



CS486 User Manual

Revision 1.0

April 23, 2025

StratoSplit

Client:

General Dynamics Mission Systems

Mentor:

Brian Donnelly, Savannah Chappus

Team Members:

Sam Cain

Nolan Newman

Dallon Jarman

Elliot Hull

Introduction

We are pleased you have chosen StratoSplit for your business needs. StratoSplit is a powerful system designed to integrate multicast audio streaming within an operator web console for real time 3d audio management and transmission that has been custom-designed to meet your needs. Some of the key features include: user role management, passwordless login, bidirectional audio panning, configuration management, and team management. The purpose of this user manual is to help you, the client, successfully install, administer, and maintain the StratoSplit product in your actual business context going forward. We aim to make sure that you can integrate this system into existing systems, build upon it, and maintain it.

Installation

As part of final delivery, the StratoSplit system should have been installed on a platform of your choice. Over time, however, you may want to move to a new platform or re-install the product. Below are the necessary hardware, toolchain, and steps to recreate our deployment environment.

Hardware: Two t2 micro EC2 Ubuntu 24.0.4 instances

Toolchain: EC2, Transit Gateway, VPC, Cloudflare, Hanko, MongoDB, Node JS, Python

AWS Setup:

1. Create VPC:

Navigate to 'VPC > Your VPCs > Create VPC' and create a VPC providing a name and IPv4 CIDR '10.99.0.0/16'. Leave everything else default.

<input checked="" type="checkbox"/>	nau-multicast	vpc-0aed22b7391ace15f	Available	Off	10.99.0.0/16
-------------------------------------	---------------	-----------------------	-----------	-----	--------------

2. Create Subnets:

Navigate to 'VPC > Subnets > Create Subnets' and create subnets as follows. Select newly created VPC and provide names, subnet zones, and CIDRs as follows:

Public 1: east 1a - 10.99.0.0/18

Public 2: east 1b - 10.99.64.0/18

Private 1: east 1a - 10.99.128.0/18

Private 2: east 1b - 10.99.192.0/18

<input type="checkbox"/>	nau-public1	subnet-...	✔ Available	vpc-0ae...	⊖ Off	10.99.0.0/18
<input type="checkbox"/>	nau-private2	subnet-...	✔ Available	vpc-0ae...	⊖ Off	10.99.192.0/18
<input type="checkbox"/>	nau-public2	subnet-...	✔ Available	vpc-0ae...	⊖ Off	10.99.64.0/18
<input type="checkbox"/>	nau-private1	subnet-...	✔ Available	vpc-0ae...	⊖ Off	10.99.128.0/18

3. Create Internet Gateway:

Navigate to 'VPC > Internet Gateways > Create Internet Gateway' within AWS and create a new internet gateway.

Create internet gateway [Info](#)

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag
Creates a tag with a key of 'Name' and a value that you specify.

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key **Value - optional** [Remove](#)

[Add new tag](#)

You can add 49 more tags.

[Cancel](#) [Create internet gateway](#)

Add new IGW to 'Public 1' routing table and 'Public 2' routing table.

<input type="checkbox"/>	nau-igw	igw-0c6d6330b3d80b0cc	✔ Attached	vpc-0aed22b7391ace15f nau-multicast
--------------------------	---------	---------------------------------------	------------	---

Routes (2)

[Both](#) [Edit routes](#)

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0c6d6330b3d80b0cc	✔ Active	No
10.99.0.0/16	local	✔ Active	No

4. Create Transit Gateway:

Navigate to 'VPC > Transit Gateways > Create Transit Gateway' within AWS. Check enable multicast support, leave all else default, and confirm.

Multicast support [Info](#)

<input type="checkbox"/>	nau-transit-gateway	tgw-061064e44de57c203	✔ Available
--------------------------	---------------------	---------------------------------------	-------------

5. Create Transit Gateway Attachment:

Navigate to 'VPC > Transit gateway attachments > Create transit gateway attachment'. Select the new Transit Gateway and the VPC. The subnets should auto populate with the public subnets. Create the transit gateway attachment.

VPC ID

Select the VPC to attach to the transit gateway.

vpc-0aed22b7391ace15f

Subnet IDs [Info](#)

Select the subnets in which to create the transit gateway VPC attachment.

us-east-1a

subnet-036ae667916ae75c1

us-east-1b

subnet-0d9ec21a1b90972c3

6. Create Transit Gateway Multicast Domain:

Navigate to 'VPC > Transit gateway multicast domains > Create transit gateway multicast domain' check enable IGMP2 support and attach transit gateway. Create the multicast domain.

Create transit gateway multicast domain [Info](#)

A multicast domain controls how traffic flows for all associated subnets. A multicast domain can only be created in transit gateway with the multicast support option enabled.

Details

Name tag - *optional*

Creates a tag with the key set to Name and the value set to the specified string.

transit-gateway-multicast-domain-01

Transit gateway ID [Info](#)

tgw-061064e44de57c203

Configure the transit gateway multicast domain

IGMPv2 support [Info](#)

Static sources support [Info](#)

Auto accept shared associations [Info](#)

7. Set up EC2 Host:

Navigate to 'EC2 > Instances > Launch an instance' and select your VPC.

▼ **Network settings** [Info](#)

VPC - required | [Info](#)

vpc-0aed22b7391ace15f (nau-multicast) 10.99.0.0/16 ↻

Subnet | [Info](#)

subnet-036ae667916ae75c1 nau-public1 ↻ [Create new subnet](#)

VPC: vpc-0aed22b7391ace15f Owner: 814304444943 Availability Zone: us-east-1a
Zone type: Availability Zone IP addresses available: 16376 CIDR: 10.99.0.0/18

Auto-assign public IP | [Info](#)

Disable ↻

Make sure inbound SSH and HTTPS traffic is enabled.

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0) Remove

Type Info	Protocol Info	Port range Info
ssh ↻	TCP	22
Source type Info	Source Info	Description - optional Info
Anywhere ↻	<input type="text" value="0.0.0.0/0"/> ×	e.g. SSH for admin desktop

▼ Security group rule 2 (TCP, 443, 0.0.0.0/0) Remove

Type Info	Protocol Info	Port range Info
HTTPS ↻	TCP	443
Source type Info	Source Info	Description - optional Info
Anywhere ↻	<input type="text" value="0.0.0.0/0"/> ×	e.g. SSH for admin desktop

Add an additional inbound rule for 'Custom UDP' over port range '5001 - 5019' from the source '10.99.0.0/16'

sgr-058a0464e12fb06f3

<input type="text" value="Custom UDP"/> ↻	UDP	<input type="text" value="5001 - 5019"/> ↻	<input type="text" value="Cust..."/> ↻	<input type="text" value="10.99.0.0/16"/> ×	<input type="text"/>	Delete
--	-----	---	---	--	----------------------	---------------------

Navigate to 'VPC > Elastic IP Addresses > Allocate Elastic IP Address' and allocate and associate Elastic IP to the new EC2 Instance.

Configure DNS using the provider of choice with this new Elastic IP Address.

8. Set up EC2 Audio Generator:

Navigate to 'EC2 > Instances > Launch an instance' and select your VPC.

▼ **Network settings** [Info](#)

VPC - required | [Info](#)

vpc-0aed22b7391ace15f (nau-multicast)
10.99.0.0/16

Subnet | [Info](#)

subnet-036ae667916ae75c1 **nau-public1**
VPC: vpc-0aed22b7391ace15f Owner: 814304444943 Availability Zone: us-east-1a
Zone type: Availability Zone IP addresses available: 16376 CIDR: 10.99.0.0/18

Auto-assign public IP | [Info](#)

Disable

Configure inbound security as per the following rules:

Inbound rules (2) [Manage tags](#) [Edit inbound rules](#)

Q Search

Name	Security group r...	IP version	Type	Protocol	Port range	Source
-	sgr-08006af56670e...	IPv4	SSH	TCP	22	0.0.0.0/0
-	sgr-078553faf5e7d3...	IPv4	Custom UDP	UDP	5000	10.99.0.0/16

Navigate to 'VPC > Elastic IP Addresses > Allocate Elastic IP Address' and allocate and associate Elastic IP to the new EC2 Instance.

9. Create Transit Gateway Multicast Domain Associations:

Navigate to your Transit Gateway Multicast Domain and create 1 association per public subnet within your VPC.

Associations (2) [info](#) [Actions](#) [Create association](#)

Q Find association by attribute or tag

<input type="checkbox"/>	Subnet ID	Attachment ID	Resource type	Resource ID	Resource owner...	State
<input type="checkbox"/>	subnet-00dd9201208d940...	tgw-attach-0376c9c81953...	VPC	vpc-0aed22b7391ace15f	814304444943	✔ A
<input type="checkbox"/>	subnet-036ae667916ae75c1	tgw-attach-0376c9c81953...	VPC	vpc-0aed22b7391ace15f	814304444943	✔ A

10. Create Multicast Groups:

Navigate to your Transit Gateway Multicast Domain. Select groups and add members based on your specific needs. Select both network interfaces and provide a multicast IP address to enable.

Add group members [Info](#)

Adding a member to a multicast group enables the network interface to receive multicast traffic sent by the sources of the multicast group.

Details

Transit gateway ID
tgw-061064e44de57c203

Group IP address
Requires a valid IPv4 or IPv6 IP Address in the 224.0.0.0/4 or ff00::/8 CIDR range.

Available network interfaces (2) [Info](#)

Refresh Create network interface

<input type="checkbox"/>	Name	Network interface ID	Subnet ID	Availability Zone	Status	Instance ID	VPC ID
<input type="checkbox"/>	-	eni-0b71b9ca4f9d1cf96	subnet-036ae667916ae75c1	us-east-1a	in-use	i-06f5286c4f4fc5ed9	vpc-0aed22b7391ace15f
<input type="checkbox"/>	-	eni-07c7874471e1d4c03	subnet-036ae667916ae75c1	us-east-1a	in-use	i-0835fc3c16abbffd3	vpc-0aed22b7391ace15f

Cancel Add group members

11. Disable Source Destination Check:

Navigate to 'EC2 > Instances' select the 'Actions' dropdown. In the networking tab click 'Change source/destination check', check 'Stop', and save the changes.

Instances (1/2) [Info](#)

Last updated less than a minute ago Refresh Connect Instance state Actions Launch instances

All states

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check
<input type="checkbox"/>	nau-host	i-06f5286c4f4fc5ed9	Stopped	t2.micro	-
<input checked="" type="checkbox"/>	nau-generator	i-0835fc3c16abbffd3	Stopped		

[i-0835fc3c16abbffd3 \(nau-generator\)](#)

[Details](#) [Status and alarms](#) [Monitoring](#) [Security](#) [Net](#)

Instance summary [Info](#)

Instance ID Public IPv4 address Private IPv4 addresses

- Connect
- View details
- Manage instance state
- Instance settings
- Networking**
- Security
- Image and templates
- Monitor and troubleshoot

- Attach network interface
- Detach network interface
- Connect RDS database
- Disaster recovery for your instances
- Change source/destination check**
- Disassociate Elastic IP address
- Manage IP addresses
- Manage ENA Express
- Manage bandwidth

Change Source / destination check ✕

The source / destination check ensures that the instance is the source or destination of all the traffic it sends and receives. Each EC2 instance performs source and destination checks by default. [Learn more](#)

Instance ID
 `i-0835fc3c16abbffd3` (nau-generator)

Network interface
 `eni-07c7874471e1d4c03`

Source / destination checking
Stop to allow your instance to send and receive traffic when the source or destination is not itself.

Stop

[Cancel](#) [Save](#)

Multicast Traffic should now be successfully enabled across your EC2 instances. Note traffic will only come through on ports with inbound traffic enabled via the security wizard. The ports and IPs used in this guide are relevant to the application we created.

Hanko Cloud:

Navigate to cloud.hanko.io and create a new Hanko project.

Select project type

Select the project type based on your requirements. This cannot be changed later, but you can always create another project.

Hanko

Authentication and user management

- Onboard and authenticate users with a range of login options, including passkeys, social logins, and enterprise SSO
- Customizable UI components for registration, login and the user profile
- Admin dashboard

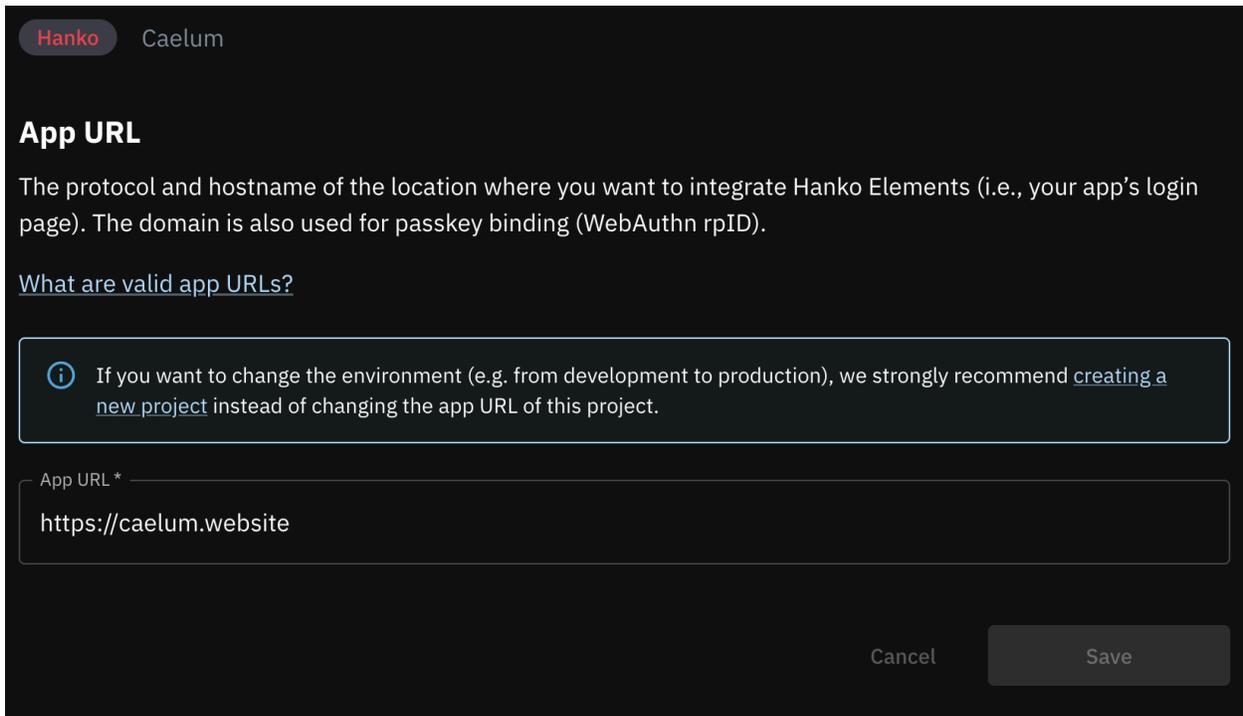
Passkey API

Passkey infrastructure

- Integrate passkeys into any app
- Supports passkey creation, authentication, and transaction use cases
- A managed FIDO2-certified WebAuthn server API

[Create project](#)

Set the app URL to the domain name or 'localhost:443'.



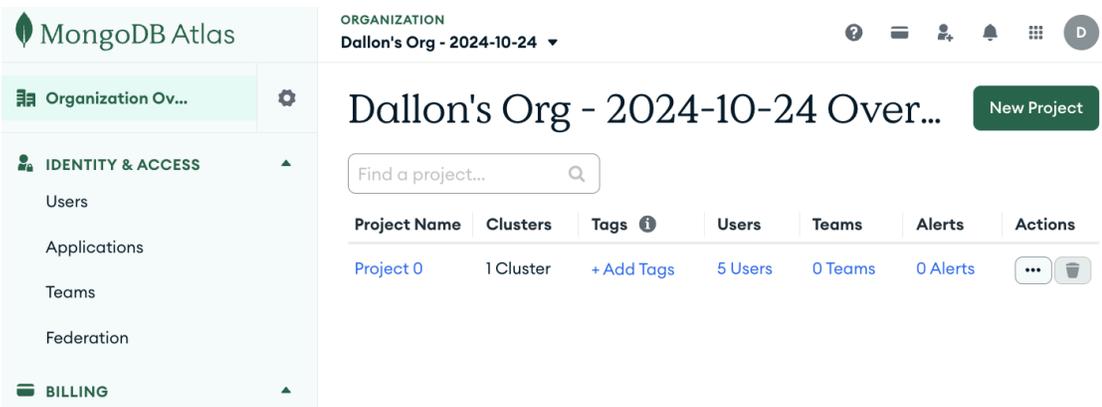
The screenshot shows the Hanko Caelum interface for configuring the App URL. At the top, there's a header with 'Hanko' and 'Caelum'. Below that, the section is titled 'App URL'. A descriptive text explains that the protocol and hostname are used for integration and passkey binding. A link 'What are valid app URLs?' is provided. A warning box states that changing the environment (e.g., from development to production) is best done by creating a new project rather than changing the app URL. A text input field labeled 'App URL *' contains the value 'https://caelum.website'. At the bottom right, there are 'Cancel' and 'Save' buttons.

Store the API url in the Dashboard page for the '.env' file on the host machine.

API URL: `https://65b795cd-6728-46f7-9d07-55dbb42b3c8a.hanko.io` 

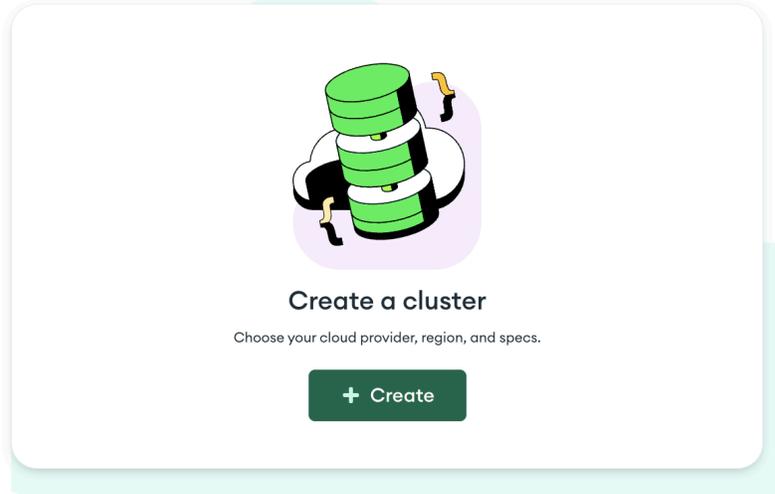
MongoDB:

1. Navigate to mongodbatlas.com and log into the cloud console.
2. Once logged in, navigate to the top right of the page and click on [New Project](#)



3. Give the project a useful name such as Capstone and hit next then Create Project.
4. Once the project is created, you will be able to create your database. Click on Create

Capstone Overview



5. Choose the Free Tier Cluster, name your cluster the name of the application, your preferred provider, and the Region that is closest to the location of server hosting your project. Then hit Create Deployment

Deploy your cluster

Use a template below or set up advanced configuration options. You can also edit these configuration options once the cluster is created.

Cluster Type	Price	Description	Storage	RAM	vCPU
M10	\$0.08/hour	Dedicated cluster for development environments and low-traffic applications.	10 GB	2 GB	2 vCPUs
Flex	From \$0.011/hour <small>Up to \$30/month</small>	For application development and testing, with on-demand burst capacity for unpredictable traffic.	5 GB	Shared	Shared
Free	Free	For learning and exploring MongoDB in a cloud environment.	512 MB	Shared	Shared

Free forever! Your free cluster is ideal for experimenting in a limited sandbox. You can upgrade to a production cluster anytime.

Configurations

Name
You cannot change the name once the cluster is created.

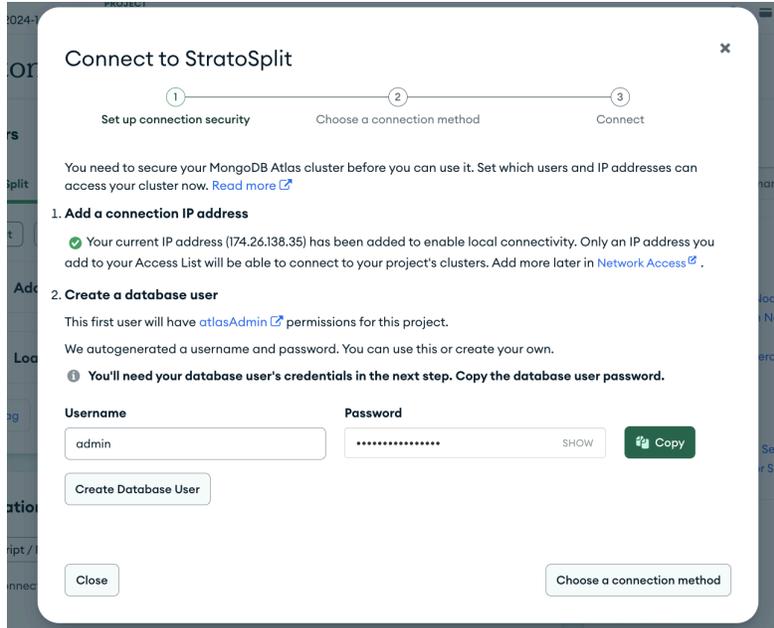
Provider
 AWS Google Cloud Azure

Region
 N. Virginia (us-east-1)
★ Recommended Low carbon emissions

Quick setup

Automate security setup Preload sample dataset

6. Create your user account that will run as the administrator. Make sure to remember this password, it can be reset later if forgotten. Then hit **Create Database User**.



7. For the connection method, choose Drivers and copy step 3 and paste that into the .env file
8. For the last step, on the left hand side, click on **Network Access** and edit the IP address in the options and change it to either 0.0.0.0/0 or to your server's IP address.

IP Access List

+ ADD IP ADDRESS

! You will only be able to connect to your cluster from the following list of IP Addresses:

IP Address	Comment	Status	Actions
174.26.138.35/32	Created as part of the Auto Setup process	● Active	EDIT DELETE

Machine 1 Host:

1. Update System Packages:

```

.ssh — ubuntu@ip-10-99-36-135: ~ — ssh -i NAU_SOCGAS.pem ubuntu...
ubuntu@ip-10-99-36-135:~$ sudo apt update && sudo apt upgrade -y

```

2. Pull Github Repository:

```
[ubuntu@ip-10-99-63-138:~]$ git clone https://github.com/StratoSplit/Caelum.git
Cloning into 'Caelum'...
remote: Enumerating objects: 323, done.
remote: Counting objects: 100% (323/323), done.
remote: Compressing objects: 100% (199/199), done.
remote: Total 323 (delta 163), reused 258 (delta 111), pack-reused 0 (from 0)
Receiving objects: 100% (323/323), 18.15 MiB | 37.54 MiB/s, done.
Resolving deltas: 100% (163/163), done.
ubuntu@ip-10-99-63-138:~$
```

3. Install Node js and Dependencies:

Install Node

```
ubuntu@ip-10-99-63-138:~$ sudo apt install -y nodejs
```

Install base dependencies and run fix

```
[ubuntu@ip-10-99-63-138:~]$ cd Caelum/app
[ubuntu@ip-10-99-63-138:~/Caelum/app]$ npm i
```

```
ubuntu@ip-10-99-63-138:~/Caelum/app$ npm audit fix
```

Install OS specific dependencies

```
.ssh — ubuntu@ip-10-99-63-138: ~/Caelum/app — ssh -i NAU_SOCGAS....
[ubuntu@ip-10-99-63-138:~/Caelum/app]$ npm install dotenv bcrypt
```

4. Set up .env:

Use your personal API URLs to set up the .env file.

```
GNU nano 7.2 .env
MONGO_URI=mongodb+srv://root:NokkikBSFJJp1WvA@capstone.zgone.mongodb.net/?retryWrites=true&w=majority
MONGO_DB_NAME=Caelum-Dallon
HANKO_API_URL=https://65b795cd-6728-46f7-9d07-55dbb42b3c8a.hanko.io
SSL_KEY_PATH=./key.pem
SSL_CERT_PATH=./cert.pem
```

5. Manually configure first admin account:

*User data was configured using MongoDB Compass connected to the database.

```
1  _id: ObjectId('67e5acd9a7dea2310b86695c')
2  userId: "ea2eb43f-a7e1-4723-a8d7-f546bafc5861"
3  username: "nolan"
4  email: "nolannew259@gmail.com"
5  lastLogin: 2025-03-27T21:55:26.052+00:00
6  createdAt: 2025-03-27T19:54:01.820+00:00
7  role: "admin"
8  team: "67da11b0dc8cdfec242b7dff"
```

Role was manually set to “admin”.

6. Run node server:

```
ubuntu@ip-10-99-63-138:~/Caelum/app$ sudo node server.js
```

Machine 2 Audio Stream Generator:

1. Update System Packages:

```
.ssh — ubuntu@ip-10-99-36-135: ~ — ssh -i NAU_SOCGAS.pem ubuntu...
ubuntu@ip-10-99-36-135:~$ sudo apt update && sudo apt upgrade -y
```

2. Install Python3 and pip:

```
.ssh — ubuntu@ip-10-99-36-135: ~ — ssh -i NAU_SOCGAS.pem ubuntu...
ubuntu@ip-10-99-36-135:~$ sudo apt install -y python3 python3-pip
```

3. Pull Github Repository:

```
.ssh — ubuntu@ip-10-99-36-135: ~ — ssh -i NAU_SOCGAS.pem ubuntu...
ubuntu@ip-10-99-36-135:~$ git clone https://github.com/StratoSplit/Caelum.git
```

4. Run stream_audio.py:

```
.ssh — ubuntu@ip-10-99-36-135: ~/Caelum/audio_stream — ssh -i NAU_...
[ubuntu@ip-10-99-36-135:~$ cd Caelum/audio_stream/
[ubuntu@ip-10-99-36-135:~/Caelum/audio_stream$ python3 stream_audio.py
Listening for pings on 239.0.0.11:5000...
█
```

Configuration and Daily Operation

In the last section, you hopefully ended with the client being able to log into (or connect to, or whatever) the installed product. In this section, you will detail whatever tasks need to be done to get the product deployed and operational. Details depend on the individual product but might include steps like “Configure admin user profile and password”, “Create user accounts”, etc. This is the bulk of your user manual, and should simply cover any tasks the client may need to do (while consulting this manual) on a regular basis to operate the product.

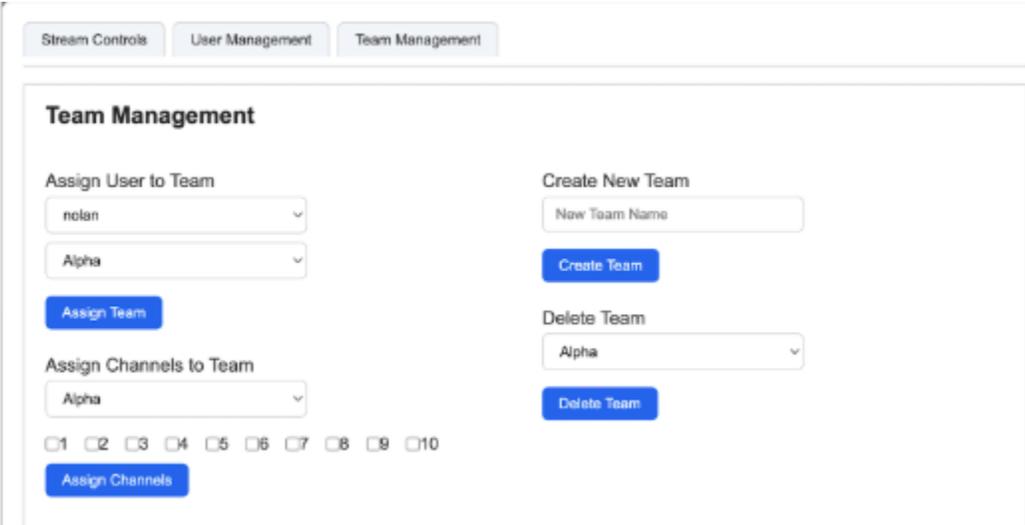


Image 1

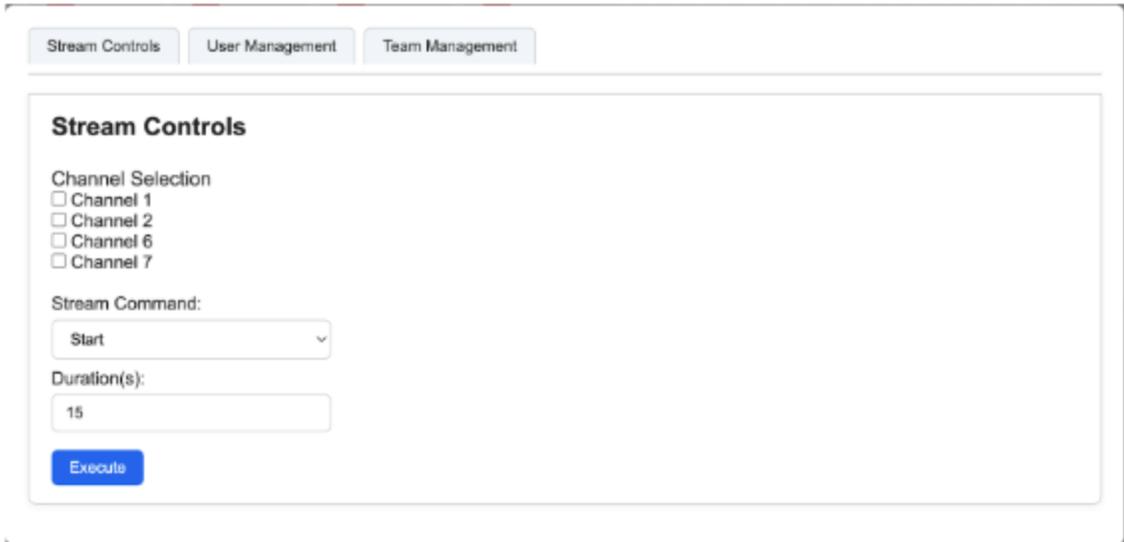


Image 2

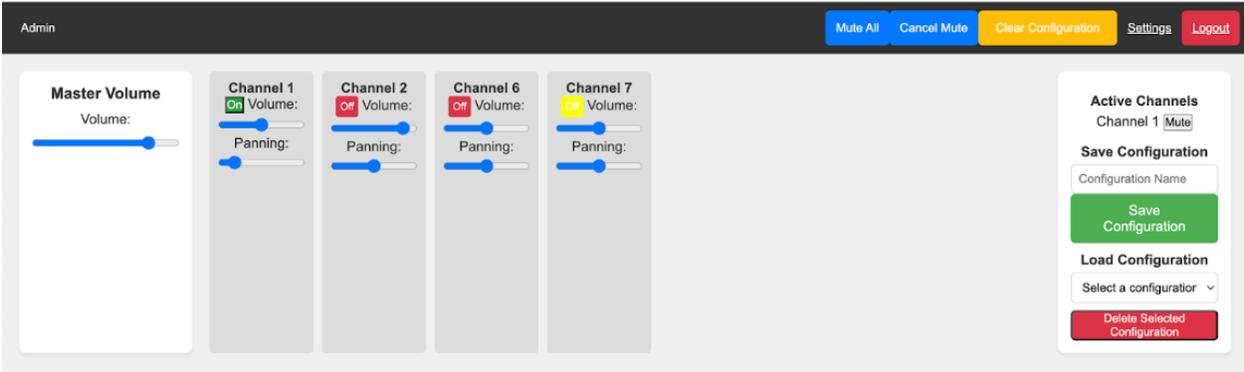


Image 3

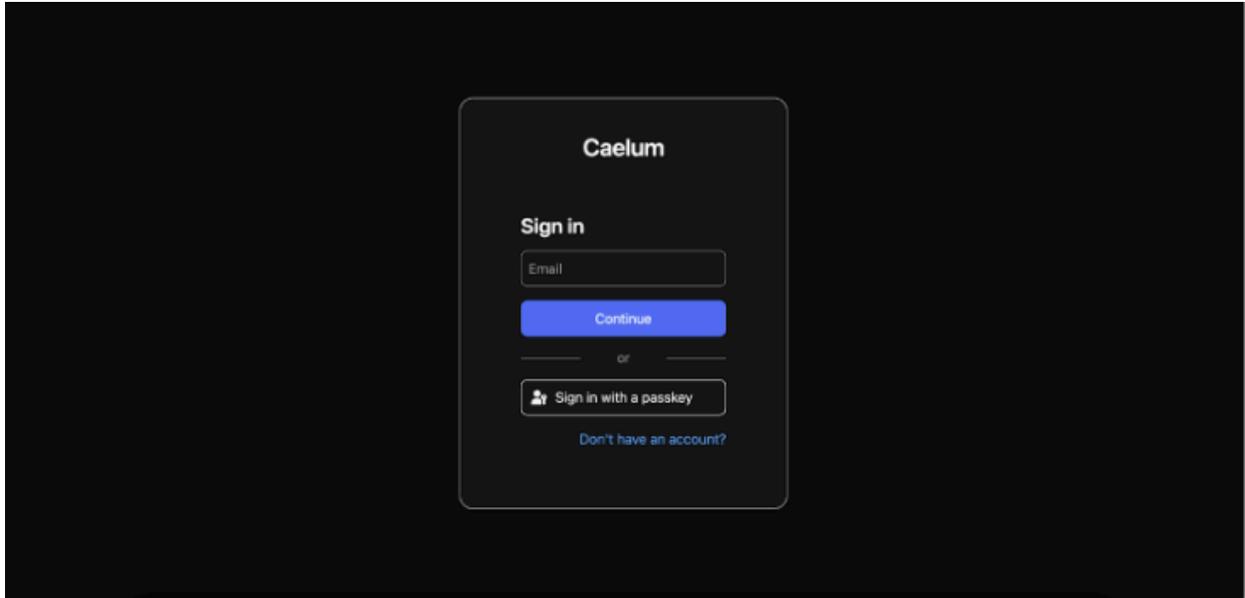


Image 4

Assigning user to a team

- Enter the admin panel in team management use the drop-down menu to assign a specific user to a specific team(image 1)

Creating a team

- Enter the admin panel under team management and enter team name into new team name box and press Create Team button(image 1)

Deleting Teams

- Enter the Admin Panel under Team Management and select team name in dropdown then press Delete Team button(image 1)

Assigning Channels to a team

- Enter the Admin Panel under Team Management and select the team from the drop down. Press channels required then, Assign Channels button(image 1)

Start Streams

- Enter admin panel under Stream Controls select streams out of currently available then enter duration and press Execute button.(Image 2)

Create Configuration

- After configuring dashboard as preferred enter configuration name and press save configuration(image 3)

Load Configuration

- Select saved configuration under drop down menu(image 3)

Deleting configuration

- Load configuration and press Delete Configuration button below it(image 3)

Controlling volume

- Volume can be controlled in a multitude of ways including; changing the master volume of the website, controlling individual channel audio using volume bar, mute all channels using mute all button. Can be saved using configurations(image 3)

Using Panning audio

- Panning can be controlled using a panning bar below the volume bar. Can be saved using configurations(image 3)

Login to website

- Enter website url and sign in using passkey, face id, or touch id(image 4)

Maintenance

1. System Updates (EC2 Instances)

Both EC2 instances—host console and audio generator—run Ubuntu and depend on up-to-date system packages for stability and security.

SSH into each instance and run:

```
sudo apt update && sudo apt upgrade -y
```

2. Dependency Maintenance (Node.js and Python)

StratoSplit uses Node.js and Python for its backend and audio streaming services. Keeping dependencies current ensures security patches and compatibility with evolving system libraries.

```
npm outdated
```

```
npm audit fix
```

```
pip list --outdated
```

3. Authentication Token Policy (Hanko)

Passwordless authentication is handled through Hanko, which issues session tokens to users. These tokens may expire or require policy updates.

Log in to the Hanko Cloud Console, navigate to your project settings, and review the current token expiration policies. If necessary, update token lifespans, revoke inactive users, or reset credentials through the Hanko dashboard or the MongoDB users collection.

Troubleshooting

AWS:

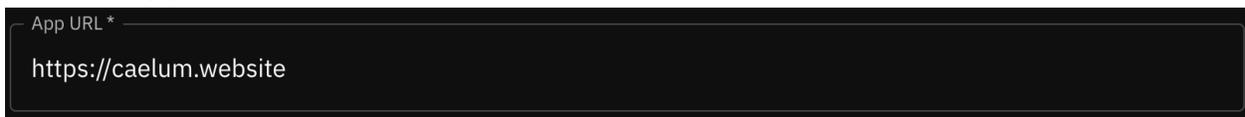
In the case that you have set up the AWS infrastructure as specific yet multicast traffic is still not enabled ensure that you disable source/destination checking and your inbound traffic rules are properly configured.

Node js:

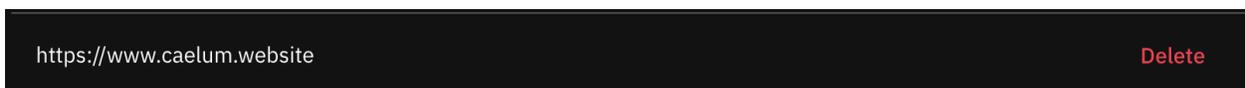
Node may be prone to various issues during set up. For example, 'Bcrypt', a package we are using, has different versions depending on the host operating system. These must be manually installed outside of running the normal "npm install" command. Refer to the 'Machine 1 Host' step 3 to see these packages. Further, packages may be outdated depending on the version of Node and npm you are running. To fix these refer to the "Dependency Maintenance" section. Lastly, if you are still having issues setting up the web application, check that your '.env' file is configured properly.

Hanko API:

When interfacing with Hanko Cloud strict CORS policies on certain browsers such as Chrome may cause problems. In order to use this system without overriding browser security policies, the console web app must be associated with a domain name. Within Hanko Cloud it is important to make sure your app url is simply the domain name without any prefixes or suffixes as seen in the screenshot below.



Beyond just this you must also add the domain with the prefix 'www.' to the allowed origins in order to ensure compatibility across all modern browsers as seen in the screenshot below.



Testing:

The Jest testing suite must be run in the "/app" subfolder of the application in order to run correctly. The web ui, to help visualize the successful tests is not functional, so the command line test coverage is the most effective way to visualize results. This command line visualization is enabled by default. Test results can also be viewed through the github web interface.

Conclusion

Thank you for choosing StratoSplit as your secure audio simulation and management platform. This user manual was developed to empower your organization with the tools and knowledge needed to confidently deploy, operate, and maintain the system in real-world contexts. StratoSplit was engineered with mission-critical environments in mind, combining modern web technologies with secure authentication, multicast audio streaming, and responsive dashboard controls. We hope this product provides you with good performance, ease of use, and flexibility to adapt to your specific needs.

With best wishes from your StratoSplit development team:

Sam Cain

Nolan Newman

Dallon Jarman

Elliot Hull

While we are all moving on to professional careers, we'd be happy to assist with brief questions in the coming months to help ensure that StratoSplit is successfully integrated and optimized for your operations. We wish you continued success in your mission and are proud to have contributed to your technological capabilities