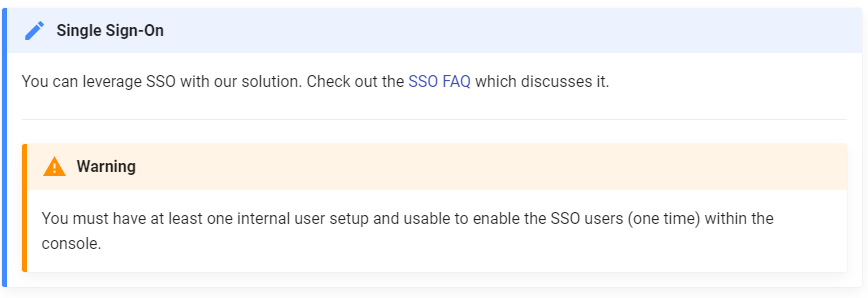
First thing you must do is replace the temporary password. Create a new password for your user.



Clicking Change Password will save your new password and pass you through to the console dashboard.

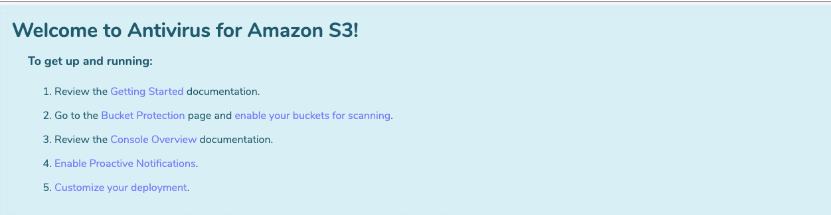


We'll get into grater detatils about what you see here, but just know this is the overall status view into your environment.

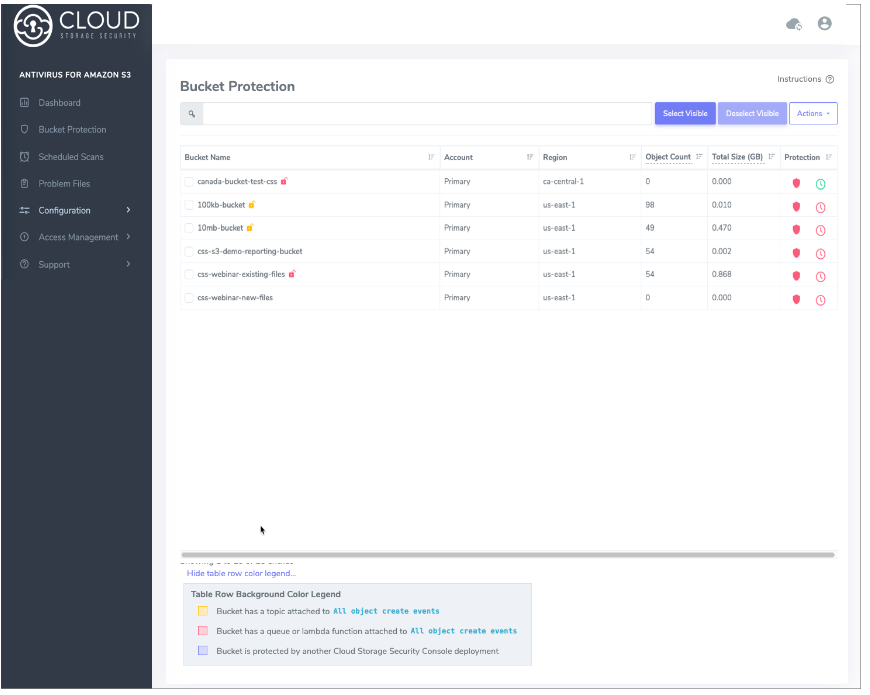


Step 2 - Enable Bucket Scanning

Notice the top information banner indicating:

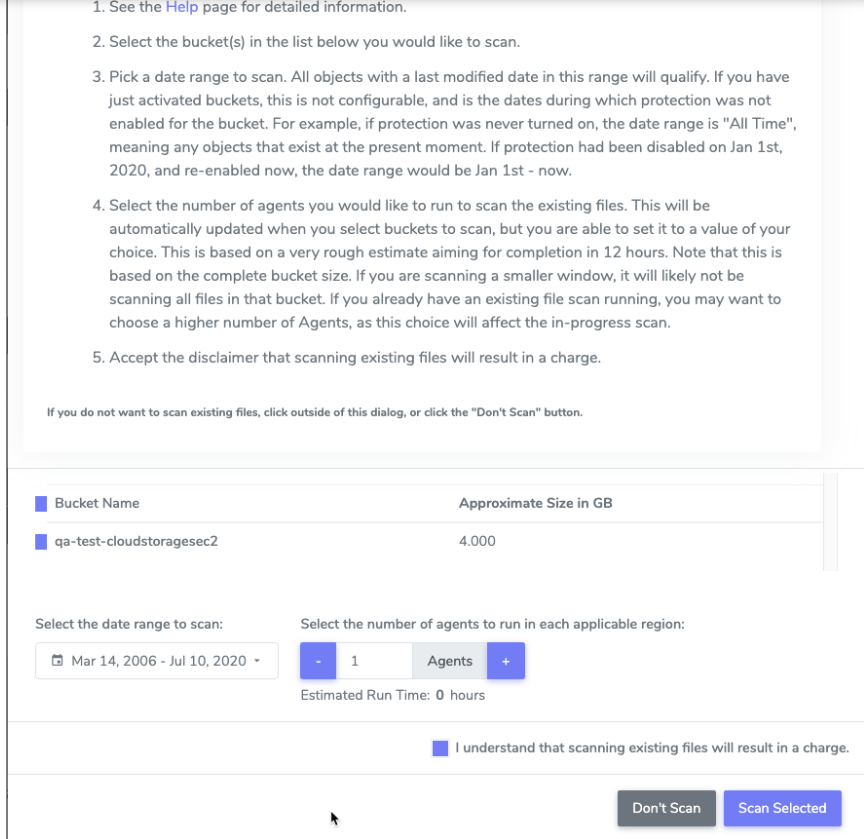


The information banner has 5 steps to get you started. All 5 steps have links to useful spots in the documentation to quickly get you started. The second will also direct you to the Bucket Protection page under Configuration where you will be able to enable your first bucket for scanning. Click the Switch to the Protected Buckets page link to enable your first Amazon S3 Bucket.



Displayed to you are all of the buckets within your AWS account. It is quite easy to enable scanning for a bucket, simply select one or multiple checkboxes for the buckets you wish to protect and select Turn On Selected from the Actions drop down button at the top of the bucket list. To get started pick a bucket in the same region as your console and turn it on. This will enabled the bucket for new object, event-based scanning.

You will also be prompted to scan the existing objects in the bucket(s). You have the choice to skip this by clicking the Don't Scan button or follow the instructions to select some or all of the buckets you had turned on to scan the existing objects as well.



**That's it!**

Once you are to this point, you should see a green shield in the row for any bucket you "turned on" above.