How to set up remote access for your S-PLAY

Create a convenient, remote access system allowing you or your clients to connect to your S-PLAY from around the world.

Security Note – Internet Connection

- Before connecting your S-PLAY to the Internet ensure your local network firewall provides security all devices have been adequately secured.
- If ever unsure consult a qualified professional.
- Ensure you have sufficient extra bandwidth to deal with influxes of traffic caused by an internet connection.
- Ensure your SSH Tunnel is configured in such a way to ensure only trusted users can access the tunnel to remotely configure the S-PLAY.

Introduction

In this application note, we are going to learn how to set up a simple remote access system for the S-PLAY alongside using SSH Tunnelling and reviewing other options. The goal is to create a system where we or our customer can connect from a laptop/PC/smartphone from anywhere we have internet access in case we want manual control of our shows.

For the purposes of this guide, we are going to assume that you have already programmed your S-PLAY with your desired cues and playlists – we will be focussing more on the necessary network structure and actual setup.

A Not secure | 3.12.104.225:8080/en/home ENTTEC EN CN Login Home Cue Library Events Triggers Playlists Scheduler Settings Status Backup Feb 11 2021 21:48:34 PM 1 noiseflpl 00:01.4 2 trispl 00,06 3 plasm 00:06 4 rainbowscroll 00:26 5 whitetest 100 Stopped 00:13 All Playlists Pages < 1/2 > 5 -Display Schedulers No Registered Schedules

By the end of this process, we are going to be able to connect to our S-PLAY remotely and see something like this:

1 - S-PLAY - remote access homepage

As you can see this is just the default S-PLAY home page.

What's different is the webpage URL at the top of the screen. We are connecting over the internet through a server with IP address (in this case 3.12.104.225), whilst our S-PLAY is on a completely different address on its local network.

This application note features step by step instructions on how to set up this remote access method with an AWS cloud server. Using these principles, you may choose to set up your server with a different service using this application note for reference.

11 enttec.com

ID: 5930032

Getting started

Requirements.

Before you begin, we will need to have the following:

- 1. S-PLAY with Internet access this can be through a 4G router or just by being connected to a network with internet access.
- 2. AWS account you can sign up for a free account with AWS here: <u>https://aws.amazon.com/</u>
- 3. A computer connected to the S-PLAY and internet so you can set up the remote access function.
- 4. (Optional) a smartphone or other internet connected device that you can use to test the remote access function once it is set up.

Remote connection options + network structure

Simple remote connection options.

If you have worked with other network-based devices and control systems before you are probably already familiar with some other remote access methods including:

- Remote Desktop Access through a local computer using a service like TeamViewer, LogMeIn, or RealVNC.
- Setting up port forwarding on a 4G router.

This remote access function, however, is designed to streamline the process for the end-user so they can use a simple URL and connect from anywhere, providing they have secure internet access. A high-level diagram of this application can be seen below:



2 - Remote access network structure

As you can see, this method uses an AWS cloud server as the intermediary to connect your device to the S-PLAY. This seems a bit counter-intuitive... why use a separate web server to make this connection? Why can't we just connect over the internet straight to the S-PLAY?

Well, we can, using the 2 methods listed before. Let's take a look at those:

21 enttec.com

Remote Desktop Apps

The most straight forward way to connect remotely is to use an app like TeamViewer or RealVNC to give access to a PC on the same network as the S-PLAY that you can treat as if you are on the same network:



3 - Remote desktop network structure

As you can see, this method requires that we have a PC on-site that is connected to our lighting control network. The remote desktop apps will connect us to the PC, and then using that remote connection, we then navigate through the on-site PC to connect to our S-PLAY as if we were there in person.

The limitation of this method is that we need to have a PC on site, and it needs to be on all the time if we are to connect to it remotely at any time.

Port forwarding on 4G routers

How about 4G routers? You can get 4G routers inexpensively and add a data SIM card to them to allow remote internet connections. You can also then set up a port forwarding rule so that whenever you connect to that router, you are re-directed to the S-PLAY



4 - Port forwarding network structure

The limitation with this method is that you need a public IPv4 address on your 4G router. Depending on where you are and what your ISPs can provide, this might be a bit difficult. For example, here in Australia, most mobile services use CGNAT which means your public ip can change many times in a hour, so you may have to get specific, and much more expensive business internet plans to get a fixed IP.

This brings us to the method using the S-PLAYs new remote connection feature. Using a separate web server to help with the connection eliminates the need for an expensive business-level data plan like we needed for port forwarding. Instead, we'll set up a cloud server once, then the S-PLAY will give us a URL that we can use to connect to it from anywhere in the world as long as we and the S-PLAY both have internet access. Stay tuned as we'll be running through how to set up this cloud server later on.

4 | enttec.com

ID: 5930032

Setting up the S-PLAY

Firstly, let's update our S-PLAY and see how this all works. In Settings, select Remote in the menu, we'll see a section titled: "Remote Access" It's asking for an IP Address, port number, username and SSH Key. These are all obtained when we set up our virtual server.

	DMX settings			~
⊏⊉ INFO	유 Network setting	iz		~
❶ OUTPUTS	$\downarrow \rightarrow$ Sync settings			~
() ARTNET				
SACN	S Remote Access			^
DMX		Enable	· • •	
윪 NETWORK		IP	0.0.0.0	
. ⇒ SYNC			8080	
REMOTE		Remote port	0000	
𝔇 DATE & TIME		Username	ec2-user	
O LOCATION		SSH Key	⊂⊉ SHOW INPUT	
PLAYBACK				
♂ FIRMWARE			C OPDATE	
ϕ reset	O Date & time set	tings		~
	O Location setting	gs		~
	Playback config	uration		~
	ে Firmware updat	e		~
	🤣 Factory reset			~

5 - S-PLAY remote access settings

We'll come back to this later once we have created our AWS server.

51 enttec.com

ID: 5930032

Setting up the cloud server

1. We'll be using Amazon Web Services as an example on how to set up a simple cloud server for remote connection. We won't go through how to make an account – that's straight-forward, but once you've created a free AWS account, you'll want to log in and look through the various services being offered. We need a "Compute" service for this function, and we'll use the EC2 version since it's free tier eligible and has the functionality we need.

Agender integrand Ag		Featured Services Analytics	Featured Services	Resources and Media	What's New on AWS	
Configuration Configuration Configuration Configuration <td></td> <td>Blockchain</td> <td>Virtual servers in the cloud</td> <td></td> <td>See announcements for AWS</td> <td></td>		Blockchain	Virtual servers in the cloud		See announcements for AWS	
Curacia Curacia Significant Curacia Curatives Significant Curacia Curacia Curacia S		Cloud Financial Management	Scalable storage in the cloud	Customer Enablement		
Solutions Normageneric Solutions Amazona DS Generic Amazona DS Generic Amazona DS Machine Lawrando Amazona DS Machine Lawra		Contact Center Containers	High performance managed relational database with full MySQL and PostgreSQL compatibility	Complete your projects faster with help from AWS Certified	Operate your AWS	
Internet of Things AVS Lambds Machine Learning Reversance Marganemet & Governance Reversance Media Services Contact the Servers Migration & Transfer Maccon VSE Media Services Contact the Servers Modia Services Contact the Servers Modia Services Contact the Servers Modia Services Contact the Servers Services Services Services Contact the Servers Services Services Solutions Pricing Documentation Learn Partner Network AWS Marketplace Customer Enablement Events Explore More Q Amazon EC2 Ourvier Pricing Toocamentation Learn Partner Network AWS Marketplace Customer Enablement Events Explore More Q Amazon EC2 Ourvier Pricing Toocamentation Learn Partner Network AWS Marketplace Customer Enablement Partner Network AWS Marketplace Socurate and pericable compute capacity for virtually any workhoad Resources Scenaptic Pricing Toocamentation Learn Partner Network AWS Marketplace Scenaptic Reverse Scenaptic Pricing Toocamentation Learn Partner Network AWS Marketplace Scenaptic Reverse Scenaptic Pricing Toocament		End User Computing Front-End Web & Mobile	Managed NoSQL database Amazon RDS Managed relational database service for MySQL, PostgreSQL,	Accelerate your business	Certification Build and validate your skills	
Amazon EC2 Ownerwine Pricing Instance Types * FAQs Getting Started Resources * <u>Compute</u> Secure and resizable compute capacity for virtually any workload 750 hours per month 		Management & Governance Media Services Migration & Transfer Networking & Content Delivery Quantum Technologies Robotics Satellite Security, Identity, & Compliance Serverless	Amazon VPC Isolated doud resources Amazon Lightsail Launch and manage virtual private servers Amazon SageMaker			
	~	Amazon EC2 Overview Feature <u> « Compute</u> Amazon EC2	s Pricing Instance Types • FAQs Getting Started R pute capacity for virtually any workload Connect with an Amazon EC2 specialist	esources → 750 hours per for 12 months with th	month	WS Account

6 - AWS Server type selection

61 enttec.com

ID: 5930032

2. Next, we'll go to "Launch Instance" to create a new server instance.

Services Q Search Services Q Search New EC2 Experience Tell us what you think	Resources			EC2 Global view 🔀 📿 🕲	
EC2 Dashboard	You are using the following Amazon EC2 resources in the Asia	Pacific (Sydney) Region:			
EC2 Global View	Instances (running) 0		Dedicated Hosts	0 Elastic IPs	
Events Tags	instances (running) 0	Auto scaling Groups 0	Dedicated hosts	U Etastic IPS	
Limits	Instances 0	Key pairs 0	Load balancers	0 Placement groups	
Instances	Security groups 1	Snapshots 0	Volumes	0	
Instances Instance Types	Easily size, configure, and deploy Microsoft SQL Server	Always On availability groups on AWS using the AWS Launch W	izard for SQL Server. Learn more	×	
Launch Templates Spot Requests Savings Plans	Launch instance To get started, launch an Amazon EC2 instance, which is a virtual server	in the cloud.	Service health	C AWS Health Dashboard	
Reserved Instances Dedicated Hosts Capacity Reservations	Launch instance V Migrate a server 🖄		Region Asia Pacific (Sydney)	Status This service is operating normally	
Images	Note: Your instances will launch in the Asia Pacific (Sydney) Region		Zones		
AMIs			Zone name	Zone ID	
AMI Catalog	Scheduled events	C	ap-southeast-2a	apse2-az3	
Elastic Block Store					
inapshots	Asia Pacific (Sydney) No scheduled events		ap-southeast-2b	apse2-az1	
ifecycle Manager			ap-southeast-2c apse2-a22		
Network & Security Security Groups	Migrate a server		Enable additional Zones		
Elastic IPs Placement Groups Key Pairs Network Interfaces	Use AWS Application Migration Service to simplify and expedito AWS. Get started with AWS Application Migration Service 🖸	te migration from physical, virtual, and cloud infrastructure			
Load Balancing Load Balancers Target Groups	Quick ID filter				
Auto Scaling Launch Configurations	Enter a resource ID				
Auto Scaling Groups					

7 - AWS – Launch Instance

3. Create a name for this instance and for the Application and OS Images, we'll just chose Amazon Linux, again because it's free tier.

	Services	Q Search	[Alt+S]
E	EC2 〉 Instar	nces > Launch an instance	
	Launch	an instance un	
		illows you to create virtual machines, or instances, that run on the AWS Cl	oud. Quickly get started by
		simple steps below.	
	Name an	nd tags Info	
	Name		
	e.g. My We	eb Server	Add additional tags
		cation and OS Images (Amazon Machine Image) Info	
		s a template that contains the sortware comguration (operating system, application s our instance. Search or Browse for AMIs if you don't see what you are looking for below	
	0 50	arch our full catalog including 1000s of application and OS images	
	Q 360		
	Rece	ents Quick Start	
		azon macOS Ubuntu Windows Red Hat !	Q
		azon macOS Ubuntu Windows Red Hat !	Q Browse more AMIs
	Lin	NS Ubuntu [®] Microsoft	Including AMIs from
	Lin		
	Lir	NS Ubuntu [®] Microsoft	Including AMIs from AWS, Marketplace and
	Amazon	NS ubuntu® Microsoft	Including AMIs from AWS, Marketplace and
	Amazon Amazon ami-0d	ukuntu [®] Microsoft Red Hat Machine Image (AMI) Imachine Image (AMI) Imachine Image (AMI)	Including AMIs from AWS, Marketplace and the Community Free tier eligible
	Amazon Amazon ami-0d	INACHINE Image (AMI)	Including AMIs from AWS, Marketplace and the Community Free tier eligible
	Amazon Amazon ami-0d	INAL INTERNATIONAL INTERNATION	Including AMIs from AWS, Marketplace and the Community Free tier eligible
	Amazon Amazon Amazo ami-odt Virtuali	INAL INTERNATIONAL INTERNATION	Including AMIs from AWS, Marketplace and the Community Free tier eligible
	Amazon Amazon Amazo ami-odt Virtuali	In Linux 2023 AMI 2023.0.20230329.0 x86_64 HVM kernel-6.1	Including AMIs from AWS, Marketplace and the Community Free tier eligible
	Amazon Amazon Amazo urii-Odi Virtuali Descript Amazon	ux Machine Image (AMI) Imachine Imachine Image (AMI) Imachine Imachine	Including AMIs from AWS, Marketplace and the Community Free tier eligible

8 - AWS – Application and OS Image Selection

4. For the Instance type we'll just go with t2 micro because – you guessed it - it's free and we really don't need this to be too powerful for what we need to do.

aws	Services	Q Search				[Alt+S]	
=	▼ Instar	nce type	Info				
	Instance ty	/pe				(All generations
	t2.micro			Free tier eligible	2		
	On-Deman On-Deman On-Deman	nd Windows pr nd SUSE pricing	GiB Memory g: 0.0146 USD per Hour icing: 0.0192 USD per Ho g: 0.0146 USD per Hour g: 0.0746 USD per Hour		•	Compa	re instance types

9 - AWS – Instance Type Selection

5. Key pair is a key file that your S-PLAY will need to be able to connect to the AWS server. **C**reate a new key pair and save this in a safe location. The key pair will be in the form of a **.pem** file which you will need to upload to your S-PLAY in the SSH Key field at the end of the settings.

Note:

- Ensure to keep this file as there is no any way to access it again if the file is lost.
- Disabling remote access on the S-PLAY will wipe all SSH configuration including the **.pem** SSH Key from the S-PLAY for security reasons.

aws	Services	Q Search	[Alt+S]
=		air (login) Info use a key pair to securely connect to your instance. Ensure that you have access to the nce.	e selected key pair before you launch
	Key pair na	me - required	Create new key pair
	Create	key pair ×	
	Enter the and acces	allow you to connect to your instance securely. name of the key pair below. When prompted, store the private key in a secure sible location on your computer. You will need it later to connect to your Learn more 2	
	ENTTEC	_cs	
	Key pair t RSA RSA en ED255 Private ke J.pem For use	crypted private and public key pair	
		Cancel Create key pair	

10 - AWS - key pair creation

81 enttec.com

6. Network Settings is where we add our port settings so that any device can access the server. Click 'Edit' on the right to access more settings.

aws	Q Search [Alt+S]
=	
	▼ Network settings Info
	Network Info
	vpc-055e67a08def82726
	Subnet Info
	No preference (Default subnet in any availability zone)
	Auto-assign public IP Info
	Enable
	Firewall (security groups) Info A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
	Create security group Select existing security group
	We'll create a new security group called 'launch-wizard-1' with the following rules:
	✓ Allow SSH traffic from Helps you connect to your instance 0.0.0.0/0
	Allow HTTPS traffic from the internet To set up an endpoint, for example when creating a web server
	Allow HTTP traffic from the internet To set up an endpoint, for example when creating a web server
	▲ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting × security group rules to allow access from known IP addresses only.

11 - AWS – Network Settings

7. By default, the SSH rule (Port range 22) will be present in Inbound security groups rules, we just need to change the source to "anywhere". In addition to this we need to add exceptions for 4 additional port ranges: 80, 8080, 13133 & 55555 by clicking 'Add security group rule'. These are ports that the S-PLAY will be using to display its web page and allow interactivity to the connecting device.

Inbound security groups rules		
Security group rule 1 (TC	P, 22, 0.0.0/0)	Remove
Type Info	Protocol Info	Port range Info
ssh	▼ТСР	22
Source type Info	Source Info	Description - optional Info
Anywhere	▼ Q. Add CIDR, prefix list or security	e.g. SSH for admin desktop
	0.0.0.0/0 ×	
A Dulas with source of 0.0	0.0/0 - !!	We are a second as the second
	0.0/0 allow all IP addresses to access your ins llow access from known IP addresses only.	tance. We recommend setting X
Add security group rule]	

12 - AWS – Add Inbound Security Group Rules



8. Enter Port Range and change Source Type to 'Anywhere' for each 4 port ranges so that any device can connect to our S-PLAY no matter where they are.

You can improve the security of the system by limiting the source ranges. For example, if you work for an integration business and you are installing S-PLAYs on your clients' projects. You can set the source to be the client's office IP address range. This means only a device in the client's office can access the S-PLAY. You could also set this to your own office IP address range if you were to make changes/updates on your clients' behalf.

Once the rules in the previous section have been set, the new server instance is ready to be launched by clicking the 'Launch instance'.

Services Q Search		[Alt+S]	
launch-wizard-1 created 2	2025-04-12100:19:39.1002		
Inbound security groups ru	ules		 Summary
Security group rule 1	(TCP, 22, 0.0.0.0/0)	Remove	
Type Info	Protocol Info	Port range Info	Number of instances Info
ssh		22	1
			Software Image (AMI)
Source type Info	Source Info	Description - optional Info	Amazon Linux 2023 AMI 2023.0.2read mor
Anywhere	 Add CIDR, prefix list or security 	e.g. SSH for admin desktop	ami-0d9f286195031c3d9
	0.0.0.0/0 ×		Virtual server type (instance type) t2.micro
			Firewall (security group)
Security group rule 2	(TCP, 80, 0.0.0.0/0)	Remove	New security group
Type Info	Protocol Info	Port range Info	Storage (volumes)
Custom TCP	TCP	80	1 volume(s) - 8 GiB
Source type Info	Source Info	Description - optional Info	Free tier: In your first year includes 750
Anywhere	 Add CIDR, prefix list or security 	e.g. SSH for admin desktop	hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable)
	0.0.0.0/0 ×		instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million
			IOs, 1 GB of snapshots, and 100 GB of
Security group rule 3	(TCP, 8080)	Remove	bandwidth to the internet.
Type Info	Protocol Info	Port range Info	
Custom TCP	ТСР	8080	Cancel Launch inst
			Review comm
Source type Info	Source Info	Description - optional Info	
Anywhere	Source Info Q. Add CIDR, prefix list or security		
Anywhere	▼ Q. Add CIDR, prefix list or secure	ity e.g. SSH for admin desktop	
Anywhere Security group rule 4	▼ Q. Add CIDR, prefix list or secure		
Anywhere Security group rule 4 Type Info	▼ Q. Add CIDR, prefix list or secure	ity e.g. SSH for admin desktop	
Anywhere Security group rule 4	 Q. Add CIDR, prefix list or security (TCP, 13133, 0.0.0.0/0) 	ty e.g. SSH for admin desktop Remove	
Anywhere Security group rule 4 Type Info	Q Add CIDR, prefix list or secure (TCP, 13133, 0.0.0.0/0) Protocol Info	ity e.g. SSH for admin desktop Remove Port range Info	
Anywhere Security group rule 4 Type Info Custom TCP	Q Add CIDR, prefix list or secure (TCP, 13133, 0.0.0.0/0) Protocol Info TCP TCP	lty e.g. SSH for admin desktop Remove Port range Info 13133 Description - optional Info	
Anywhere Security group rule 4 Type Info Custom TCP Source type Info	Q Add CIDR, prefix list or secure (TCP, 13133, 0.0.0.0/0) Protocol Info TCP Source Info	lty e.g. SSH for admin desktop Remove Port range Info 13133 Description - optional Info	
Anywhere Security group rule 4 Type Info Custom TCP Source type Info		lty e.g. SSH for admin desktop Remove Port range Info 13133 Description - optional Info	
Anywhere Security group rule 4 Type Info Custom TCP Source type Info	 Add CIDR, prefix list or security (TCP, 13133, 0.0.0.0/0) Protocol info TCP Source info Q Add CIDR, prefix list or security (0.0.0.0/0 ×) 	lty e.g. SSH for admin desktop Remove Port range Info 13133 Description - optional Info	
Anywhere Security group rule 4 Type Info Custom TCP Source type Info Anywhere Security group rule 5	 	Ity e.g. SSH for admin desktop Remove Port range info 13133 Description - optional info ity e.g. SSH for admin desktop Remove	
Anywhere Anywhere Security group rule 4 Type Info Custom TCP Source type Info Anywhere Security group rule 5 Type Info	 Add CIDR, prefix list or security (TCP, 13133, 0.0.0.0/0) Protocol info TCP Source info Q. Add CIDR, prefix list or security (CCP, 55555, 0.0.0.0/0) Protocol info 	Ity e.g. SSH for admin desktop Remove Port range Info 13133 Description - optional Info e.g. SSH for admin desktop Remove Port range Info	
Anywhere Security group rule 4 Type Info Custom TCP Source type Info Anywhere Security group rule 5	 	Ity e.g. SSH for admin desktop Remove Port range info 13133 Description - optional info ity e.g. SSH for admin desktop Remove	
Anywhere Anywhere Security group rule 4 Type Info Custom TCP Source type Info Anywhere Security group rule 5 Type Info	 Add CIDR, prefix list or security (TCP, 13133, 0.0.0.0/0) Protocol info TCP Source info Q. Add CIDR, prefix list or security (CCP, 55555, 0.0.0.0/0) Protocol info 	Ity e.g. SSH for admin desktop Remove Port range info 13133 Description - optional info ty e.g. SSH for admin desktop Remove Port range info S5555 Description - optional info	

13 - AWS - Port Settings & Launch Instance

9. After the instance is successfully created, it will bring us to the "Next Steps" menu. From here we click "Connect to instance" which brings us to this screen showing us the public IP address and Username of our instance.

1 2 3 4 rk gateway or r
rk gateway or
rk gateway or r
rk gateway or r
hOnEC2Inst latchOnEC2Inst bles or disables an EC2 instanc OnEC2Instanc
Sydney 🔻

14- AWS - connect to instance

10. We can enter both these values into the appropriate lines on our S-PLAY remote access settings. Then, open the .pem file created from Step 5 with Notepad and copy the key into the SSH Key field. Click update to ensure those are saved.

Remote Acces	.5		^		
	Enable]
		http://54.252.180.241:8080		ENTTEC_CS.p	
	IP	54.252.180.241			🔏 🗘 🕘 🖻 🗊
	Remote port	8080			 ☆ Add to Favourites ⑦ Compress to Zip file
	Username	ec2-user			Copy as path Ctr Properties Alt
	SSH Key	⊏⊉ SHOW INPUT			Share with Skype
		UPDATE			Show more options sh

15- S-PLAY - update remote access settings



93 - PC - Key pair .pem file to be entered in SSH Key section

11 enttec.com

ID: 5930032



11. The last step in this configuration process is to modify an access setting on our newly generated AWS cloud server, so the S-PLAY can access it. To do this, connect through to your instance. This opens up a new tab and a command prompt window. To update the setting, we've put together a short code segment to go through and make the necessary changes.

Here is the code segment you will require:

/usr/bin/sudo /usr/bin/sed -i -e 's/.*GatewayPorts.*/GatewayPorts yes/g' /etc/ssh/sshd_config /usr/bin/sudo /usr/bin/systemctl restart sshd

aws Services	Q Search [Alt+S]
, #_ ~_ #### ~~ _#####\	Amazon Linux 2023
~~ \### ~~ \#/	https://aws.amazon.com/linux/amazon-linux-2023
~~~ / ~~/ _/_/'	
Last login: Wed Apr	12 03:56:58 2023 from
[ec2-user@ip- [ec2-user@ip- [ec2-user@ip-	<pre>~]\$ /usr/bin/sudo /usr/bin/sed -i -e 's/.*GatewayPorts.*/GatewayPorts yes/g' /etc/ssh/sshd_config ~]\$ /usr/bin/sudo /usr/bin/systemctl restart sshd ~]\$</pre>

16 - AWS - server command prompt window

12. After copying that code segment in, the necessary update is made. We can now go back to our S-PLAY screen and use the given URL to connect remotely. You should notice that the globe icon has now changed to green – indicating that the remote access setting is active and the URL will allow S-PLAY access from your smart phone or any other device from other network.

	Semote Access		^
⊏⊉ INFO	Enable		
❶ OUTPUTS		http://54.252.180.241:8080	
ARTNET			
S SACN	IP	54.252.180.241	
O DMX	Remote p	ort 8080	
윪 NETWORK	Usernam	e ec2-user	
A SYNC			
REMOTE	SSH Key	⊏∳ SHOW INPUT	
⑤ DATE & TIME		<b>DUPDATE</b>	
O LOCATION			
PLAYBACK	O Date & time settings		~
♂ FIRMWARE	Location settings		~
$\phi$ reset	Playback configuration		~

17 - S-PLAY - successfully updated remote connection settings.

#### Remote access multiple S-PLAYs in one server

If you have multiple S-PLAYs, they are allowed to be accessed remotely within the same AWS cloud server. Simply add extra ports in the exiting cloud server by the following guide and configure multiple S-PLAYs to be accessible via one single AWS.

1. Click 'Instance' from the menu on the left, select the existing 'Instance ID' from the list for the additional S-PLAY to be added in. This brings us to the instance summary page showing the instance settings.

ew EC2 X	Instances (2) Info								C	Connect	Instance state 🔻	Actions 🔻 📕	unch instances 🔹 🔻
eperience El us what you think	Q. Find instance by attrib	ute or tag (case-sensitive)											< 1 > @
Dashboard	Name 🔻	Instance ID	Instance state	v Instance type	▼ Status check	Alarm status	Availability Zone 🛛 🔻	Public IPv4 DNS v	Public IPv4	▼ Elastic IP	V IPv6 IPs	v Monitoring	▼ Security grou
Global View	Remote Access	i+0492b92798fbcc3e8		RQ t2.micro	<ul> <li>Initializing</li> </ul>	No alarms 🕇	ap-southeast-2c	ec2-3-26-22-111.ap-so	3.26.22.111	-	-	disabled	launch-wizard
its	ENTTEC	i-093ecb0147a874e3a	Running	QQ t2.micro	⊘ 2/2 checks passed	No alarms 🕂	ap-southeast-2c	ec2-13-54-210-114.ap	13.54.210.114	-	-	disabled	launch-wizard
	4												
s													
inces													
nces													
inces													
nces nce Types													
nces nce Types ch Templates Requests													
nces nce Types ch Templates Requests 1gs Plans													
inces ince Types ich Templates : Requests ngs Plans rved Instances													
nnces Innce Types Inch Templates : Requests Ings Plans													

18 – AWS - Add extra S-PLAY into the existing server from AWS EC2 Menu.

2. In Instance summary page, navigate to 'Security' and select the 'Security Groups'. From here it will open up a page to allow Inbound rules to be edited.

Services Q. Sear	rch	[Alt+S]					D 👃 Ø Sydney
w EC2 X	EC2 > Instances > i-0492b92798fbo	c3e8					
s what you think	Instance summary for i-0492 Updated less than a minute ago	b92798fbcc3e8 (Remote Acce	ss S-PLAY) Info				C Connect Instance state V Acti
ashboard lobal View s	Instance ID i-0492b92798fbcc3e8 (Remote Ar	ccess S-PLAY)		Public IPv4 addre	55		Private IPv4 addresses 7 172.31.24.20
	IPv6 address -			Instance state G Stopped			Public IPv4 DNS -
es	Hostname type IP name: ip-172-31-24-20.ap-southea	st-2.compute.internal		Private IP DNS na	me (IPv4 only) -20.ap-southeast-2.compute.	internal	
es e Types	Answer private resource DNS name IPv4 (A)			Instance type t2.micro			Elastic IP addresses
n Templates equests	Auto-assigned IP address			VPC ID	08def82726 🔀		AWS Compute Optimizer finding ① Opt-in to AWS Compute Optimizer for recommendations.   Learn more [2]
s Plans ed Instances	IAM Role			Subnet ID	i4225ca457627 🔀		Auto Scaling Group name
ed Hosts y Reservations	IMDSv2 Required						
	Details Security Network	ing Storage Status checks	Monitoring	Tags			
talog	▼ Security details						
Block Store	IAM Role			Owner ID D 1413669522	04		Launch time Wed Apr 12 2023 10:40:50 GMT+1000 (Australian Eastern Standard Time)
is ots le Manager	Security groups	vizard-1)					
	▼ Inbound rules						
rk & Security y Groups	Q, Filter rules						<
Ps	Name	Security group rule ID	Port range	Protocol	Source	Security groups	Description
nt Groups		sgr-01a7bfd9565b7522a	22	TCP	0.0.0/0	launch-wizard-1 🔀	-
s		sgr-027916ae7fb6ee2c4	80	TCP	0.0.0/0	launch-wizard-1 🛂	-
k Interfaces		sgr-0955431d10fc0188d	13133	TCP	0.0.0/0	launch-wizard-1 🗹	
alancing	-	sgr-02b7f112c8db3bc2b	8080	TCP	0.0.0/0	launch-wizard-1 🗹	-
alancers		sgr-0ba094989a97c7939	55555	TCP	0.0.0/0	launch-wizard-1	-
Groups	Outbound rules						
icaling	Q. Filter rules						<
ch Configurations							

19 – AWS - Instances configuration summary page.

3. Select 'Inbound rules' tag and click on 'Edit inbound rules'.

w EC2 ×	EC2 > Security Groups > sg-0f6883a8805987489 - launch-wizard-			
us what you think ashboard	sg-0f6883a8805987489 - launch-wi	zard-1		Actions V
lobal View	Details			
s	Security group name D launch-wizard-1	Security group ID D sg-0f6883a8805987489	Description B launch-wizard-1 created 2023-04-12T00:37:51.2712	VPC ID Ø vpc-055e67a08def82726
nces Icces Icce Types	Owner	Inbound rules count 5 Permission entries	Outbound rules count 1 Permission entry	
h Templates Requests gs Plans	Inbound rules Outbound rules Tags			
ved Instances ated Hosts ity Reservations	You can now check network connectivity with Reachability Analyz	er		Run Reachability Analyzer 🛛 🗙
5	Inbound rules (5)			C Manage tags Edit inbound rules
	Q Filter security group rules			< 1 > 🐵
Italog Block Store		P version v Type v Protocol	▼ Port range ▼ Source 22 0.0.0.0/0	▼ Description ▼
es hots	- sgr-027916ae7fb6ee2c4 IF	Pv4         SSH         FCP           Pv4         HTTP         TCP           Pv4         Custom TCP         TCP	80 0.0.0/0 13133 0.0.0/0	-
cle Manager ork & Security	sgr-02b7f112c8db3bc2b	Pv4         Custom TCP         TCP           Pv4         Custom TCP         TCP	8080 0.0.0.0/0 55555 0.0.0.0/0	-
ity Groups : IPs	- <u>3</u> gr-004034393437473 Ir	re constituer iter	33333 0.00.0/0	-
nent Groups iirs irk Interfaces				
latancing				
Groups				
icaling				

20 – AWS – Security Group Settings Page.

4. Click 'Add rule" and set 'Port range' to be a value between 1000 to 65000 (excepting 5555) and 'Source' to be same as above ports '0.0.0.0/0'. You can create multiple ports here all at once to allow all your S-PLAYs to be accessed from this server. Don't forget to 'Save rules'.

Here in the below example, one extra port 8081 is added for the additional S-PLAY and we will use this when setting up the S-PLAY.

bound rules Info									
ecurity group rule ID	Type Info	Pro	tocol Info	Port range Info	Source Info		Description - optional Info		
pr-01a7bfd9565b7522a	SSH	<b>T</b>	CP	22	Custom 🔻	Q		Delete	
						0.0.0.0/0 ×			
pr-027916ae7fb6ee2c4	HTTP	▼ T0	CP	80	Custom 🔻	Q		Delete	
						0.0.0.0/0 ×			
r-0955431d10fc0188d	Custom TCP	▼ T0	CP	13133	Custom 🔻	Q		Delete	
						0.0.0.0/0 🗙			
pr-02b7f112c8db3bc2b	Custom TCP	<b>T</b>	CP	8080	Custom 🔻	Q		Delete	
						0.0.0.0/0 ×			
pr-0ba094989a97c7939	Custom TCP	▼ T0	CP	55555	Custom 🔻	Q		Delete	
						0.0.0.0/0 ×			
	Custom TCP	▼ T0	CP	8081	Anywhere-IPv4 <b>v</b>	۹		Delete	
						0.0.0.0/0 🗙			
Add rule									
Add Tale									

21 – AWS – Editing inbound rules to add extra port.

S-PLAY (70092) Visit the ENTTEC <u>website</u> for the latest version

5. Before we configure our S-PLAY, the IP address and the Username from the server are required. Go back to the instance summary and click 'Connect' button on the top right corner that will navigate us to the page showing the required information.

w EC2 ×	EC2 > Instances > i-093ecb0147a874e3a		
as what you think	Instance summary for i-093ecb0147a874e3a (ENTTEC) Info Updated less than a minute ago		Connect     Instance state ▼     Actions ▼
Joshboard Jobal View	Instance ID	Public IPv4 address	Private IPv4 addresses
3	i-093ecb0147a874e3a (ENTTEC)	🗇 3.26.115.206   open address 🗹	172.31.27.21
	IΡνδ address	Instance state Running	Public IPv4 DNS  C ec2-3-26-115-206.ap-southeast-2.compute.amazonaws.com   open address 🔀
	- Hostname type	Private IP DNS name (IPv4 only)	ecc-s-co-i i s-cocap-southeast-c.compute.amazonaws.com   open address 🕑
nces	IP name: ip-172-31-27-21.ap-southeast-2.compute.internal	Private IP DNS name (IPV4 only) ip-172-31-27-21.ap-southeast-2.compute.internal	
nces nce Types	Answer private resource DNS name	Instance type	Elastic IP addresses
h Templates	IPv4 (A)	t2.micro	-
equests	Auto-assigned IP address D 3.26.115.206 [Public IP]	VPC ID © vpc-055e67a08def82726	AWS Compute Optimizer finding  Opt-in to AWS Compute Optimizer for recommendations.   Learn more
s Plans	IAM Role	Subnet ID	Auto Scaling Group name
red Instances ited Hosts		🗇 subnet-02bf34225ca457627 🖸	-
ty Reservations	IMDSv2 Required		
s			
	Details Security Networking Storage Status checks	Monitoring Tags	
italog	▼ Instance details Info		
Block Store	Platform D Amazon Linux (Inferred)	AMI ID	Monitoring disabled
es	Platform details	AMI name	Termination protection
tots te Manager	Linux/UNIX	al2023-ami-2023.0.20230329.0-kernel-6.1-x86_64	Disabled
le Manager rk & Security	Stop protection Disabled	Launch time 😰 Wed May 03 2023 10:52:25 GMT+1000 (Australian Eastern Standard Time) (abo	AMI location out 6 hours) of amazon/al2023-ami-2023.0.20230329.0-kernel-6.1-x86_64
y Groups	Instance auto-recovery Default	Lifecycle normal	Stop-hibernate behavior disabled
ment Groups	AMI Launch index	Key pair assigned at launch	State transition reason
airs	0	ENTTEC_CS	-
rk Interfaces	Credit specification standard	Kernel ID	State transition message
alancing	Usage operation	RAM disk ID	Owner
Groups	RunInstances	-	141366952204
icaling	ClassicLink -	Enclaves Support	Boot mode
Configurations	Current instance boot mode	Allow tans in instance metarlata	Lice BRA ac minet OS hostname
Services	Q Search	[Alt+S]	∑ \$ Ø Sydney ▼
Connect t	Connect to instance     instance info ur instance i-0492b92798fbcc3e8 (Remote Access S-PLAY) using any o	f these options	
EC2 Insta	ance Connect Session Manager SSH client	EC2 serial console	
	92798fbcc3e8 (Remote Access S-PLAY)		
Public IP add			
_ J4.2J2.1			
User name	name defined in the AMI used to bunch the instance. If you didn't def	ine a custom user name, use the default user name,	
User name Enter the user ec2-user.	name defined in the AMI used to bunch the instance. If you didn't def	ine a custom user name, use the default user name,	
User name Enter the user i	name defined in the AMI used to illunch the instance. If you didn't def	ine a custom user name, use the default user name,	
User name Enter the user r ec2-user ec2-user	name defined in the AMI used to flunch the instance. If you didn't def		

22 – AWS – Retrieving IP address and Username of the cloud server.

ID: 5930032



6. Now we can start setting on the additional S-PLAY. Access to the S-PLAY webpage and navigate to Settings tab. Enable the Remote Access from your additional S-PLAY, enter the IP, Username and SSH Key (the .pem Key pair file created in Page 8) while the Remote Port at the value set from the last step.

Here in our example is 8081. Press Update, and the remote access globe sign should turn green which means it is active.



23 – S-PLAY – setting up the newly created port to the additional S-PLAY.

#### **Remote Access: Troubleshooting**

On first connection, the S-PLAY will automatically try to configure the server's gateway by running:

```
/usr/bin/sudo /usr/bin/sed -i -e 's/.*GatewayPorts.*/GatewayPorts yes/g' /etc/ssh/sshd_config
/usr/bin/sudo /usr/bin/systemctl restart sshd
```

If the Username provided in setup doesn't have any sudo rights or sshd_config is located in different place, you will need to manually update the sshd_config on your AWS Server to set "GatewayPorts yes" and restart the sshd service.

To access the terminal, navigate to the server instances on AWS. Press Instance ID and then 'connect' on the top right corner which brings us to the page as below. Click 'Connect' again to open the terminal.

LL2 > Instances > I-U442D92/98TDCC588 > Connect to instance	EL2 > Instance 5 > F04920927990bc23e8 > Connect to instance         Connect to instance info         Connect to jour instance F04920927990bc23e8 (Remote Access S-PLAY) using any of these options         EC2 Instance Connect       Session Manager         SSH client       EC2 serial console         Instance ID       Instance 404920927990bc23e8 (Remote Access S-PLAY)         Public IP address       S 4.252.180.241         User name       Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, e2-user.	5	Services Q Search	[Alt+S]	← → ♂ ≜ us-east-2.console.aws.am
Connect to instance Info       Connect to your instance Info         Connect to your instance Info       Connect to your instance Info         EC2 Instance Connect       Session Manager       SSH client         EC2 Instance Connect       Session Manager       SSH client         EC2 Instance ID       Instance ID       Instance ID         Instance ID       S 54 client       EC2 serial console         Public IP address       S 4.252.180.241       End of the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ec2-user.	Connect to instance Info       [ec2-user@ip-172-31-29-165 -]3         Connect to your instance I-0492b92798/bcc3e8 (Remote Access S-PLAY) using any of these options       [ec2-user@ip-172-31-29-165 -]3         Instance ID       Instance ID         Image: Instance I address       [image: Image: Ima		EC2 > Instances > i-0492b92798fbcc3e8 >	Connect to instance	( _ / Amazon Lir
Instance ID DI-0492b92798fbcc3e8 (Remote Access S-PLAY) Public IP address DI 54.252.180.241 User name Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ec2-user.	Instance ID Instance ID Instance ID Instance ID Instance ID Public IP address I S4.252.180.241 User name Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ec2-user ec2-user I Note: In most cases, the default user name, ec2-user, is correct. However, read your AMI usage instructions to			e Access S-PLAY) using any of these options	https://aws.amazon.com/amazon-li [ec2-user@ip-172-31-29-165 -]\$
I-0492b92798fbcc3e8 (Remote Access S-PLAY) Public IP address     S4.252.180.241 User name Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ec2-user.	<ul> <li>☐ i-0492b92798fbcc3e8 (Remote Access S-PLAY)</li> <li>Public IP address</li> <li>☐ 54.252.180.241</li> <li>User name</li> <li>Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ec2-user.</li> <li>ec2-user</li> <li>O Note: In most cases, the default user name, ec2-user, is correct. However, read your AMI usage instructions to</li> </ul>		EC2 Instance Connect Session Manag	er SSH client EC2 serial console	
<ul> <li>54.252.180.241</li> <li>User name</li> <li>Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ec2-user.</li> </ul>	St4252.180.241 User name Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ec2-user. ec2-user Ic2-user Ic2-user in most cases, the default user name, ec2-user, is correct. However, read your AMI usage instructions to			AY)	
User name Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ec2-user.	User name Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ec2-user   Note: In most cases, the default user name, ec2-user, is correct. However, read your AMI usage instructions to		Public IP address		
Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ec2-user.	Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ec2-user.  C2-user  Note: In most cases, the default user name, ec2-user, is correct. However, read your AMI usage instructions to		<b>5</b> 4.252.180.241		
ec2-user	Note: In most cases, the default user name, ec2-user, is correct. However, read your AMI usage instructions to		Enter the user name defined in the AMI used to launch t	he instance. If you didn't define a custom user name, use the default user name,	
			ec2-user		
					i-097f4794eba8b1bb3
	i-097f4794eba8b1bb3 Public IPs: 18.217.232.203 Private IPs: 172.31.28.16			Cancel Connect	FINITE FOR THE PROPERTY FINITE ITENTS



ID: 5930032

To allow the S-PLAY to manage your AWS server's gateway in needs to permit this, run:

/usr/bin/sudo /usr/bin/sed -i -e 's/.*GatewayPorts.*/GatewayPorts yes/g' /etc/ssh/sshd_config

/usr/bin/sudo /usr/bin/systemctl restart sshd

It's worth noting that. **/etc/ssh/sshd_config** can be located in a different folder depending on the operating system running on your remote server.

### Wrapping up

That brings us to the end of the configurations we need to do for remote connections but remember that we set up this server to be accessible from any IP address, so for security it's highly recommended to use the S-PLAY's password lock function. You can do that by going to your S-PLAY's home page and clicking "user" drop down and clicking "change passwords".

To connect remotely, just go back to our remote access settings and look for the URL that the S-PLAY displays. This address is generated by the S-PLAY according to the settings you have just input and is the address you need to enter to access your S-PLAY remotely.

#### Conclusion

By following these steps, you can create a control panel on your smart phone or tablet to intuitively control the S-PLAY, call shows, and adjust brightness's. This guide gives you a run down on a basic workflow and control panel, but this is just the beginning. With a bit of time and ingenuity, you can create even more sophisticated control panels.

This brings us to the end of this guide on how to set up remote access on your S-PLAY. By following these steps, you can set up your S-PLAY to be accessible from around the world over the internet.

We hope you found this application note useful!

# **CONTRACT OF CONTRACT OF CONT OF CONT OF CONTRACT OF CONTACT OF CONTACT OF CONTRACT OF CONTRACT OF CONTRACT OF CON**

17 | enttec.com

ID: 5930032