VCOM Virtual Matrix

Documentation for VCOM Virtual Matrix

Intracom Systems, LLC

Table of contents

1. Installation

1.1 Hardware Requirements

Operating System Requirements
The VCOM Virtual Matrix can be installed on virtually any modern Windows based operating system however Windows 11 Professional or Windows Server 2022 are highly recommended.

Memory Requirements
The memory requirement for the VCOM Virtual Matrix are very minimal and system size does not realistically need to be considered. It is recommended to use 8GB of memory with any modern OS which will also provide sufficient resources for operation of the Virtual Matrix.

Storage Requirements
The storage requirements for VCOM Virtual Matrix in the standard configuration are not substantial but some incremental storage space is required for Activity/Debug Logs. In the standard configuration, a minimum of a 128GB SSD is recommended although a 256GB SSD is preferred. An SSD is specified only for reliability.

If the system is configured with audio recording, additional diskspace may be required. Recording in WAV file format, at the default audio sampling rate of 32KHz, would require 225 MB per recording hour but after MP3 compression will likely be 10% of that value. As an example, if recording 1 channel with active audio for 5 hours per day for an entire year, it would require and estimated 40GB of disk space. When the system is configured with audio recording, a TB drive is recommended.

Computational Requirements (N/A for for VCOM WebRTC Clients)
The computational requirements for the Virtual Matrix depends on the number of active connections to the system and how the system is being utilized. In a “Heavy” use configuration, there would be many users simultaneously monitoring multiple audio sources including multiple conferences with large groups of users. In a moderate use configuration, there would be many users simultaneously monitoring single sources or conferences with smaller groups of users. In a “Light” use configuration, there would some users monitoring audio sources and conferences while other users just periodically

communication with specific other users. To determine the computation requirements each of the use cases is assigned a value for the ‘Number of Connections’ relative to the ‘Number of CPU Cores’ as follows:

`Number of CPU Cores`

Number of Connections	**Heavy**	**Moderate**	**Light**
	50	75	100
100	2	1	1
200	4	2	2
300	6	4	3
400	8	5	4
500	10	7	5
600	12	8	6
700	14	9	7
800	16	11	8
900	18	12	9
1000	20	13	10
1100	22	15	11
1200	24	16	12

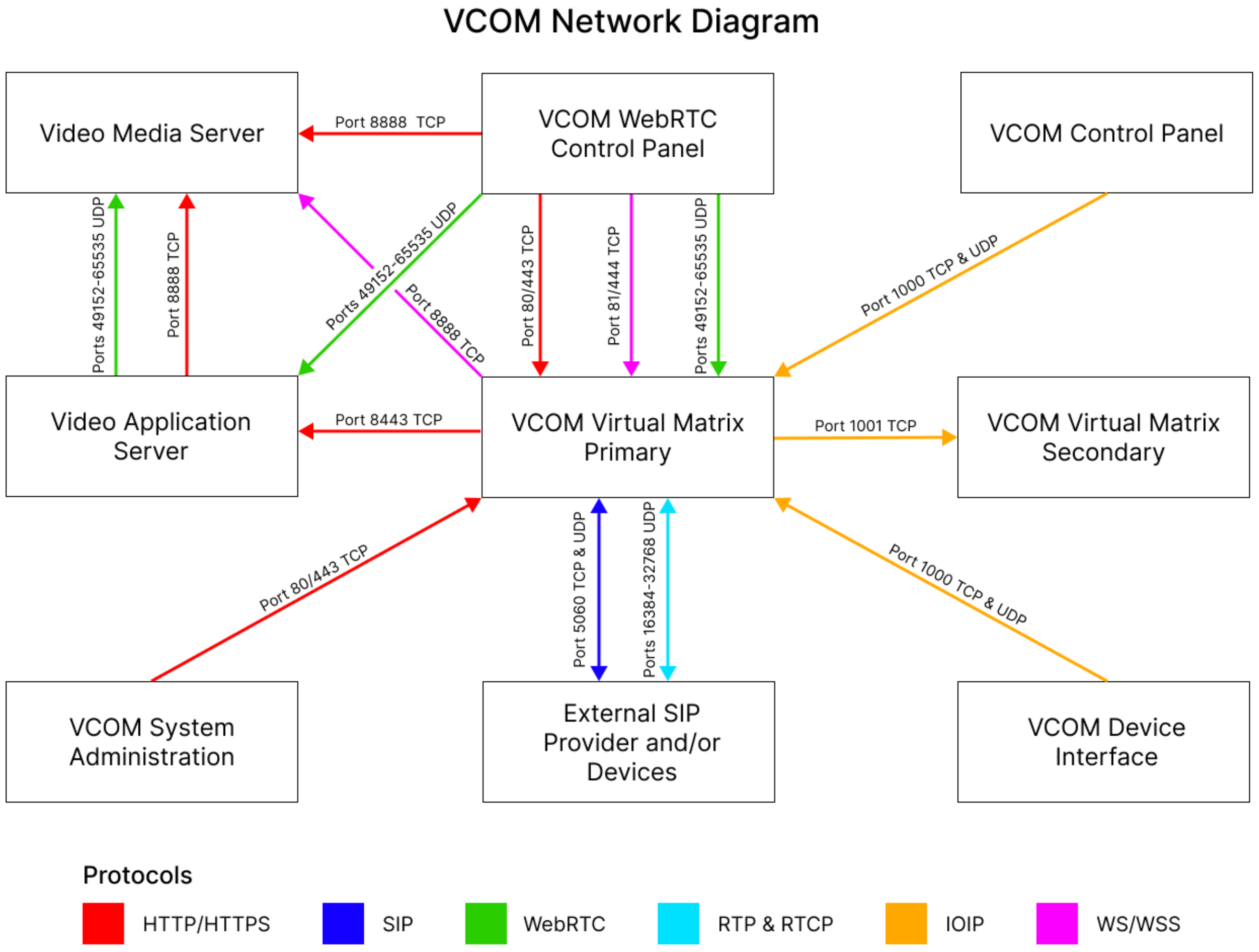
The CPU itself must have an average CPU benchmark (aka CPU Mark per PassMark) of approximately 1250 per core. If the CPU does not meet this criteria, the data provide must be scaled appropriately.

For reference, the standard server provided by Intracom has an Intel Core i7-8700 with 12 cores and a PassMark benchmark of 15222 or an average of 1268 per core. With the above recommendations, the server can support 600+ connections in a “Heavy” use configuration, 900+ connections in a “Moderate” configuration or 1200+ connections in a “Light” use configuration.

Additional factors effecting computational requirements would be the co-location of the Device Interface with a Dante Virtual Sound card on the same server as the Virtual Matrix.

1.2 Network Requirements

Network Diagram



Arrows denote direction of connection origination. All connections are bidirectional.

Bandwidth Requirements

The network bandwidth requirements must be carefully analyzed to ensure proper bandwidth is available at any point where multiple clients will share the same physical connection point. The most obvious connection point where this is critical is at the server where bandwidth requirements will be the sum of the requirements of every possible client. The least obvious connection point where this is also important occurs when multiple remote clients in one physical location need to access the server in another physical location as the bandwidth requirements for the connection between these two points will be the sum of the requirements for all remote clients.

To determine the bandwidth requirements it is necessary first to determine the network bandwidth utilization per client connection, which is indicated below for the various audio sample rates that can be configured.

VCOM Control Panel and VCOM Device Interface:

Audio Sample Rate	Data Rate (Kbps) [ATS=20ms*]	Data Rate (Kbps) [ATS=40ms*]	Data Rate (Kbps) [ATS=60ms*]	Data Rate (Kbps) [ATS=80ms*]	Data Rate (Kbps) [ATS=100ms*]
8 KHz	32	23.6	20.8	19.4	18.56
16 KHz	44.8	36.4	33.6	32.2	31.36
32 KHz	46.8	38.4	35.6	34.2	33.36

VCOM WebRTC Control Panel:

Audio Sample Rate	Data Rate (Kbps)
48 KHz	200

ATS = Audio Time Slice per packet which controls how many 20ms audio frames are transmitted within a single UDP packet. As each UDP packet requires a fixed amount of overhead, the more frames sent at the same time, the less the UDP overhead which conserves network bandwidth. Conversely, the more audio frames sent per transmission, the greater the system latency and the potential audible consequence of a lost packet. The default is 20ms.

To determine server bandwidth requirements, first determine maximum potential bandwidth utilization by multiplying the number of clients (users and devices interfaced) by the Data Rate associated with appropriate Audio Sample Rate for the configured Audio Time Slice per packet. The product is the bandwidth required if every client were to receive audio simultaneously (maximum download bandwidth requirement) and also the bandwidth required if every client were to send audio simultaneously (maximum upload bandwidth requirement). In a typical system, the maximum download bandwidth requirement must be allocated for, as several system functions can require simultaneous audio transmission to all clients. The maximum upload bandwidth requirement however will realistically never be achieved as it is not feasible that all audio sources in a system would be active simultaneously since the result would be inaudible. As such the upload bandwidth to be allocated must be made based on the estimation of the number of simultaneous active audio sources noting that inactive audio sources will have no bandwidth requirements.

Firewall Requirements

VCOM uses the below ports. It is only necessary to open the ports for the VCOM features you use in the "Required for" column below. In VCOM version 6.5 and later the Windows firewall rules are automatically created upon installation. The WebRTC Media audio uses the ephemeral port range which should not need to be opened on the firewall.

Port or Port Range	Protocol	Description	Required for
80	TCP (HTTP)	System Administration and WebRTC Control Panel data (Unsecure)	Not Required
443	TCP (HTTPS)	System Administration and WebRTC Control Panel data (Secure)	System Administration and WebRTC Control Panel
81	TCP (WS)	WebRTC Control Panel Signaling data (Unsecure)	Not Required
444	TCP (WSS)	WebRTC Control Panel Signaling data (Secure)	WebRTC Control Panel
1000	TCP (IOIP)	Control Panel for Windows/iOS/Android & Device Interface data	Control Panel
1000	UDP (IOIP)	Control Panel for Windows/iOS/Android & Device Interface audio	Control Panel
1001	TCP (IOIP)	Virtual Matrix Failover data	Failover
5060	TCP (SIP)	SIP Signaling data	SIP
5060	UDP (SIP)	SIP Signaling data (Default but can be disabled to force TCP)	SIP
16384-32768	UDP (RTP+RTCP)	SIP Media audio	SIP
49152 to 65535	UDP (WebRTC)	WebRTC Media audio	WebRTC Control Panel
8443	TCP (WSS)	Video Application Server	Video Streaming
8888	TCP/UDP	(separate) Media Server	Video Streaming

1.3 WebRTC Audio Connection

When the client logs into the server, the client and the server work together determine the network path for the audio connection. If the client and server are both located on the same private network, the audio connection is straight forward and a connection is made directly between the client and server. If the server is located on a private network and the client is on the public Internet or the client is on separate private network that is also connected to the public internet, the audio connection is more complex as the connection must be established via the firewall(s) of the private network(s). In 80% of network installations, this is all handled automatically and transparently such that the audio connection is routed directly to and through the firewall(s) of the private network(s) without further considerations necessary. However, in 20% of the network installations, typically on highly secure corporate networks using Symmetric NATs, the firewall restrictions are such that the audio connection cannot be routed directly to and through the firewall of the private network. In this situation, the audio connection must be routed through a relay server located in the public Internet. This relay server is referred to as a “TURN” server which stands for ‘Traversal Using Relays around NAT’. If a TURN server is required, please refer to the ‘TURN Server’ section for setup and configuration information. If provisioning a TURN server is not feasible, a TURN server can be provided as a service by Intracom. Using a TURN server is completely secure as all WebRTC audio packets must be encrypted using TLS (Transport Layer Security) by definition and can only be decrypted by the intended recipient.

1.4 Software Installation

Download VCOM Virtual Matrix from our downloads page and unzip the installer.

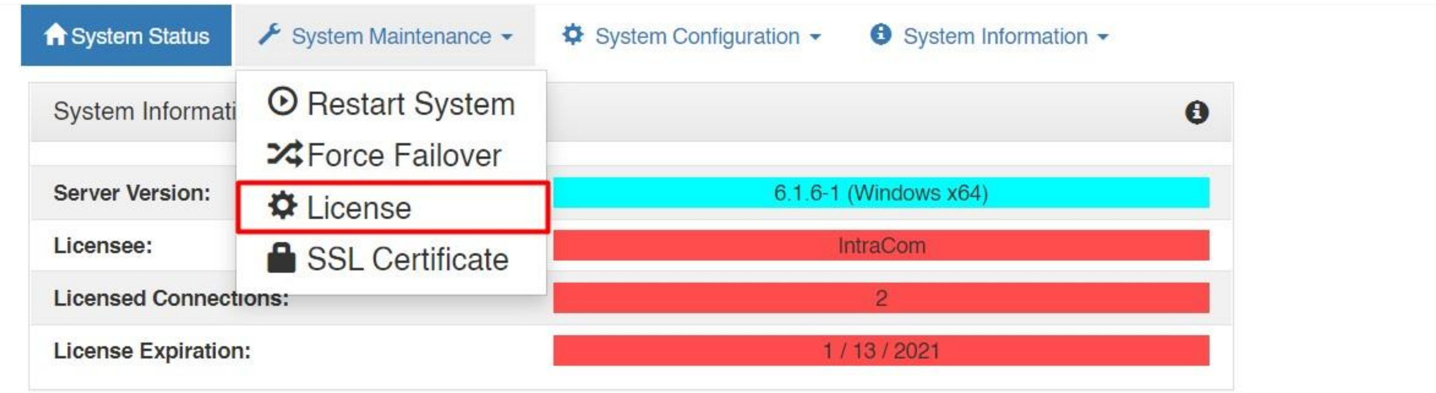
Run the installer and follow the prompts. You will need to accept Intracom Systems’ License Agreement to install the software. During the installation process you will be asked if you want to install the VCOM Virtual Matrix to run as a service or application. Servers should run VCOM as a service.

To open the VCOM Virtual Matrix once installed click on your ‘VCOM Virtual Matrix’ shortcut icon on your desktop or click on your start menu and select ‘All Programs.’ Find ‘Intracom’ and select ‘VCOM Virtual Matrix.’

Note, you can run the VCOM Virtual Matrix before licensing but will not be able to connect Control Panels or Device Interfaces.

1.5 Licensing

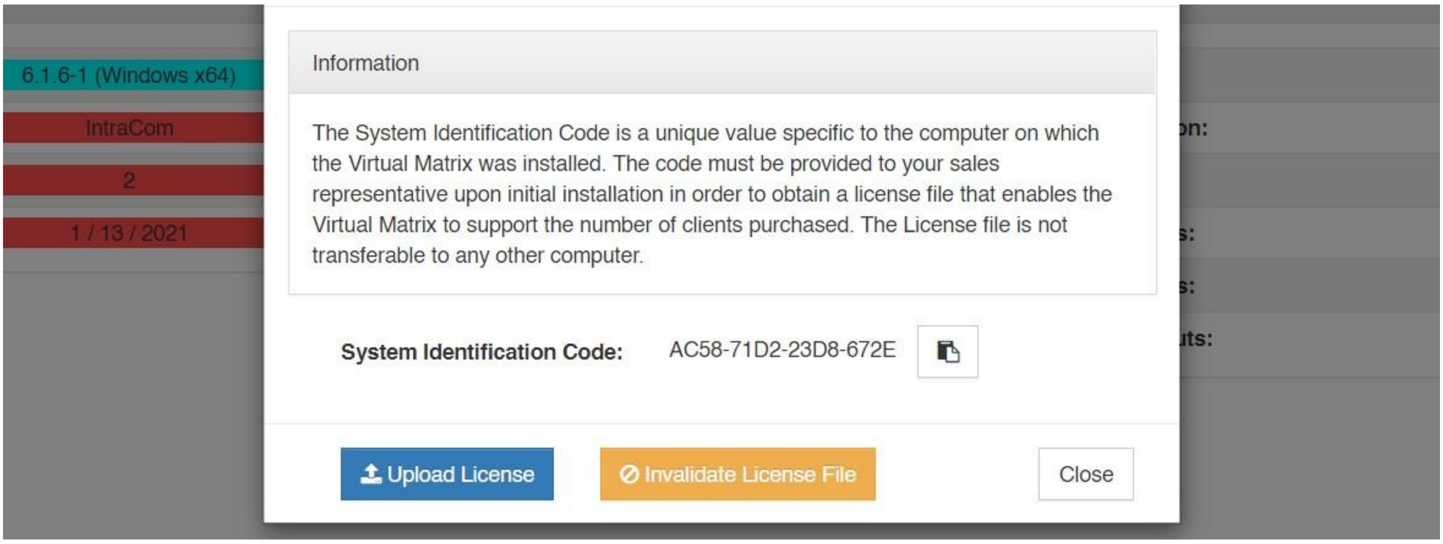
To license your VCOM System you need to acquire a valid license file from Intracom. To do so you must provide Intracom with your unique ‘System Identification Code’ generated automatically when you install the VCOM Virtual Matrix. The ‘System Identification Code’ is a unique value specific to the computer on which the Virtual Matrix was installed and is not transferable to any other computer. If the server you are running the VCOM Virtual Matrix on has dual network cards make sure the correct one is chosen before sending the system identification code as it is dependent on the network card being used.



System Informati

Server Version:	6.1.6-1 (Windows x64)
Licensee:	IntraCom
Licensed Connections:	2
License Expiration:	1 / 13 / 2021

1) Log into the VCOM System Administration and in the upper left corner select 'License' from the 'System Maintenance' tab.



Information

The System Identification Code is a unique value specific to the computer on which the Virtual Matrix was installed. The code must be provided to your sales representative upon initial installation in order to obtain a license file that enables the Virtual Matrix to support the number of clients purchased. The License file is not transferable to any other computer.

System Identification Code: AC58-71D2-23D8-672E

2) If you do not have a VCOM license copy the code and send it to your VCOM sales representative. If you already have a VCOM license click 'Upload License' and select the license file.

Once the license file is installed, the VCOM Virtual Matrix will be ready to accept connections under the default configuration for 40 users consisting of 20 guest users that work using the guest template, 10 VCPs set for Windows Desktop, and 10 VDIs set for 4 wire interfaces.

The guest template allows for users to use their own user name for logging into the VCP on any supported device using the password of “guest”. This is useful during temporary/ demonstration in which you can assign the necessary selectors for the event, give the users the Virtual Matrix IP address, and the users can use their own user name with the password of “guest”.

The 10 preprogrammed “Panels” all have the user name of “panelxx”, where xx= the associated number of the panel 01-10. For example, Panel #1 would use “panel01” as the user name. All panels do not have a password; so leave this blank when signing into the Virtual Matrix from the VCP.

The 10 preprogrammed “VDIs” are setup for a 4-wire interface. Like the aforementioned panels, the VDIs use “ioxx”, where xx= the associated number of the VDI 01-10. The VDIs also do not have a password, so leave this blank when signing into the Virtual Matrix from the VDI.

1.6 SSL Introduction

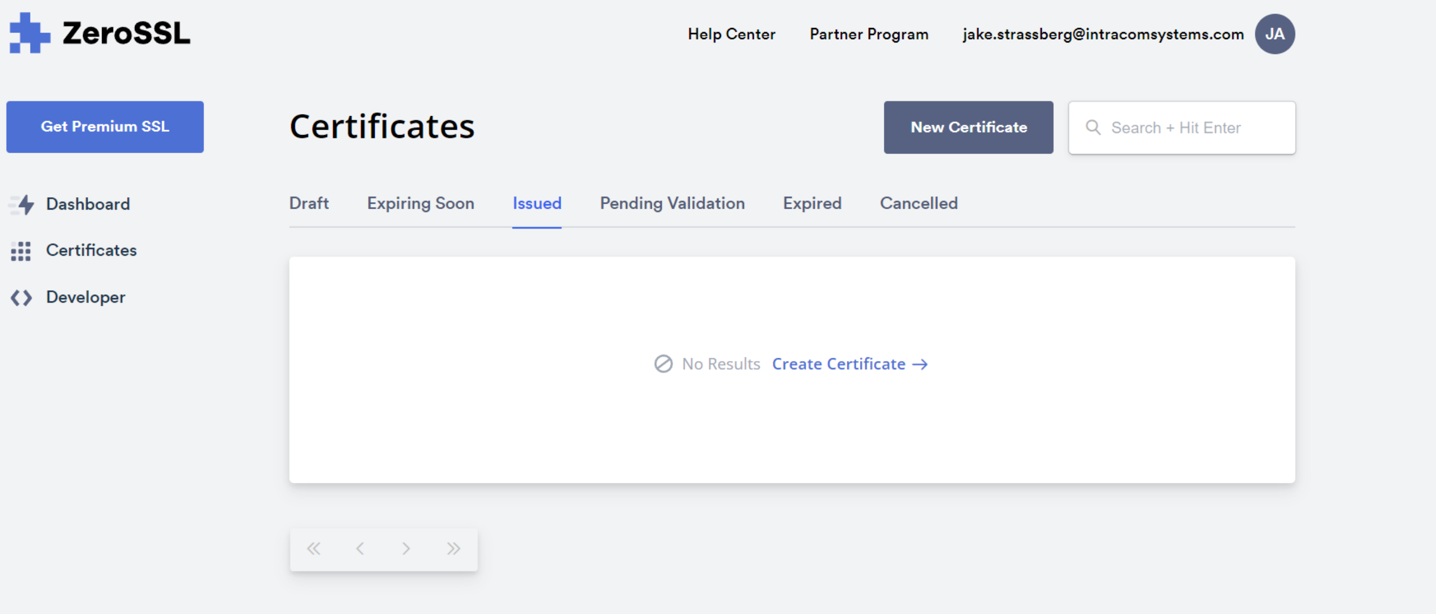
SSL allows for a secure, encrypted connection to be established between the VCOM Virtual Matrix server and the VCOM WebRTC Control Panel as well as the VCOM System Administration. The VCOM Virtual Matrix server will automatically generate a self-signed SSL certificate upon first launch.

By default, browsers do not trust self-signed certificates. As such when you try to access the System Administration or WebRTC Control Panel through a browser you will likely see a warning message or be blocked entirely. Despite the warning message, your connection to VCOM is still secure and encrypted. To avoid this warning message it is recommended to install the System Administration and WebRTC Control Panel apps. Additionally, the self-signed certificate can be installed on your device so it is trusted. On iOS this step is required if you do not plan to install a certificate authority signed certificate on the server.

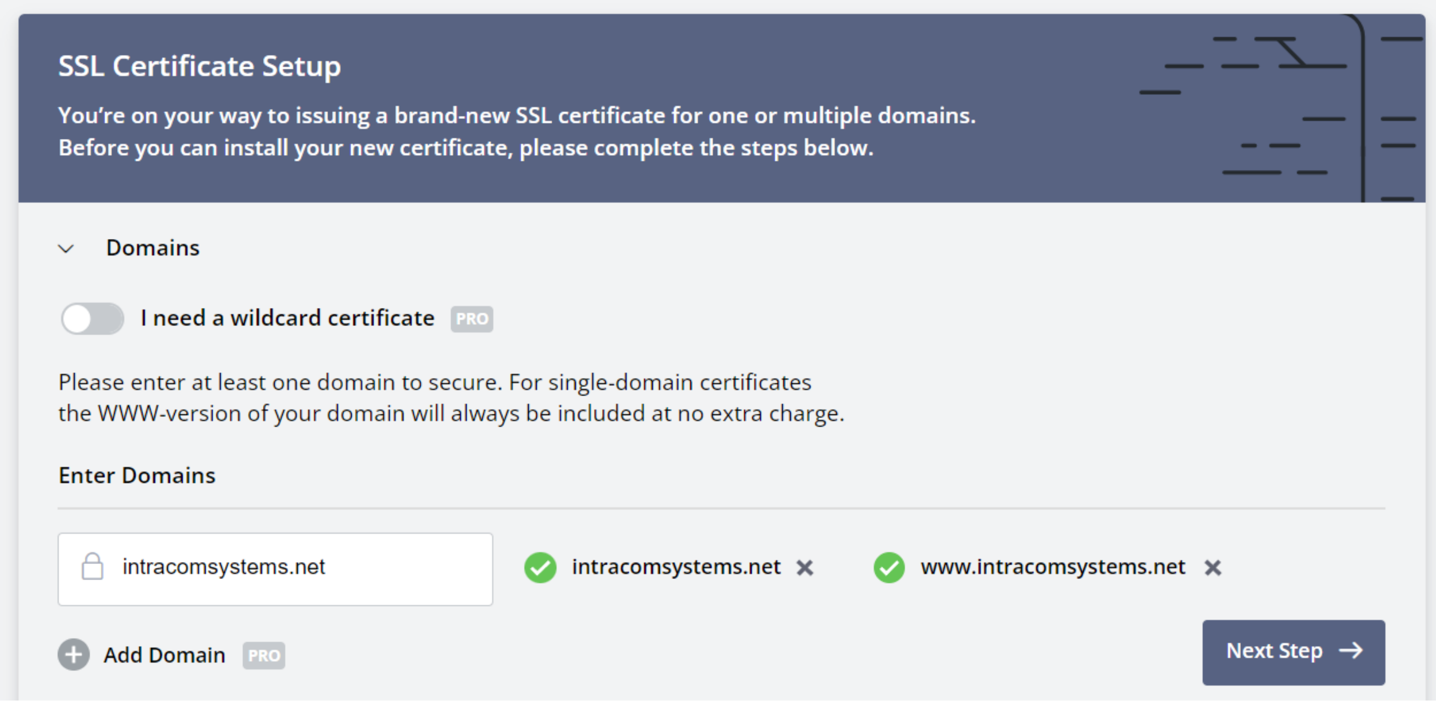
It recommended to install a certificate authority signed certificate on the VCOM server. Organizations that generate their own certificates can do so and install the certification on VCOM as they would with any other server. For organizations that do not have this capability, or for VCOM servers that are cloud hosted, the guide below can be followed to generate and install a certificate authority signed certificate.

1.7 SSL (CA Certificate)

To generate a CA (Certificate Authority) SSL certificate a domain name must be registered for the server. Additionally, the VCOM Virtual Matrix server must be accessible on the public internet. The steps below show how to generate an SSL certificate using zerossl.com however the steps will be similar for all SSL providers.



Make an account at zerossl.com then click Create Certificate.



You're on your way to issuing a brand-new SSL certificate for one or multiple domains. Before you can install your new certificate, please complete the steps below.

I need a wildcard certificate PRO

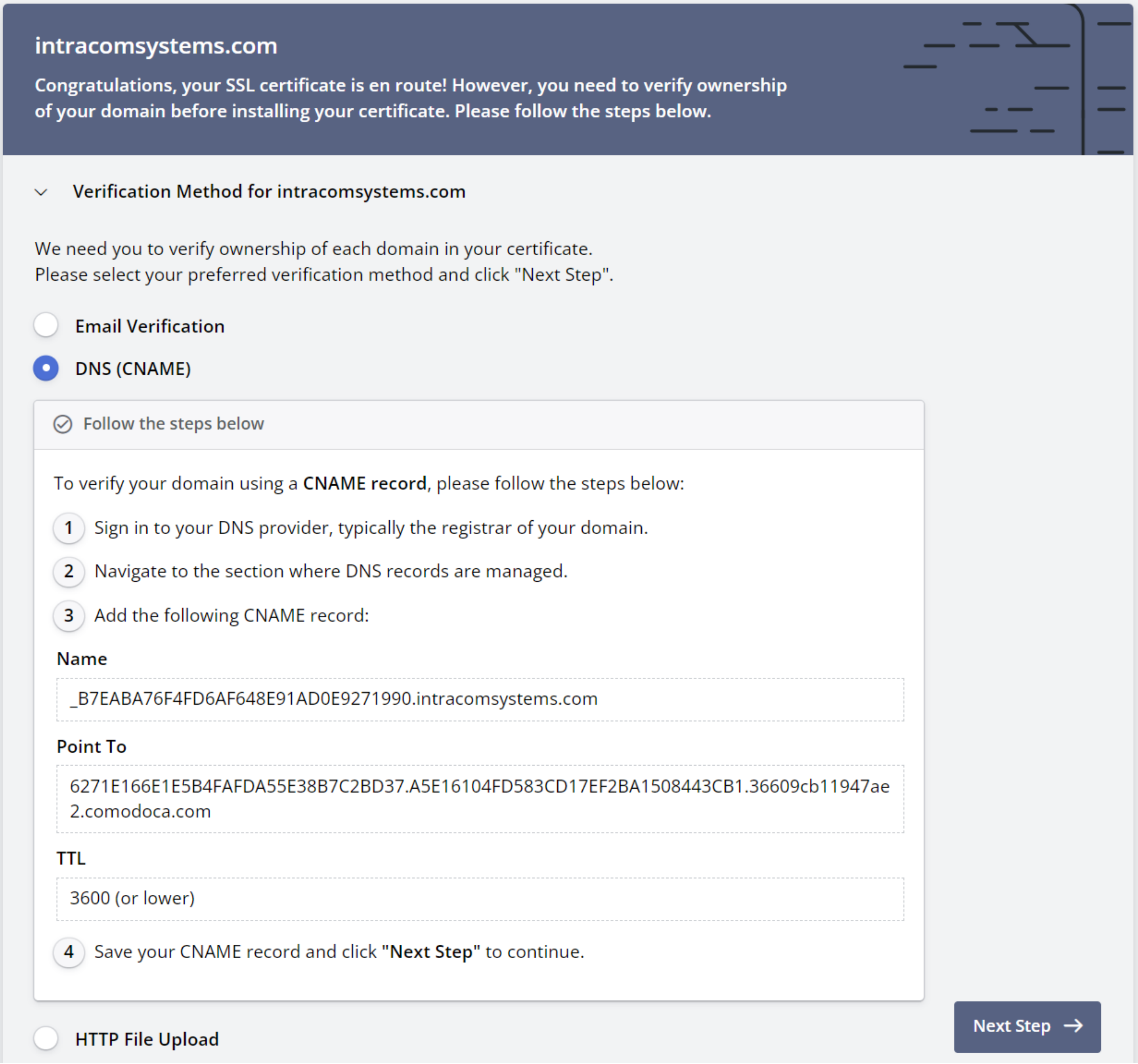
Please enter at least one domain to secure. For single-domain certificates the WWW-version of your domain will always be included at no extra charge.

Enter Domains

intracomsystems.net

✓ intracomsystems.net ✕ ✓ www.intracomsystems.net ✕

Enter your domain name in the field then click Next Step. Proceed through the prompts.



intracomsystems.com

Congratulations, your SSL certificate is en route! However, you need to verify ownership of your domain before installing your certificate. Please follow the steps below.

Verification Method for intracomsystems.com

We need you to verify ownership of each domain in your certificate.
Please select your preferred verification method and click "Next Step".

○ Email Verification

● DNS (CNAME)

Follow the steps below

To verify your domain using a **CNAME record**, please follow the steps below:

1 Sign in to your DNS provider, typically the registrar of your domain.

2 Navigate to the section where DNS records are managed.

3 Add the following CNAME record:

Name

_B7EABA76F4FD6AF648E91AD0E9271990.intracomsystems.com

Point To

6271E166E1E5B4FAFDA55E38B7C2BD37.A5E16104FD583CD17EF2BA1508443CB1.36609cb11947ae2.comodoca.com

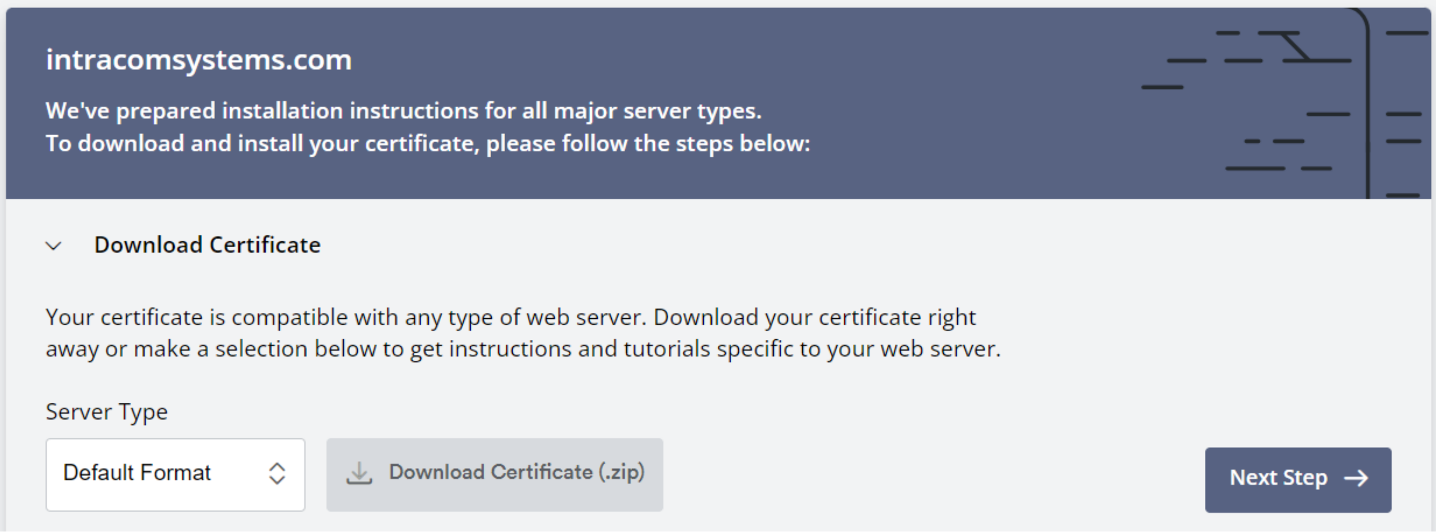
TTL

3600 (or lower)

4 Save your CNAME record and click **"Next Step"** to continue.

○ HTTP File Upload

There are a variety of methods that can be used to verify ownership of your domain. For this guide we have chosen the DNS (CNAME) option however any of the methods will work. Follow the instructions to create the necessary DNS records then click the Verify button.



intracomsystems.com

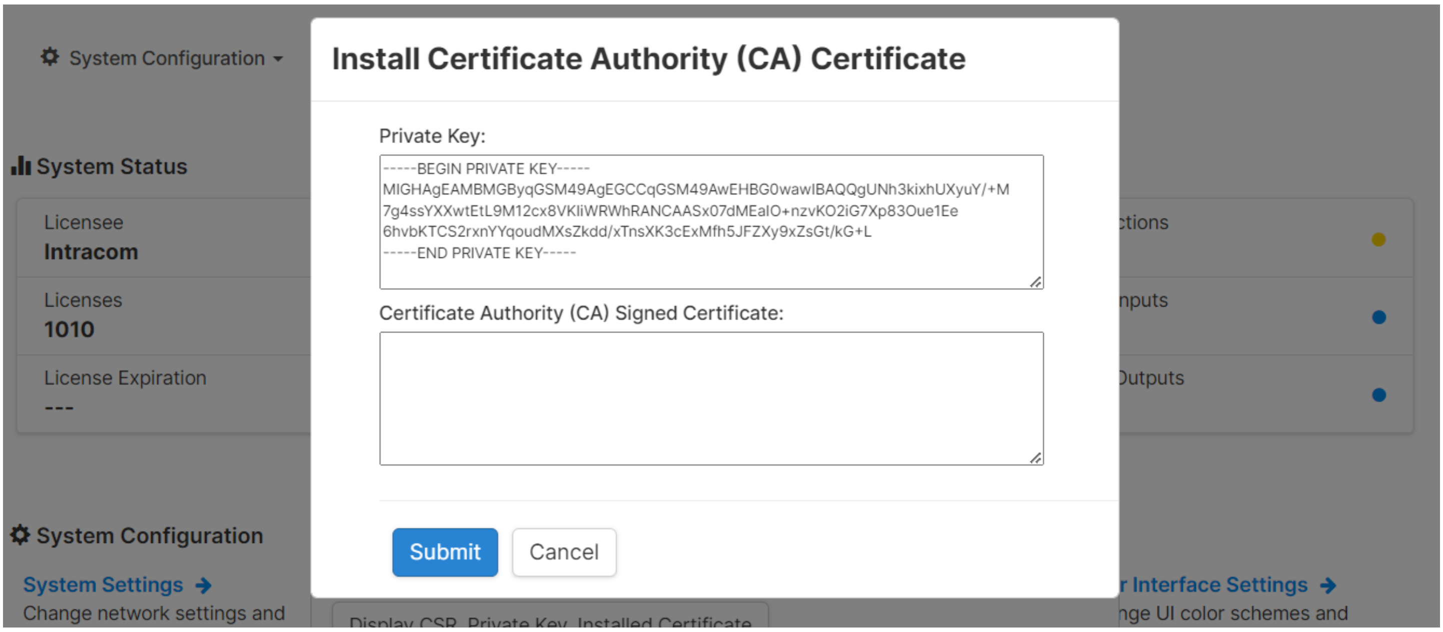
We've prepared installation instructions for all major server types.
To download and install your certificate, please follow the steps below:

Download Certificate

Your certificate is compatible with any type of web server. Download your certificate right away or make a selection below to get instructions and tutorials specific to your web server.

Server Type

Once the verification process is complete you will be able to download the certificate. Extract the zip and you will have 3 files: ca_bundle.crt, certificate.crt, and private.key. The contents of these files need to be uploaded to VCOM. Log into the System Administration and from the System Maintenance dropdown select Certificate. Click Install Signed Certificate.



Licensee
Intracom

Licenses
1010

License Expiration

Change network settings and

nge UI color schemes and

Install Certificate Authority (CA) Certificate

Private Key:

```
-----BEGIN PRIVATE KEY-----
MIGHAgEAMBMGByqGSM49AgEGCCqGSM49AwEHBG0wawIBAQQgUNh3kixhUXyuY/+M
7g4ssYXXwtEtL9M12cx8VKliWRWhRANCAASx07dMEalO+nzvKO2iG7Xp83Oue1Ee
6hvbKTCS2rxnYYqoudMXsZkdd/xTnsXK3cExMfh5JFZXy9xZsGt/kG+L
-----END PRIVATE KEY-----
```

Certificate Authority (CA) Signed Certificate:

Open the private.key file in a text editor to copy its contents. On Windows, to open the file in notepad you can right-click the file and select Open With > Notepad. Copy the contents of the file and past it into the Private Key field.

Next, copy the contents of the certificate.crt file and paste it into the Certificate Authority (CA) Signed Certificate field.

Lastly, copy the contents of the ca_bundle.crt file and paste it directly below the certificate in the Certificate Authority (CA) Signed Certificate field. Press Submit.

1.8 SSL (Self-Signed Certificate)

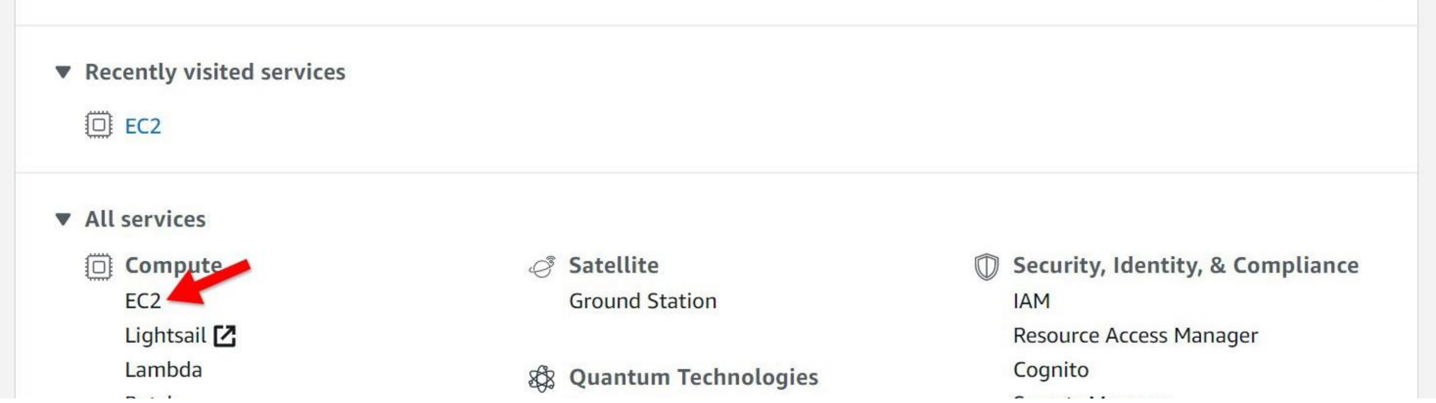
If you do not wish to generate a certificate authority signed certificate the instructions below can be followed to install the self-signed certificate that comes preinstalled on the VCOM server.

Installing the Self-Signed Certificate on iOS
1. From the WebRTC Control Panel login screen press the button to download the SSL certificate
2. A popup will display with instructions on how to install the certificate on your device

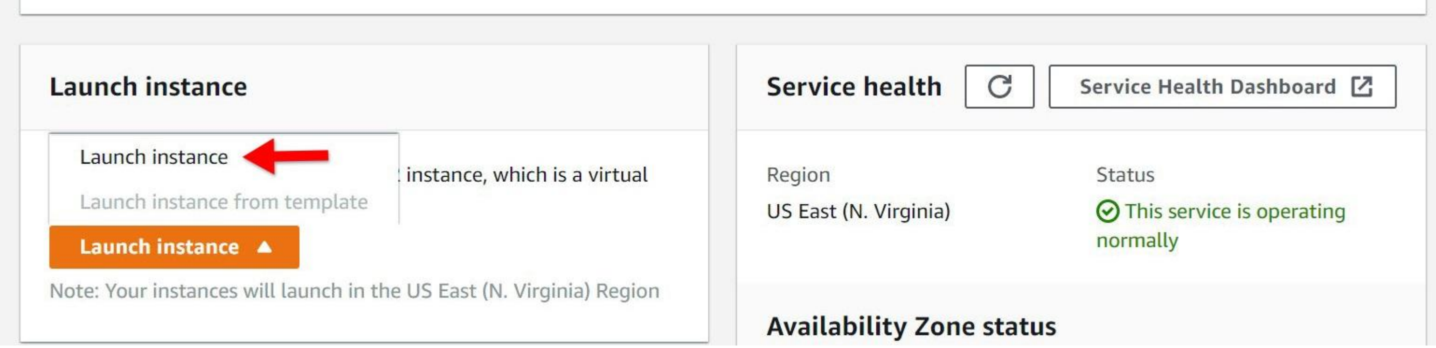
Installing the Self-Signed Certificate on Android
1. Download the certificate
2. Settings app -> Security -> Encryption & Credentials -> Install a Certificate -> Select CA Certificate option
3. Select Install Anyway
4. Select the Intracom Certificate that you downloaded previously

2. AWS Installation

This portion of the guide will show you how to create a virtual machine in the AWS EC2 Cloud.

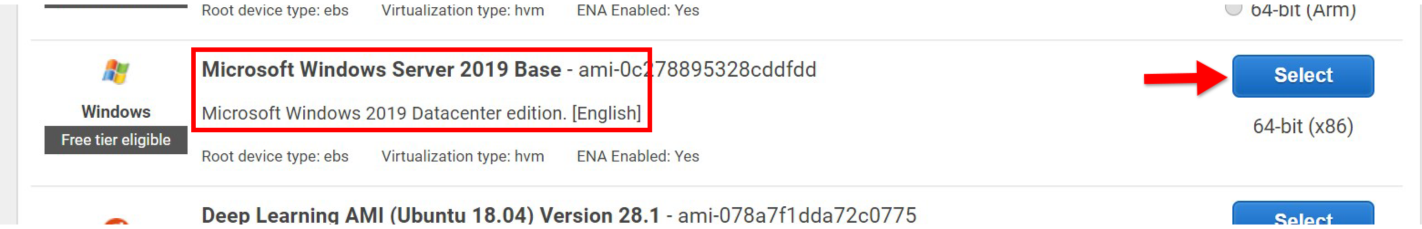


From the AWS Management Console select EC2 under the Compute services section.



Note: Your instances will launch in the US East (N. Virginia) Region

Click the orange Launch instance button then click Launch instance.



Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Microsoft Windows Server 2019 Base - ami-0c278895328cddfdd

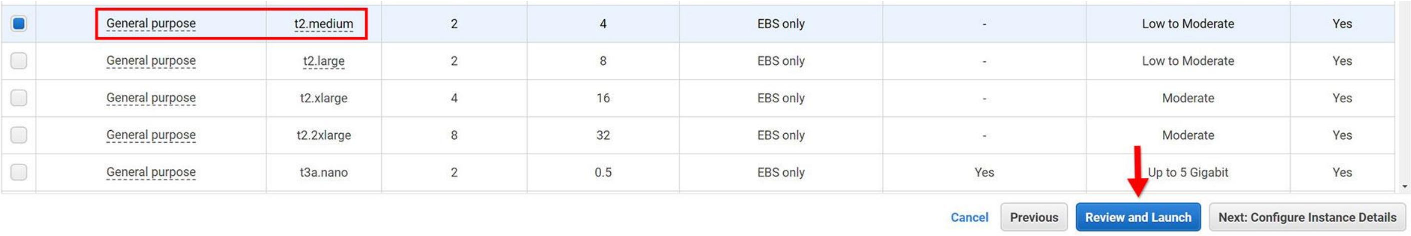
Microsoft Windows 2019 Datacenter edition. [English]

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Deep Learning AMI (Ubuntu 18.04) Version 28.1 - ami-078a7f1dda72c0775

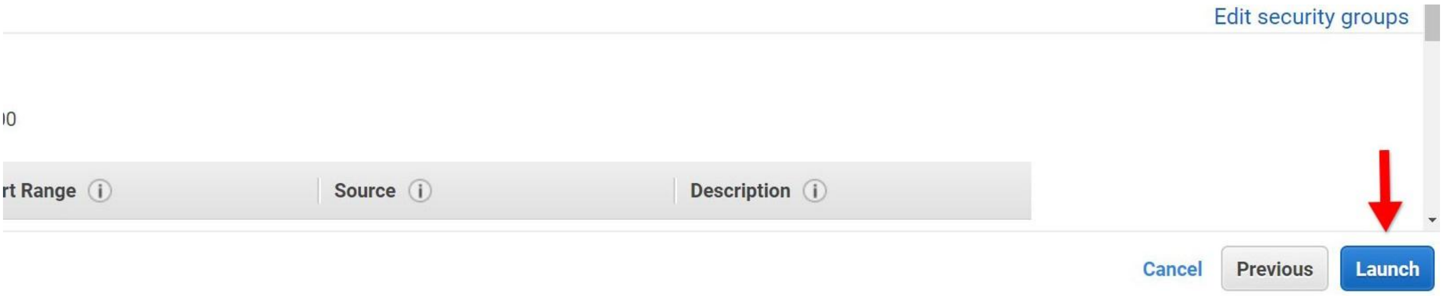
Scroll through the server OS options and select the Microsoft Windows Server 2019 Base image.

Note: VCOM can be run on all modern Windows Operating Systems. You may use a different version than what is show above.



☑	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
□	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
□	General purpose	t3a.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes

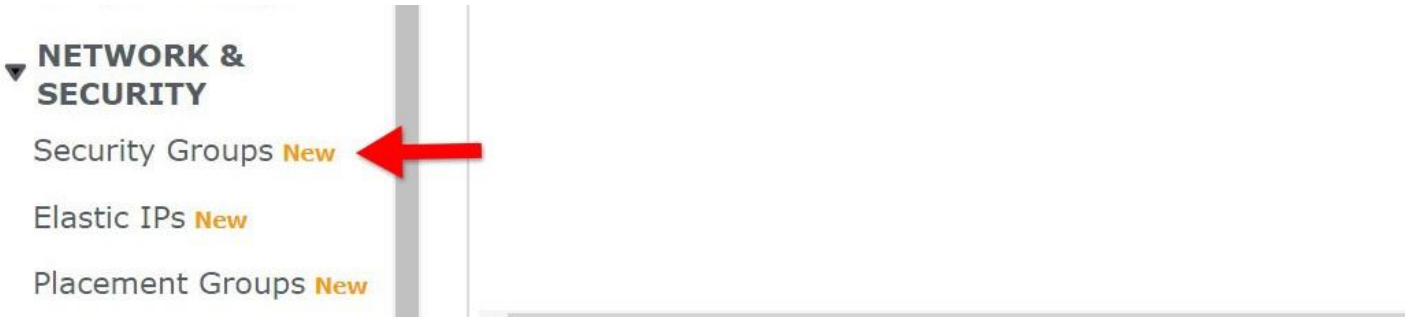
You will now select the hardware specifications for your EC2 instance. System hardware requirements are dependent on the number of concurrent users that will be accessing the system. Please refer to the VCOM Virtual Matrix Intercom System Requirements document for more information. For the purpose of this guide of this guide I have selected the t2.medium specifications featuring 2 processor cores and 4 Gb of RAM.



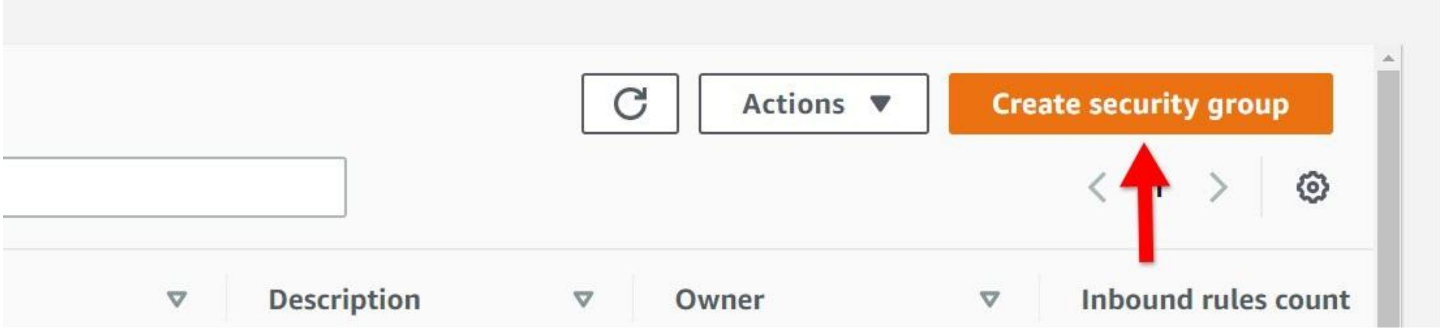
After reviewing your EC2 server options click the Launch button on the bottom right to create and start the server.

2.1 AWS Security Group (firewall) Configuration

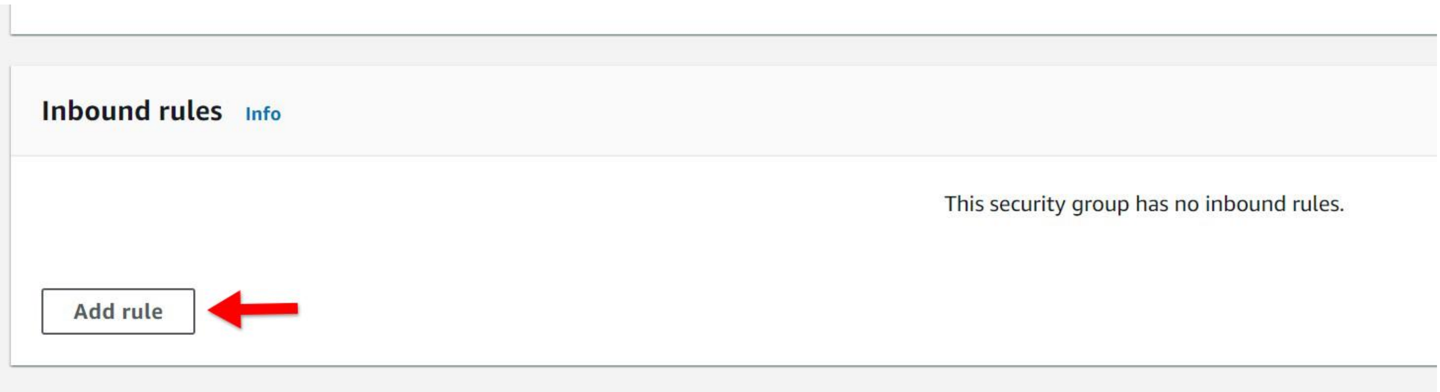
VCOM Virtual Matrix uses a variety of ports which will need to be open for the software to function properly. This portion of the guide will show you how to create to configure an AWS Security Group for VCOM Virtual Matrix.



From the left-hand site of the AWS EC2 Management Console click the Security Groups option under the Network & Security section.



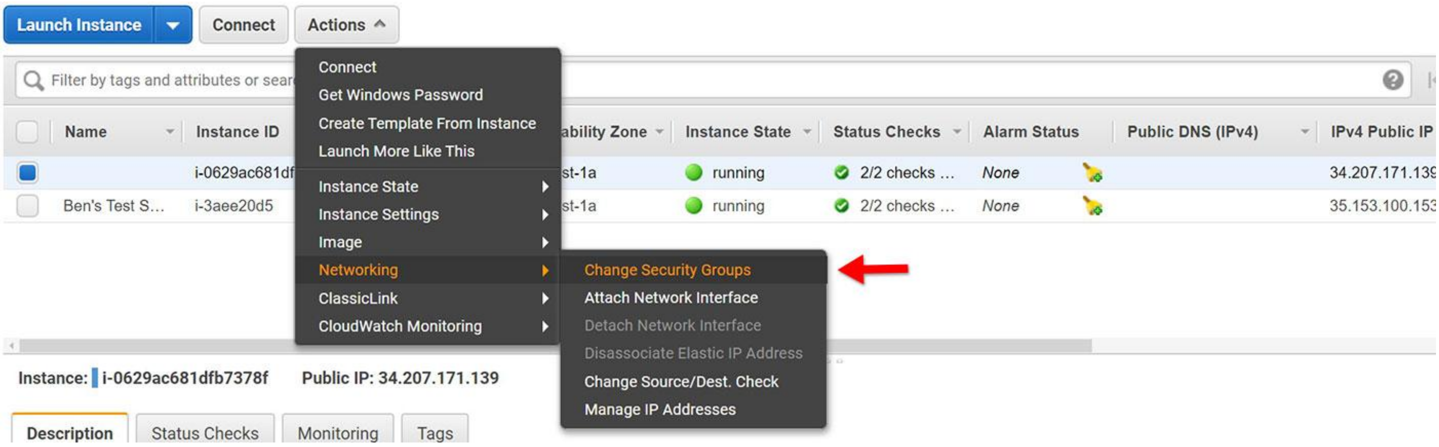
On the top right click Create security group.



This security group has no inbound rules.

Enter a Security group name and Description (other options can be left default). Scroll down and under the Inbound rules section click Add rule. A list of ports used by VCOM Virtual Matrix is available in the Network Requirements section of our documentation. Add a rule for every required port.

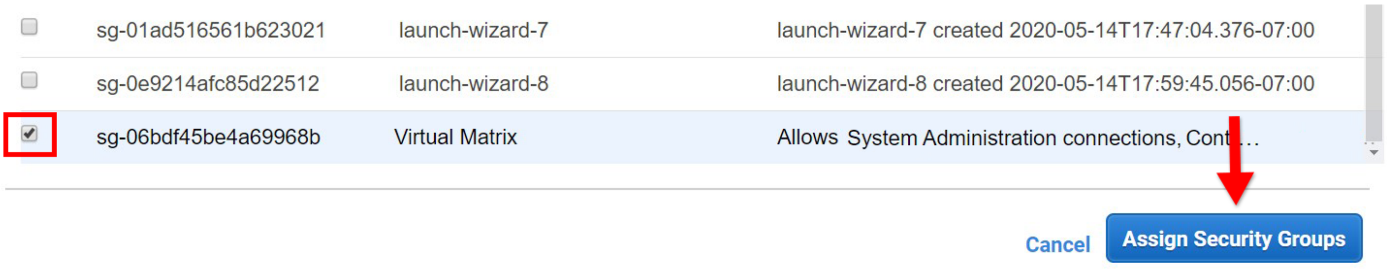
Note: If you do not add an inbound rule for port 3389 TCP & UDP you will not be able to connect to the server via RDP.



Name	Instance ID	ability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
	i-0629ac681df	st-1a	running	2/2 checks ...	None		34.207.171.139
Ben's Test S...	i-3aee20d5	st-1a	running	2/2 checks ...	None		35.153.100.153

Instance: i-0629ac681dfb7378f Public IP: 34.207.171.139

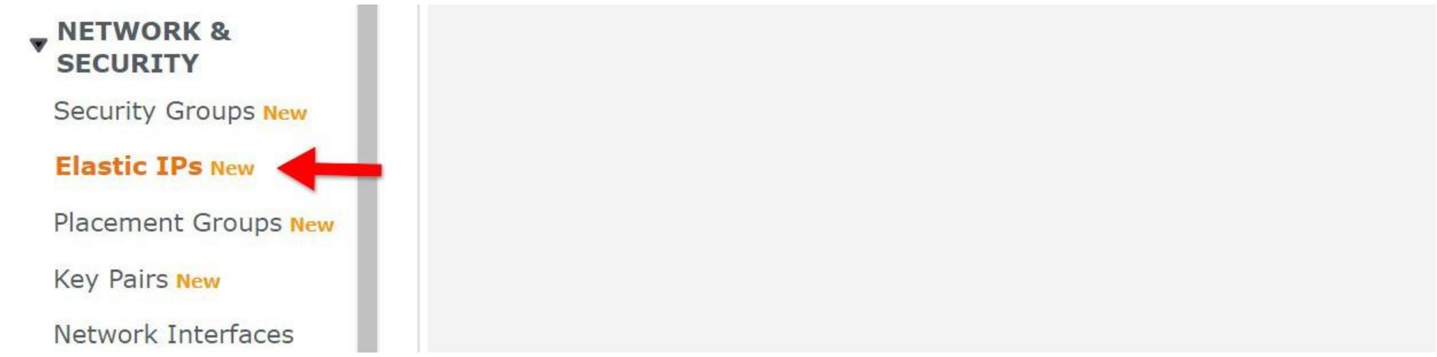
Navigate back to the Instances page and select your new server instance. From the Actions menu at the top go to the Networking section and select Change Security Groups.



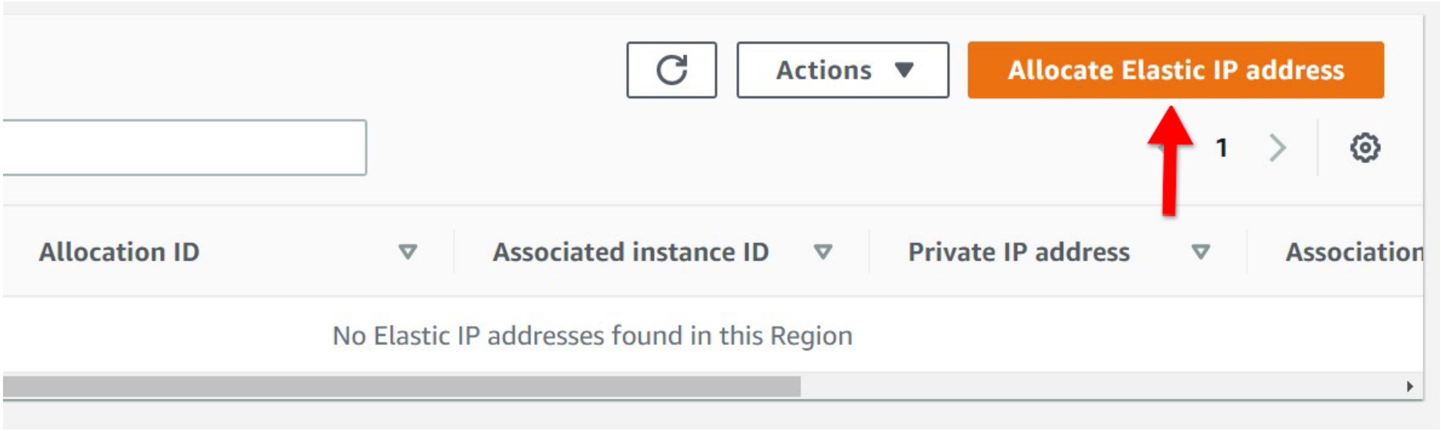
□	sg-01ad516561b623021	launch-wizard-7	launch-wizard-7 created 2020-05-14T17:47:04.376-07:00
□	sg-0e9214afc85d22512	launch-wizard-8	launch-wizard-8 created 2020-05-14T17:59:45.056-07:00
☑	sg-06bdf45be4a69968b	Virtual Matrix	Allows System Administration connections, Cont…

Deselect the default Security Group assigned to the instance and select the Security Group you just created. Finally, click Assign Security Groups to complete the process.

2.2 Static IP Address Configuration (recommended)



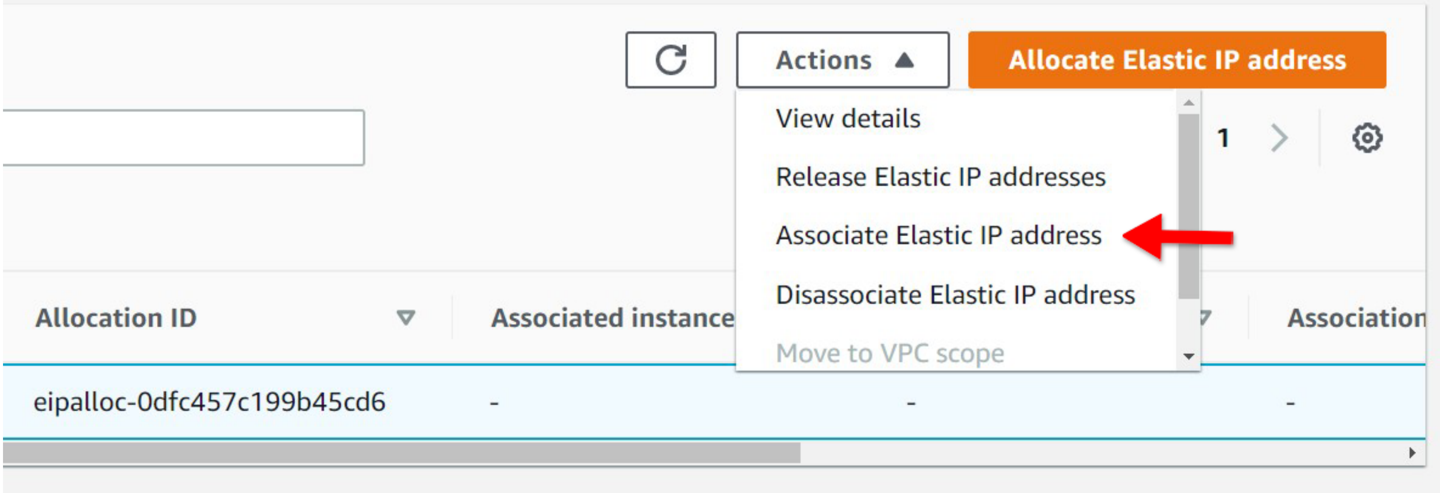
From the left side menu select Elastic IPs



Allocation ID	Associated instance ID	Private IP address	Association

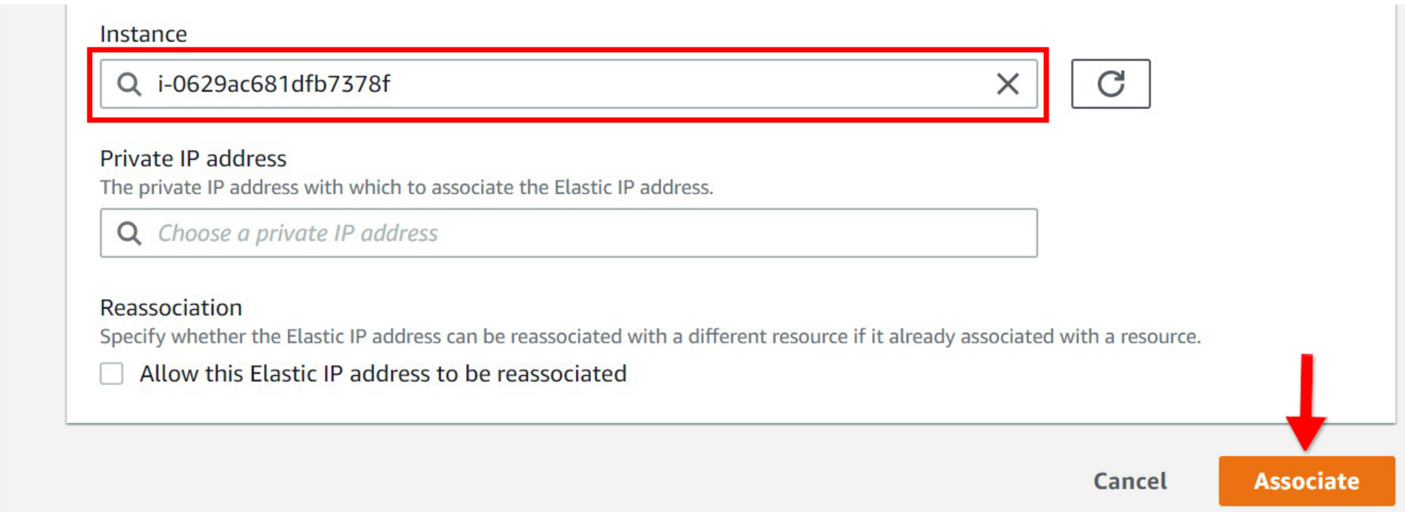
No Elastic IP addresses found in this Region

Click Allocate Elastic IP address on the top right. Leave all options as default and click Allocate.


Actions
Allocate Elastic IP address
View details
Release Elastic IP addresses
Associate Elastic IP address
Disassociate Elastic IP address
Move to VPC scope
1

Allocation ID	Associated instance		Association
eipalloc-0dfc457c199b45cd6	-	-	-

Ensure that the IP address you were just given is selected on the list and then from the Actions menu select Associate Elastic IP address.



Instance

i-0629ac681dfb7378f

Private IP address

The private IP address with which to associate the Elastic IP address.

Choose a private IP address

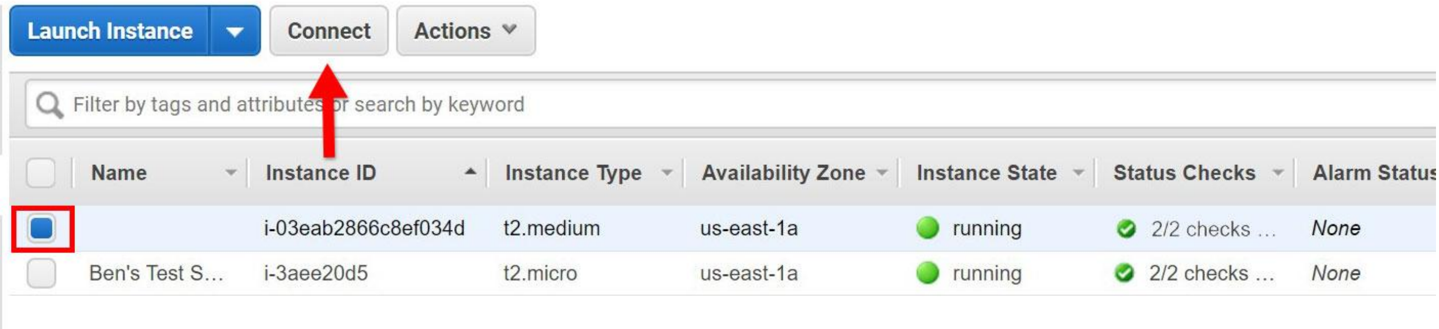
Reassociation

Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.

□ Allow this Elastic IP address to be reassociated

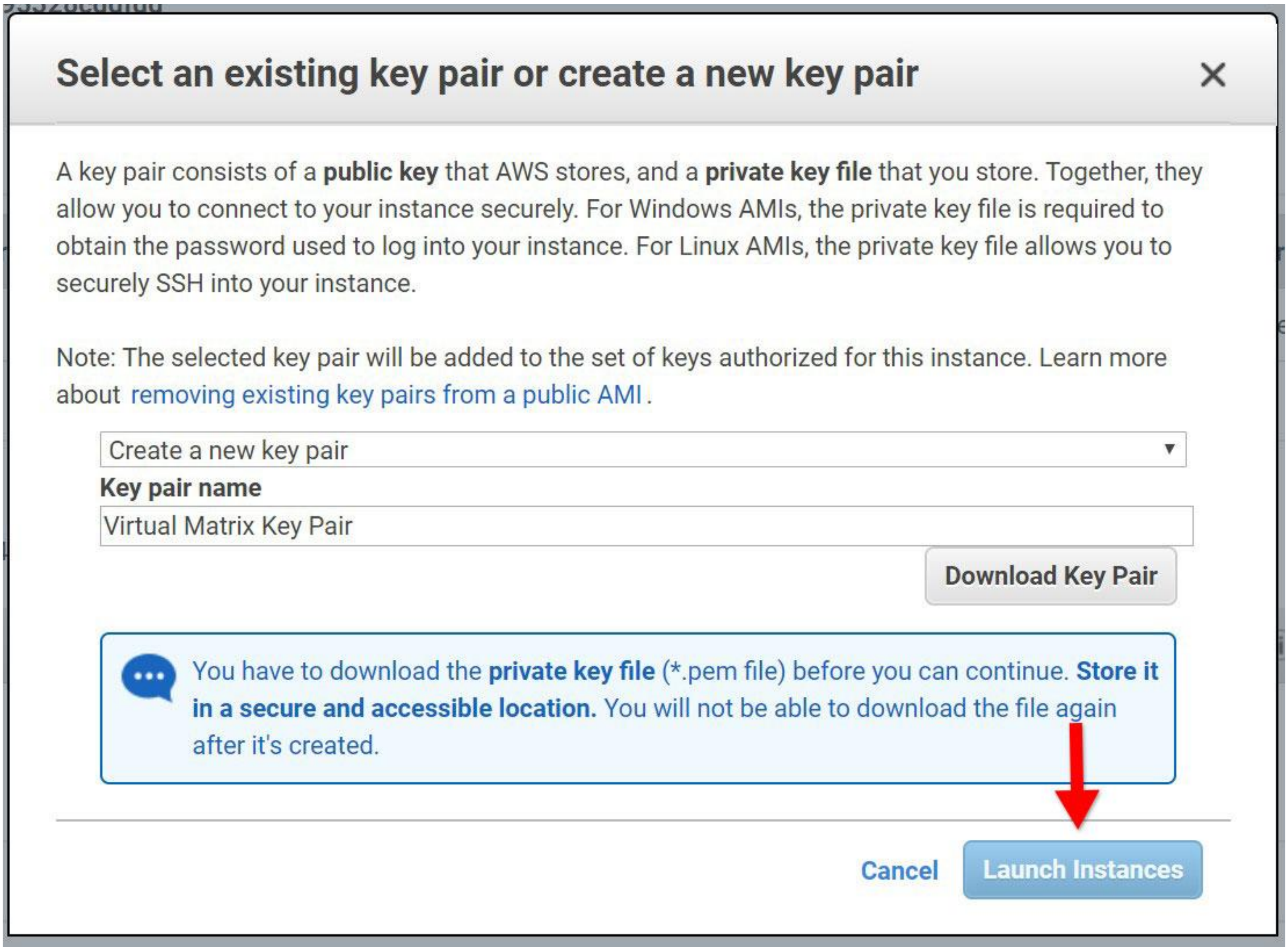
Select your EC2 instance from the list and then click Associate. All other options can be left default.

2.3 Connecting to the EC2 Instance



	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status
☑		i-03eab2866c8ef034d	t2.medium	us-east-1a	● running	✓ 2/2 checks ...	*None*
□	Ben's Test S...	i-3aee20d5	t2.micro	us-east-1a	● running	✓ 2/2 checks ...	*None*

Select your server from the list and click the Connect button at the top.



Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI .

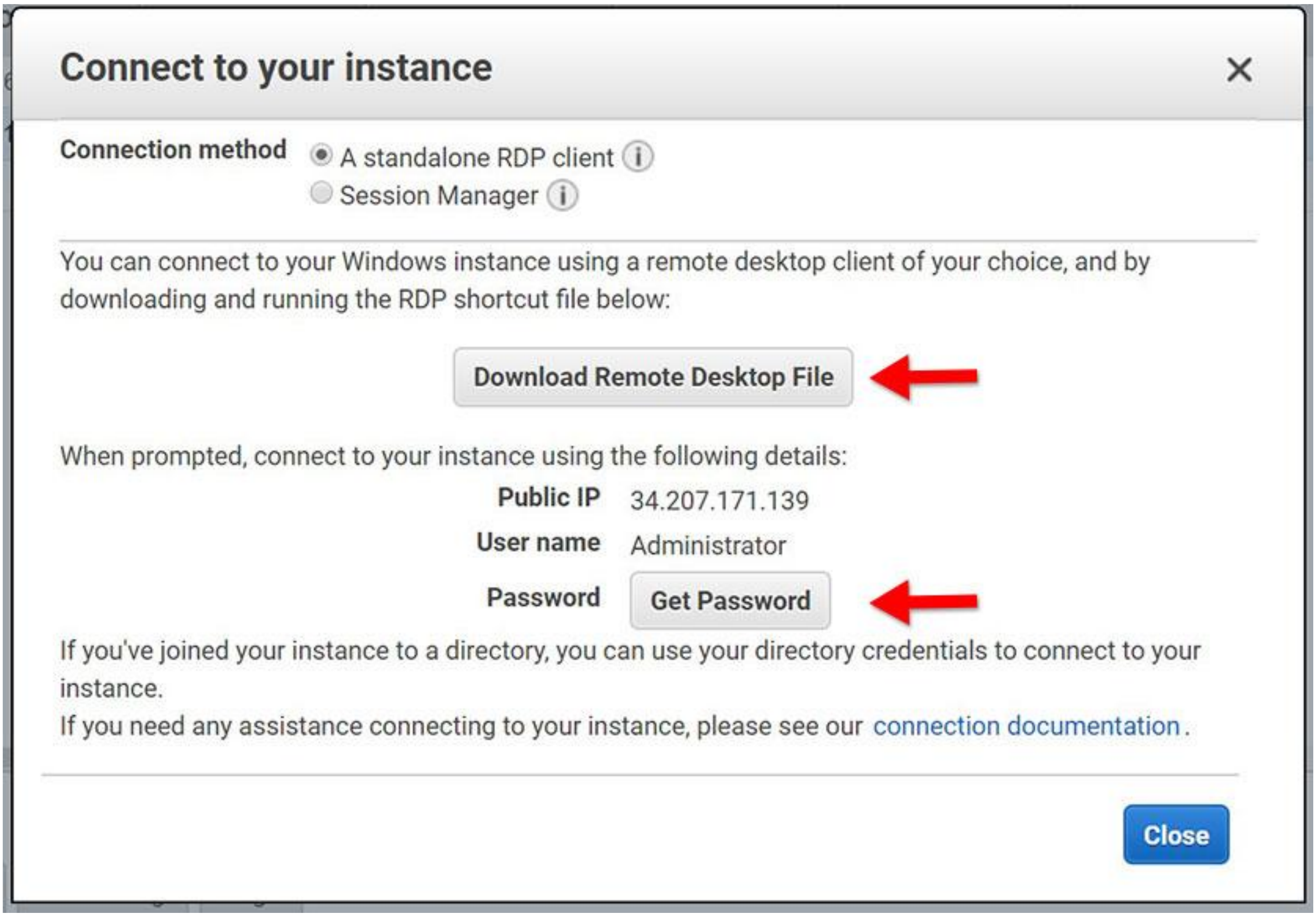
Create a new key pair ▾

Key pair name

Virtual Matrix Key Pair

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

The options you select from this menu will vary depending on if you have an existing key pair you want to use or wish to continue without a key pair. For the purposes of this guide I have chosen to create a new key pair. If you create a new key pair, you will need to enter a name and then download the key pair. After completing these steps click Launch Instances



Connect to your instance

Connection method ● A standalone RDP client ○ Session Manager

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

When prompted, connect to your instance using the following details:

Public IP 34.207.171.139

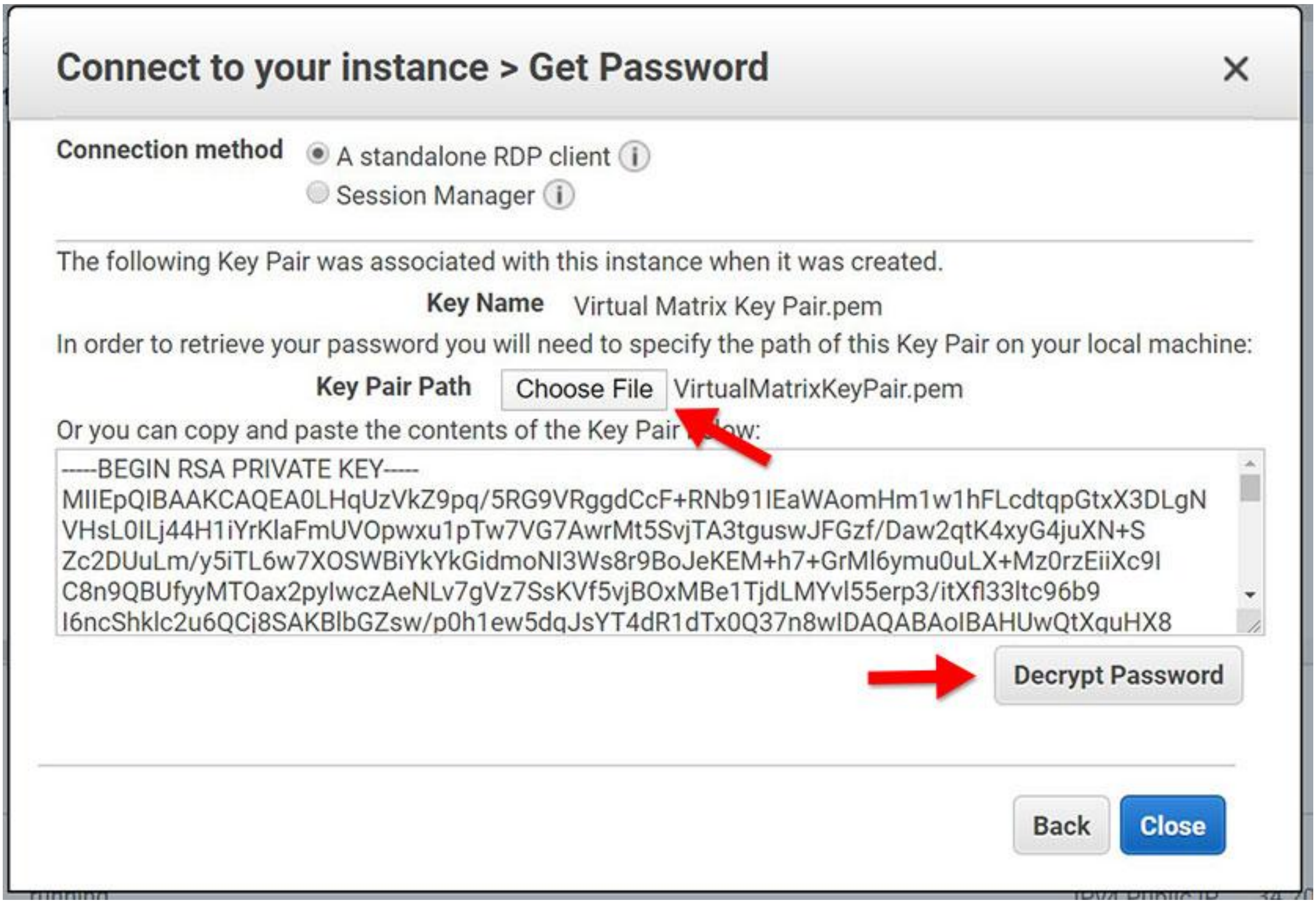
User name Administrator

Password

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

If you need any assistance connecting to your instance, please see our connection documentation.

Click the button to Download Remote Desktop File and then Click the Get Password button. Save the Remote Desktop File and remember its location as you will need it in the next section of this guide.



Connect to your instance > Get Password ✕

Connection method ● A standalone RDP client ⓘ
○ Session Manager ⓘ

The following Key Pair was associated with this instance when it was created.

Key Name Virtual Matrix Key Pair.pem

In order to retrieve your password you will need to specify the path of this Key Pair on your local machine:

Key Pair Path [Choose File] VirtualMatrixKeyPair.pem

Or you can copy and paste the contents of the Key Pair below:

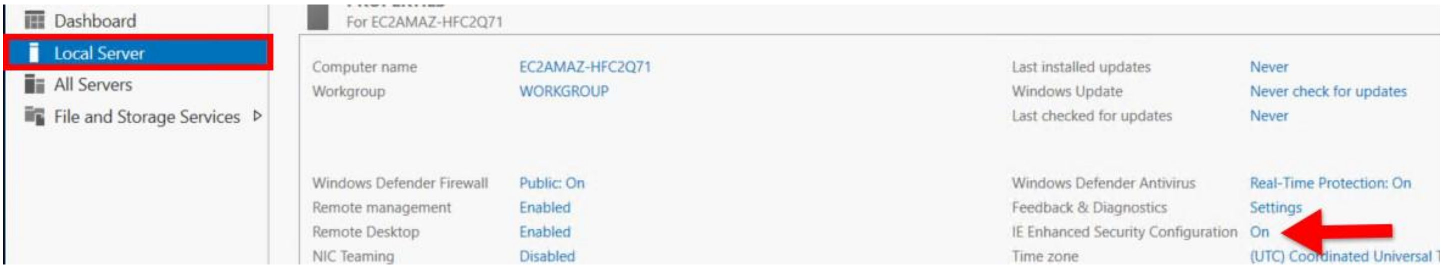
```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA0LHqUzVkZ9pq/5RG9VRggdCcF+RNb91IEaWAomHm1w1hFLcdtqpGtxX3DLgN
VHsL0ILj44H1iYrKlaFmUVOpwxu1pTw7VG7AwrMt5SvjTA3tguswJFGzf/Daw2qtK4xyG4juXN+S
Zc2DUuLm/y5iTL6w7XOSWBiYkYkGidmoNI3Ws8r9BoJeKEM+h7+GrMl6ymu0uLX+Mz0rzEiiXc9I
C8n9QBUfyyMTOax2pylwczAeNLv7gVz7SsKVf5vjBOxMBe1TjdLMYvl55erp3/itXfl33ltc96b9
I6ncShklc2u6QCj8SAKBlbGZsw/p0h1ew5dqJsYT4dR1dTx0Q37n8wIDAQABAoIBAHUwQtXquHX8
```

Click the Choose File button and then navigate to your saved key pair file to upload it. Then, click the Decrypt Password button and copy your password. It is recommended to save the password somewhere so you can connect to the server in the next section.

2.4 Configuring the EC2 Instance

Disabling Internet Explorer Enhanced Security

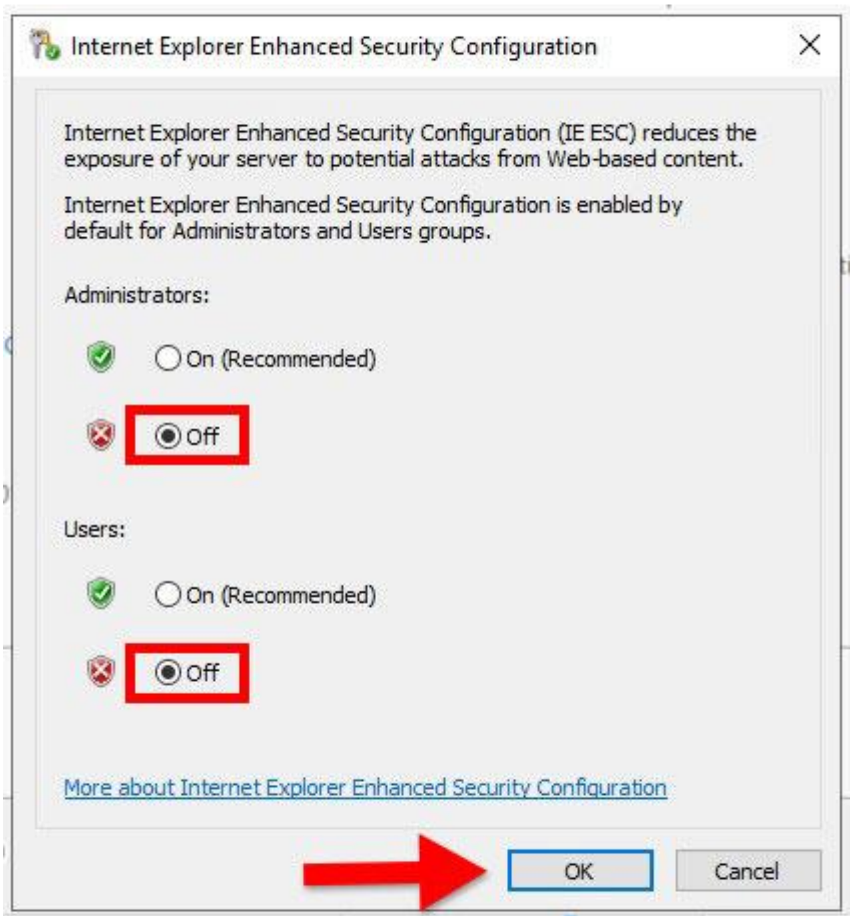
By default, IE does not downloading files from the internet. This portion of the guide will show you how to disable IE Enhanced Security. This step is necessary only if you are using Windows Server and plan to download VCOM Virtual Matrix from the internet. You can skip this portion of the guide if you plan to transfer the VCOM Virtual Matrix installer to the server using RDP.



For EC2AMAZ-HFC2Q71

Computer name	EC2AMAZ-HFC2Q71	Last installed updates	Never
Workgroup	WORKGROUP	Windows Update	Never check for updates
		Last checked for updates	Never
Windows Defender Firewall	Public: On	Windows Defender Antivirus	Real-Time Protection: On
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Enabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC) Coordinated Universal T

To connect to your server double click the Remote Desktop File and paste in your password when prompted. If you select the Remember me option, then you will not need to renter the credentials in the future. By default, Windows Server will have IE Enhanced Security enabled. With this setting turned on you will not be able to download the VCOM Virtual Matrix software via the internet. To disable it, launch the Server Manager application and then select Local Server from the left. On the right, click the On button next to the line that says IE Enhanced Security Configuration.


Internet Explorer Enhanced Security Configuration

Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.

Internet Explorer Enhanced Security Configuration is enabled by default for Administrators and Users groups.

Administrators:

○ On (Recommended)

● Off

Users:

○ On (Recommended)

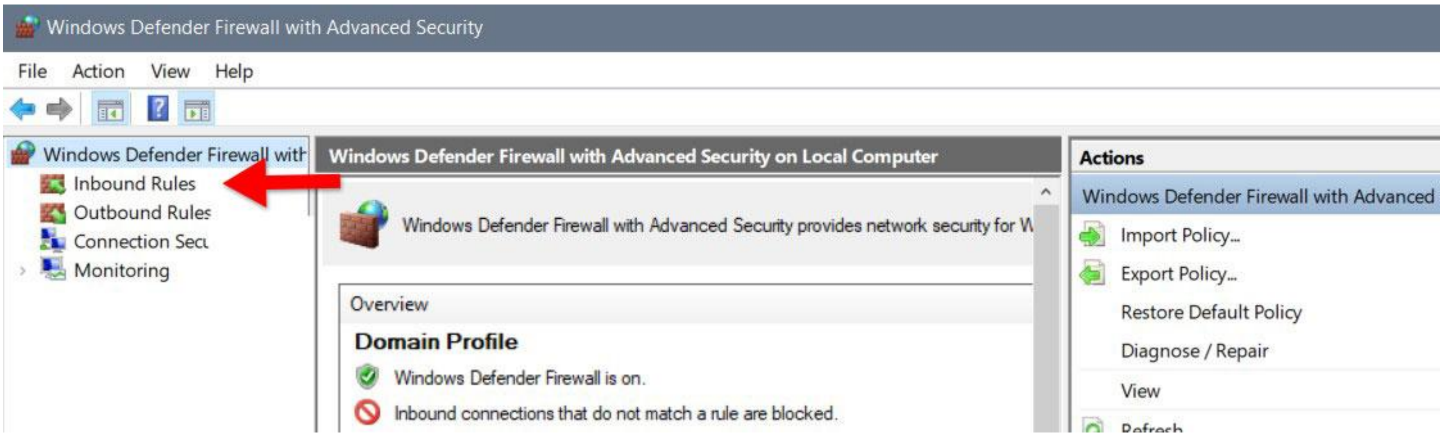
● Off

More about Internet Explorer Enhanced Security Configuration

Disable the IE Enhanced Security Configuration as show above then click Ok. You will now be able to download the VCOM Virtual Matrix Software from our website.

Windows Firewall Configuration

You will need to either disable the Windows firewall entirely or configure Inbound Rules for all of the ports required by VCOM Virtual Matrix. To create an Inbound Rule launch the Control Panel > Firewall > Advanced Settings. Click Inbound Rules and then click New Rule. A list of ports used by VCOM Virtual Matrix is available in the Network Requirements section of our documentation. Add a rule for every required port.


Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Secu
Monitoring
Windows Defender Firewall with Advanced Security on Local Computer
Actions
Windows Defender Firewall with Advanced
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Overview

Windows Defender Firewall with Advanced Security provides network security for W

Domain Profile

Windows Defender Firewall is on.

Inbound connections that do not match a rule are blocked.

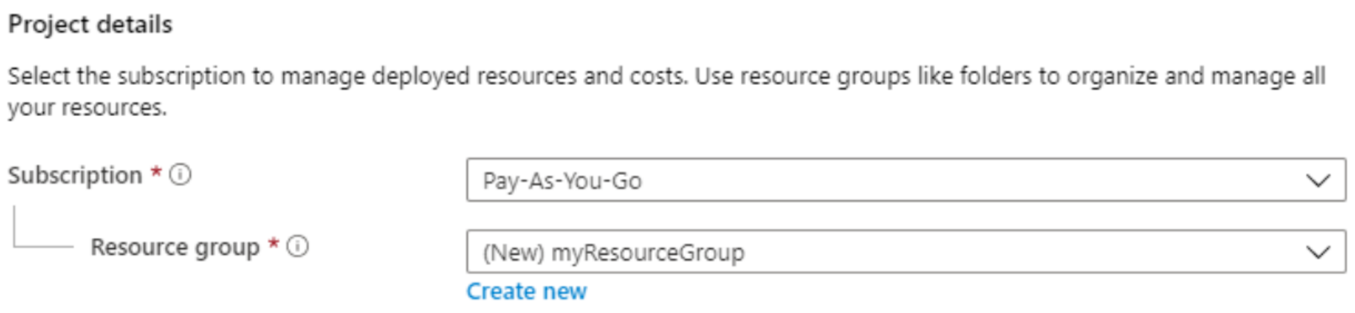
Software Installation and Licensing

Please follow the VCOM Virtual Matrix Software Installation and Licensing documentation to complete the setup.

3. Azure Installation

This portion of the guide will show you how to create a virtual machine in the Azure Cloud.

From the Services menu select Virtual Machines. From the Virtual Machines page select Create and then select Virtual Machine.



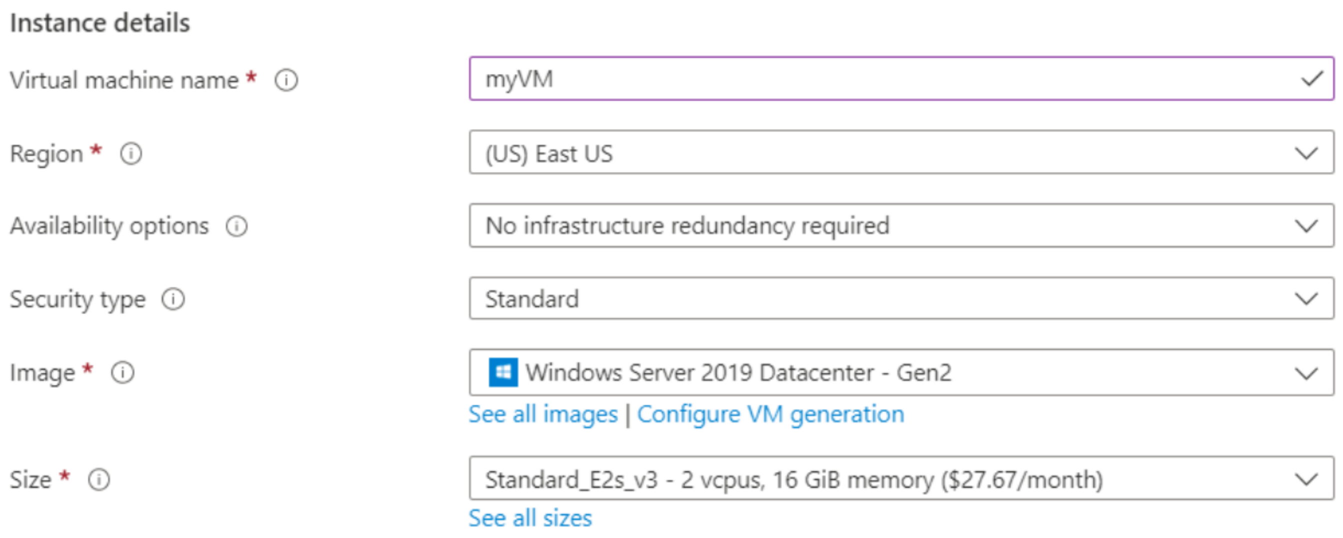
Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ: Pay-As-You-Go

Resource group * ⓘ: (New) myResourceGroup

Select the Basics tab and select an existing Resource group or create a new one.



Instance details

Virtual machine name * ⓘ: myVM

Region * ⓘ: (US) East US

Availability options ⓘ: No infrastructure redundancy required

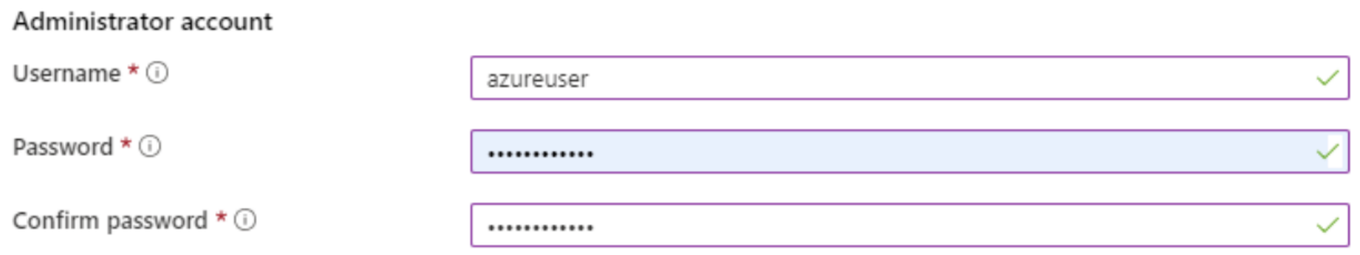
Security type ⓘ: Standard

Image * ⓘ: Windows Server 2019 Datacenter - Gen2

Size * ⓘ: Standard_E2s_v3 - 2 vcpus, 16 GiB memory ($27.67/month)

Specify your instance details. System hardware requirements are dependent on the number of concurrent users that will be accessing the system. Please refer to the VCOM Virtual Matrix Intercom System Requirements for more information.

Note: VCOM can be run on all modern Windows Operating Systems. You may use a different version than what is show above.



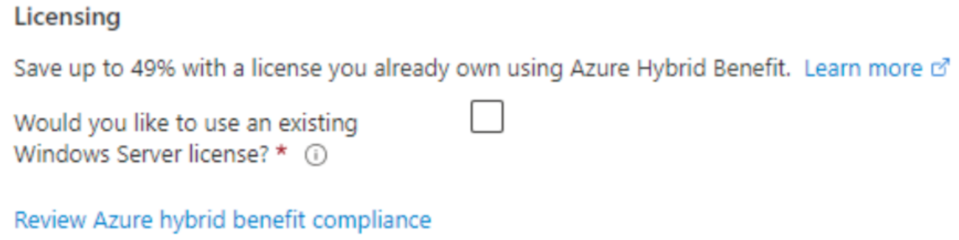
Administrator account

Username * ⓘ azureuser ✓

Password * ⓘ •••••••••••• ✓

Confirm password * ⓘ •••••••••••• ✓

Under Administrator account provide a username and password.

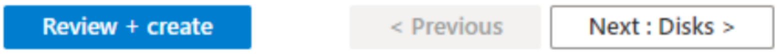


Licensing

Save up to 49% with a license you already own using Azure Hybrid Benefit. Learn more

Would you like to use an existing Windows Server license? * ⓘ □

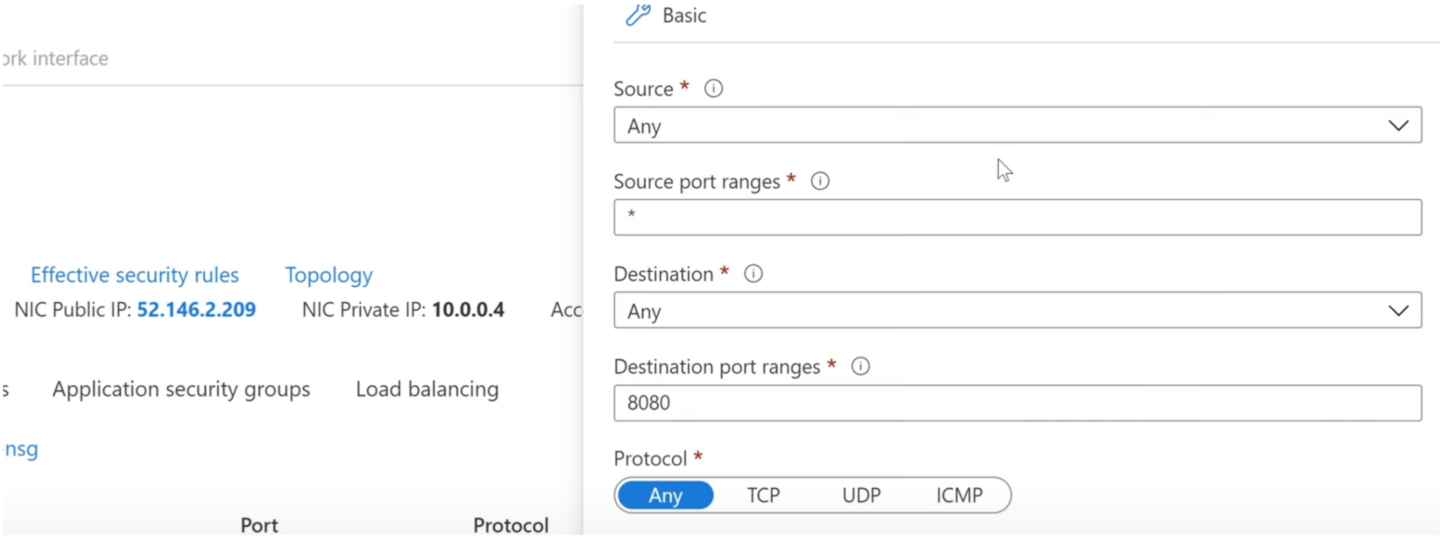
Review Azure hybrid benefit compliance



Click the Review + Create button at the bottom of the page.

3.1 Firewall Configuration

On the left side of the screen select Networking and then click Add inbound port rule.



NIC Public IP: 52.146.2.209

NIC Private IP: 10.0.0.4

Source * ⓘ Any

Source port ranges * ⓘ *

Destination * ⓘ Any

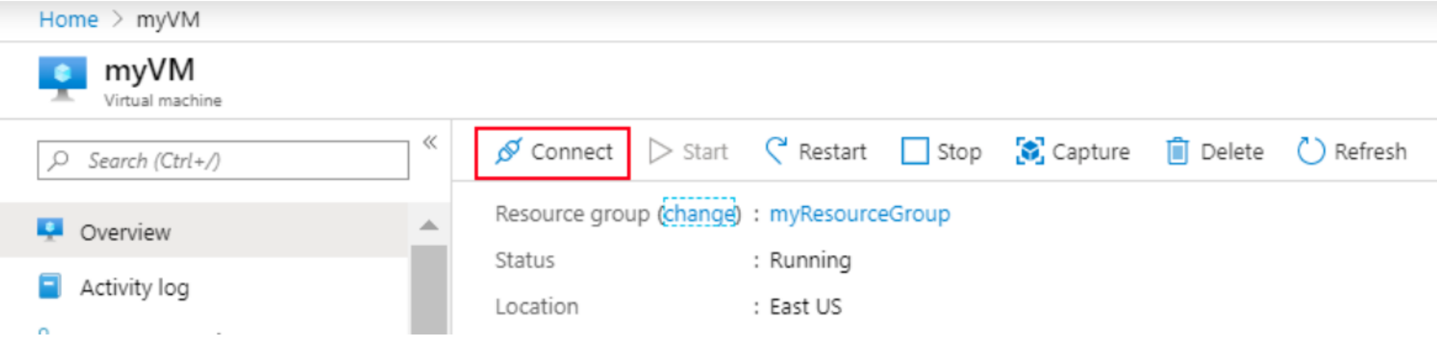
Destination port ranges * ⓘ 8080

Protocol * [✓ Any] TCP UDP ICMP

A list of ports used by VCOM Virtual Matrix is available in the Network Requirements section of our documentation. Add a rule for every required port.

Note: If you do not add an inbound rule for port 3389 TCP & UDP you will not be able to connect to the server via RDP.

3.2 Connecting to the server instance

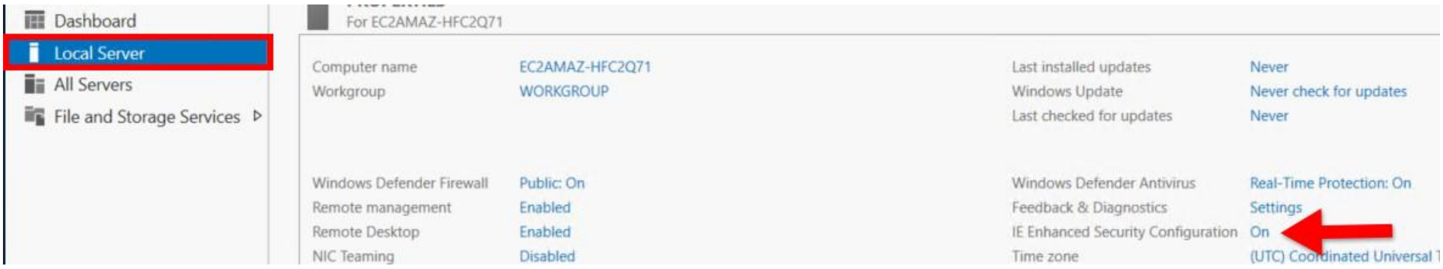


Resource group (change) : myResourceGroup
Status : Running
Location : East US

From the Overview page select Connect and then RDP. Then click Download RDP file. Double click the RDP file and click connect then enter in the username and password for the server.

3.3 Configuring the server instance

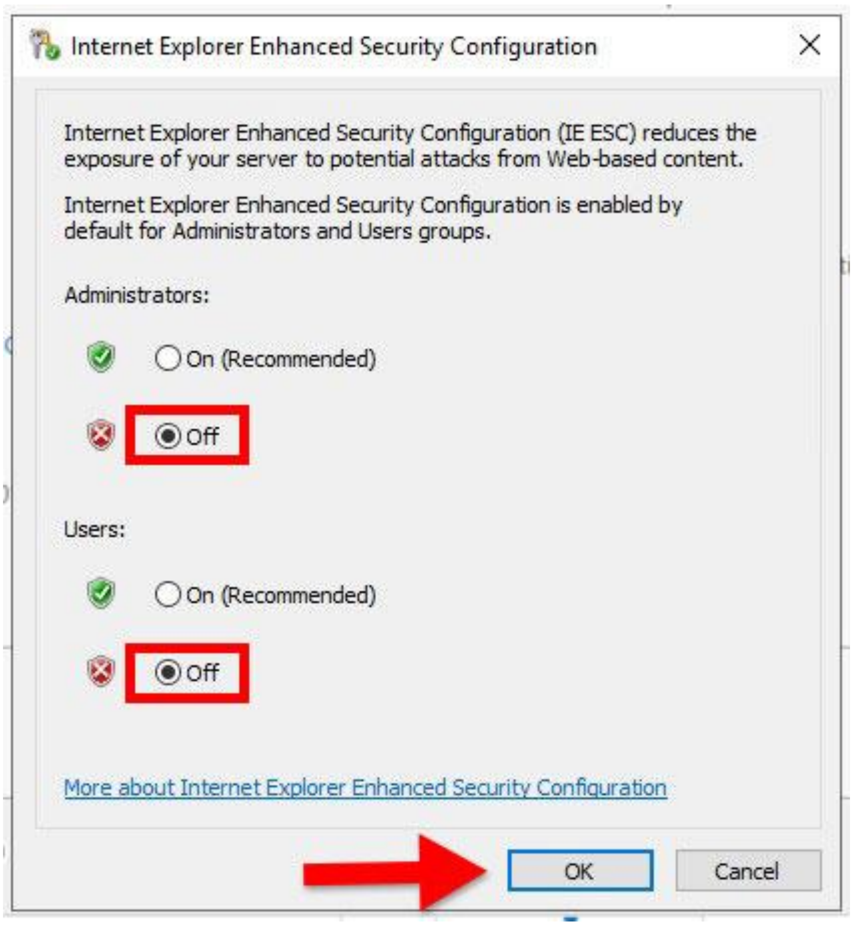
Disabling Internet Explorer Enhanced Security
By default, IE does not downloading files from the internet. This portion of the guide will show you how to disable IE Enhanced Security. This step is necessary only if you are using Windows Server and plan to download VCOM Virtual Matrix from the internet. You can skip this portion of the guide if you plan to transfer the VCOM Virtual Matrix installer to the server using RDP.



For EC2AMAZ-HFC2Q71

Computer name	EC2AMAZ-HFC2Q71	Last installed updates	Never
Workgroup	WORKGROUP	Windows Update	Never check for updates
		Last checked for updates	Never
Windows Defender Firewall	Public: On	Windows Defender Antivirus	Real-Time Protection: On
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Enabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC) Coordinated Universal T

To connect to your server double click the Remote Desktop File and paste in your password when prompted. If you select the Remember me option, then you will not need to renter the credentials in the future. By default, Windows Server will have IE Enhanced Security enabled. With this setting turned on you will not be able to download the VCOM Virtual Matrix software via the internet. To disable it, launch the Server Manager application and then select Local Server from the left. On the right, click the On button next to the line that says IE Enhanced Security Configuration.



Internet Explorer Enhanced Security Configuration

Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.

Internet Explorer Enhanced Security Configuration is enabled by default for Administrators and Users groups.

Administrators:

○ On (Recommended)

● Off

Users:

○ On (Recommended)

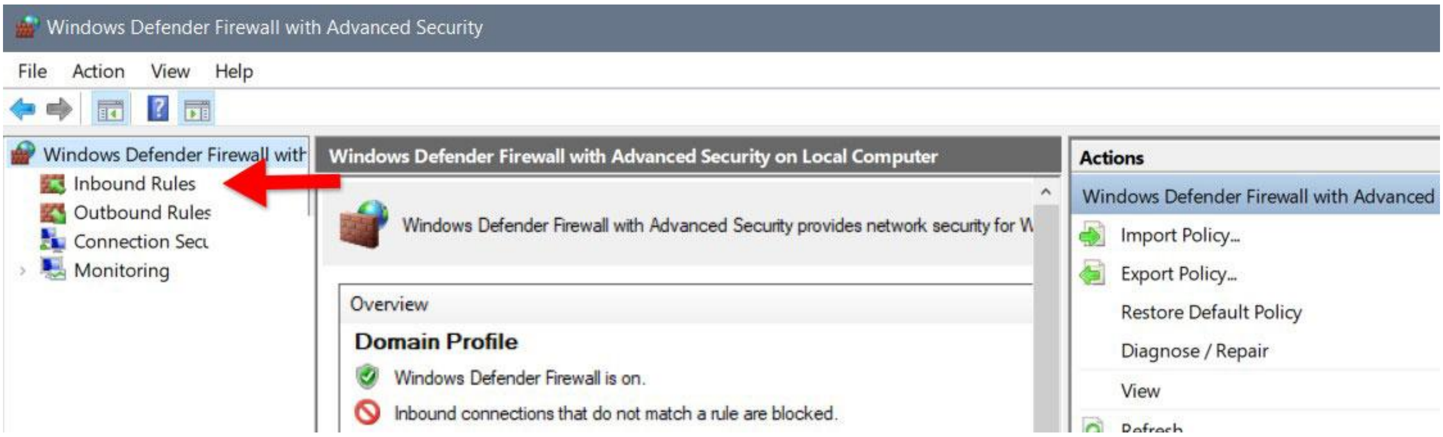
● Off

More about Internet Explorer Enhanced Security Configuration

Disable the IE Enhanced Security Configuration as show above then click Ok. You will now be able to download the VCOM Virtual Matrix Software from our website.

Windows Firewall Configuration

You will need to either disable the Windows firewall entirely or configure Inbound Rules for all of the ports required by VCOM Virtual Matrix. To create an Inbound Rule launch the Control Panel > Firewall > Advanced Settings. Click Inbound Rules and then click New Rule. A list of ports used by VCOM Virtual Matrix is available in the Network Requirements section of our documentation. Add a rule for every required port.


Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Secu
Monitoring
Windows Defender Firewall with Advanced Security on Local Computer
Windows Defender Firewall with Advanced Security provides network security for W
Overview
Domain Profile
Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Actions
Windows Defender Firewall with Advanced
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh

Software Installation and Licensing

Please follow the VCOM Virtual Matrix Software Installation and Licensing documentation to complete the setup.

4. TURN Server Provisioning

The open-source TURN server called Coturn is highly recommended as the TURN server to be installed, if a TURN server is required, although likely any TURN server can be used. Following are the requirements and setup instructions for the Coturn TURN server.

4.1 Minimum Server Requirements

Operating System: Linux (recommend Ubuntu 18.3 or higher)
CPU Requirements: 2 vCPUs
RAM: 2 GB
DISK: 10 GB
Network bandwidth required per client: 100 Kbps (aka 1000 clients per 100 Mbps of bandwidth)
Approximate Clients per vCPU: 100

4.2 Software Installation

Once the cloud-based server has been provisioned, access the server via SSH (Secure Shell). To install the server, perform the following steps:

Install the Coturn Software
1. Run `sudo apt-get update`.
2. Run `sudo apt-get upgrade`.
3. Run `sudo apt-get install coturn`.

Download and Install the Configuration File
4. Preserve the default Coturn configuration file by running `mv /etc/turnserver.conf /etc/turnserver.conf.original`.
5. Download the preconfigured ‘turnserver.conf’ configuration here.

By default, the Coturn server will be accessible on the default TURN port # of 3478 with a Username of ‘intracom’ and Password of ‘vcom’. If a different port #, Username or Password is desired, these items can be changed in this configuration file.

6. Using the SCP (Secure Copy) protocol of SSH, or any other applicable method, copy the pre-configured ‘turnserver.conf’ configuration file to the /etc directory.

Start the Server

7. Run `systemctl start coturn` to start the server.

Connect the Coturn Server to the VCOM Server

8. To have the VCOM server use the newly provisioned TURN server, login to the System Administration and from the System → System Settings dialog, change the ICE Server Host Name to 'turn:<TURN_SERVER_HOST_NAME>:<TURN_SERVER_PORT_NUMBER>’ and configure the ICE Server User Name and ICE Server Password as appropriate.

5. Video Media Server

The VCOM WebRTC Control Panels have live video capture and streaming functionality. Clients can stream their webcam video into the system which can then be viewed by other clients. Your server must be licensed to use this functionality and a separate, Linux-based server needs to be provisioned to run the Media Server.

5.1 Installation

The server can be bare metal or virtualized. A system configured with the below specifications can handle approximately 20 streams with 40 viewers. As there is no upper limit on the number of connections and since video server resource utilization is linear, the maximum number of streams supported can be increased simply by providing a more powerful system.

Minimum System Requirements:
Processor: 2Ghz dual core
Memory: 4Gb
Storage: 25Gb
OS: Ubuntu 18.04 LTS, an ISO is available to download here

On the Linux server open a Terminal window and run the following command:

```
wget -O - https:rts''-downloads.s3.amazonaws.com/Install_Video_Media_Server.sh | bash
```

Note: The above command will download a script that will update your system's package information. If this fails you can try running sudo apt-get update or try running the Software Updater application that comes installed with Ubuntu.

The Video Media Server will be installed as a service and will be set to run on system startup. The service will automatically start after the installation.

The following commands can be used to manually start or stop the Media Server:

```
sudo service kurento-media-server start
```

```
sudo service kurento-media-server stop
```

5.2 STUN Server

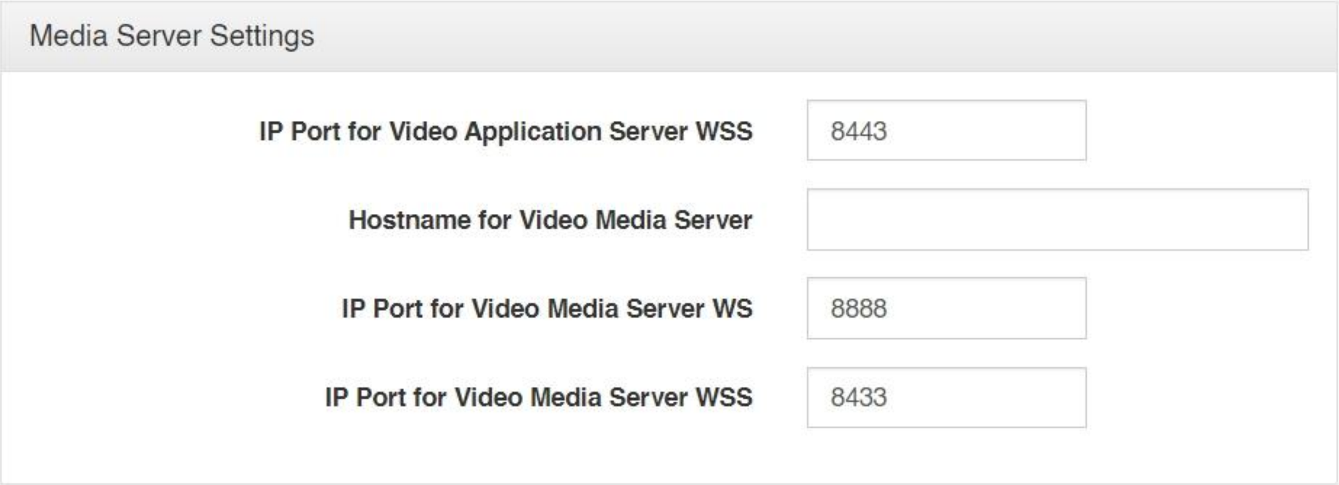
If the Media Server is deployed behind a NAT it is necessary to configure the Media Server to use a STUN server. Follow the steps below to configure the Media Server to use Google's public STUN server.

1. Run the following command: `sudo nano /etc/kurento/modules/kurento/WebRtcEndpoint.conf.ini`
2. Paste the following lines into the file:

   `stunServerAddress=172.253.117.127`

   `stunServerPort=19302`
3. Type ctrl + X to finish editing the file. When prompted, press Y to save changes and then press Enter.
4. Run the following command: `sudo service kurento-media-server restart`

5.3 Configuration



Media Server Settings

IP Port for Video Application Server WSS	8443
Hostname for Video Media Server	
IP Port for Video Media Server WS	8888
IP Port for Video Media Server WSS	8433

After the installation go into the System Administration and click the System Configuration tab. Enter in the Hostname of the Video Media Server then click save.

6. System Administration

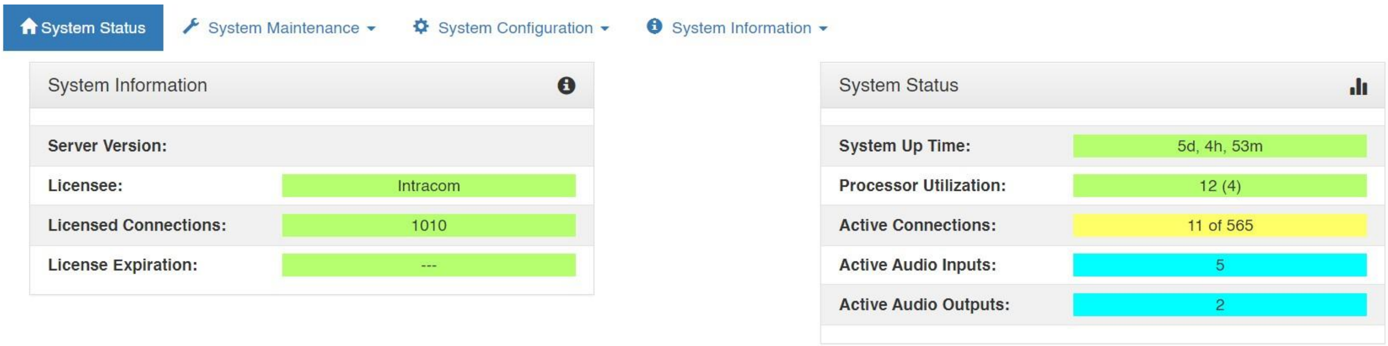
6.1 Logging In

If you are using the VCOM System Administration from the same machine VCOM is installed on:
After VCOM Virtual Matrix is installed on the machine, a shortcut will be placed on the desktop called ‘VCOM System Administration.’ Click on the shortcut. A browser window will appear. The VCOM System Administration application can also be accessed by typing ‘localhost’ into the URL box and pressing enter.

If you are using the VCOM System Administration from a different machine:
Open a browser window and type the local IP address of the machine running VCOM into the URL box and press enter.

The default master ‘Login Name’ and ‘Login Password’ are both ‘admin’. Once logged in, credentials can be changed. After logging in you will be prompted to upload a license file. You will be shown your ‘System Identification Code,’ which is a unique value specific to the computer on which the Virtual Matrix was installed. This code must be provided to your sales representative upon initial installation to obtain a license file that enables the Virtual Matrix to support the number of clients purchased. The license file is not transferable to any other computer. When the license file is received, click ‘Upload License’.

6.2 System Status



System Information

Server Version:	
Licensee:	Intracom
Licensed Connections:	1010
License Expiration:	---

System Status

System Up Time:	5d, 4h, 53m
Processor Utilization:	12 (4)
Active Connections:	11 of 565
Active Audio Inputs:	5
Active Audio Outputs:	2

System Information fields are color-coded. Red indicates a problem; Yellow a potential problem; and Green normal operations. Blue fields are informational. The ‘System Information’ area in the upper, left-hand side of the System Administration main window displays the name of the licensee, the number of clients licensed, and expiration date. ‘License Expiration’ will typically display ‘---’ which means a system has been purchased and a perpetual license has been granted. Demo, trial, and rental systems will display a numerical value in days reflecting the limited duration for which a license has been granted.

System Status

System Status fields are color-coded. Red indicates a problem, Yellow a condition that needs attention, and Green normal operations. Blue fields are informational.

The ‘System Status’ on the right side of the System Administration main window displays general system metrics.

System Up Time: Displays how long the VCOM Virtual Matrix has been running in days, hours, and minutes.

Processor Utilization: Displays CPU utilization of the server or PC hosting the VCOM Virtual Matrix.

Failover Status: Displays the operational status of the Primary and Secondary servers when Failover is licensed and configured.

Active Connections: Displays how many clients are connected to the Virtual Matrix at any given moment out of how many clients are configured. Clients include VCOM Control Panels, VCOM Device Interfaces, and SIP Devices.

Active Audio Inputs: Displays how many active audio channels are being streamed from clients into the Virtual Matrix at any given time.

Active Audio Outputs: Displays how many active audio channels are being streamed out of the Virtual Matrix to clients at any given time.

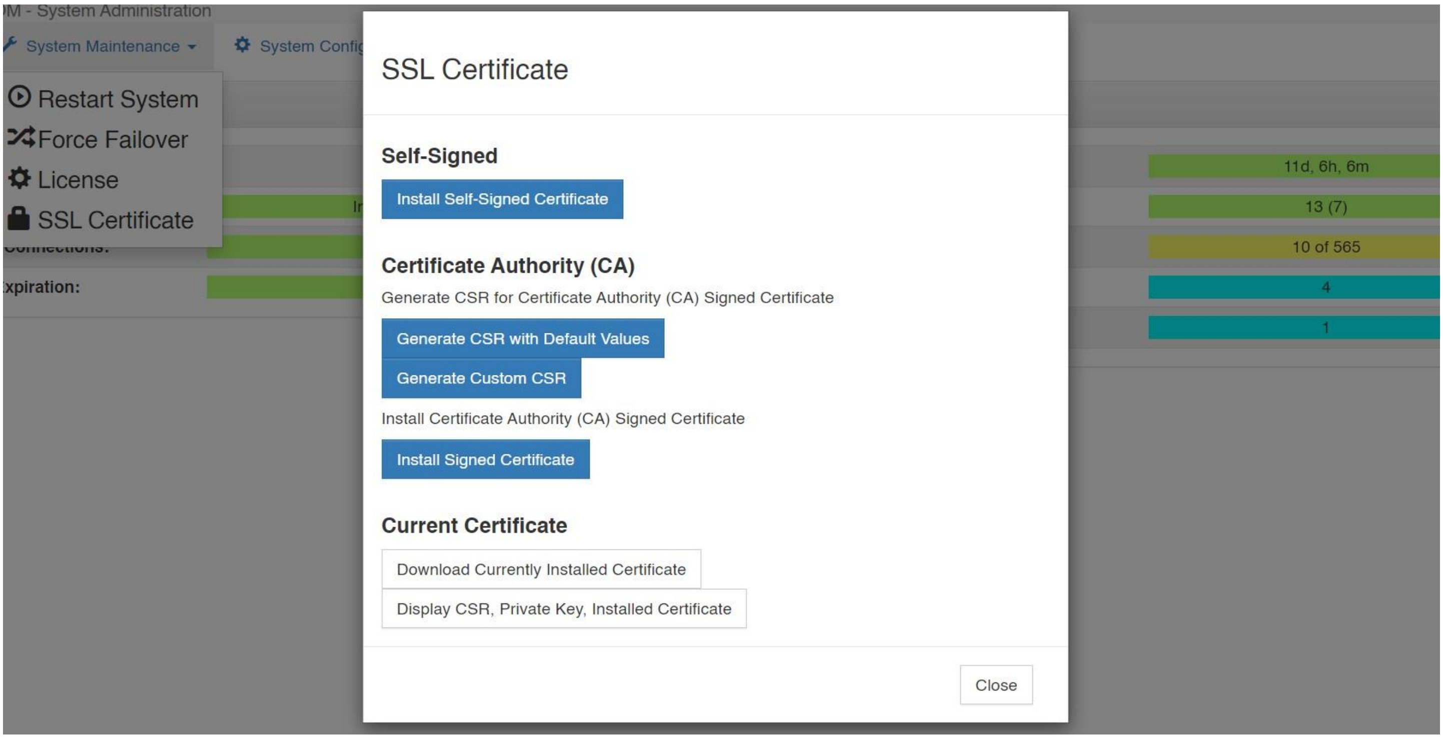
6.3 System Maintenance

Restart System: This feature restarts the system. A warning message will first appear noting that selecting this feature will temporarily render the system inoperable and asking if you wish to proceed. This feature is only available to the system administrator logged in with the master username and password.

Force Failover: Forces the Primary to relinquish control to Secondary Server.

Force Failback: Forces the Secondary to relinquish control to Primary Server.

6.3.1 SSL Certificate


M - System Administration
System Maintenance
System Config
Restart System
Force Failover
License
SSL Certificate
xpiration:
11d, 6h, 6m
13 (7)
10 of 565
4
1
Install Self-Signed Certificate
Generate CSR with Default Values
Generate Custom CSR
Install Signed Certificate
Download Currently Installed Certificate
Display CSR, Private Key, Installed Certificate
Close

SSL Certificate

Self-Signed

Certificate Authority (CA)

Generate CSR for Certificate Authority (CA) Signed Certificate

Install Certificate Authority (CA) Signed Certificate

Current Certificate

VCOM Virtual Matrix generates its own self-signed certificate upon initial launch. All data transmitted between the VCOM Virtual Matrix and the System Administration as well as the VCOM WebRTC Control Panels is encrypted. However, browsers will display a warning because a self-signed certificate is being used. It is possible to install a certificate signed by a Certificate Authority in which case no browser warning will be displayed.

Install Self-Signed Certificate: Generates and installs a self-signed certificate onto the VCOM server.

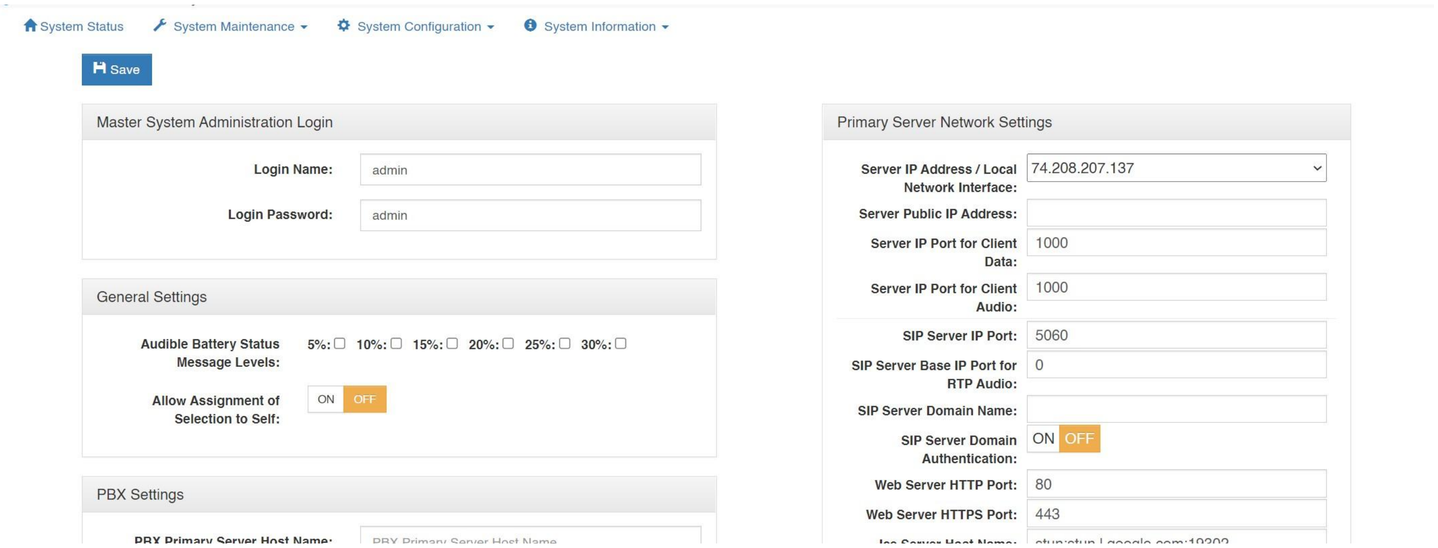
Generate CSR with Default Values: Prompts the user for the Domain Name(s) with which to generate a CSR to send to a Certificate Authority.

Generate Custom CSR: Prompts the user for Domain name(s), Organization Name, County Name, and State/Province. These values are used to generate a CSR to send to a Certificate Authority.

Install Signed Certificate: Installs a certificate generated by a certificate authority.

6.4 System Configuration

6.4.1 System Settings



Master System Administration Login

Login Name: admin

Login Password: admin

General Settings

Audible Battery Status Message Levels: 5%: □ 10%: □ 15%: □ 20%: □ 25%: □ 30%: □

Allow Assignment of Selection to Self: ON [✓ OFF]

PBX Settings

PBX Primary Server Host Name: PBX Primary Server Host Name

Primary Server Network Settings

Server IP Address / Local Network Interface: 74.208.207.137

Server Public IP Address:

Server IP Port for Client Data: 1000

Server IP Port for Client Audio: 1000

SIP Server IP Port: 5060

SIP Server Base IP Port for RTP Audio: 0

SIP Server Domain Name:

SIP Server Domain Authentication: ON [✓ OFF]

Web Server HTTP Port: 80

Web Server HTTPS Port: 443

Ice Server Host Name: stun:stun.l.google.com:19302

Master System Administrator Login : Displays and allows you to edit the master system administrator login name and login password.

Audio Settings

Audio Mix Sample Rate: Controls the maximum sampling rate supported by the Virtual Matrix and thereby dictates the maximum fidelity for all Client connections. There are 3 possible settings: Narrowband (8 KHz), Wideband (16 KHz), and Ultra-Wideband (32 KHz), which is the default setting. Narrowband is approximately the same fidelity as a phone connection while Wideband more closely approximates the fidelity of a professional analog, hardware-based Intercom system. Clients by default will be set to the System's Audio sampling rate. However, the client audio sampling rate can be specified at a lower rate but never at a higher rate. Higher audio sampling rates have more significant requirements both in computational speed and network bandwidth so careful consideration must be made when choosing this setting with respect to server hardware and network infrastructure.

Voice Activity Indication Voice Activity Indication Color: Changes the text color and background color used to indicate voice activity on a given selector. The system interchanges its base colors (yellow text / navy background) with the selected activity indication colors (variable). For typical applications, the default color provides a subtle but noticeable indicator. For some applications, such as maintenance panels for hoot and holler systems, a more pronounced indicator (black text / white background) is generally required.

Audio Output Level Gain (Post-Mix): Adjusts the output level from the VCOM Virtual Matrix to the Control Panels and Device Interfaces in 6dB intervals 3 times to a maximum of 18dB. This is a global change throughout the system.

Primary Server Network Settings

Server IP Address / Local Network Interface: The IP address of the server hosting the Virtual Matrix.

Server Public IP Address: The public IP address that is used to route data to the Server's IP address within the LAN. This is only used when Network Address Translation (NAT) is being used on your LAN.

Server IP Port for VCOM Client Data: The TCP/IP port (default: port 1000) that all client side Control Panels and Device Interfaces use to transport data to the Virtual Matrix. The system has no restriction other than reserved ports. If the Virtual Matrix is behind a firewall and external access is required, a Port Forwarding entry must be added to route all traffic on this port to the internal Virtual Matrix IP address.

Server IP Port for Client Audio: The UDP port (default: port 1000) that all client-side Control Panels and Device Interfaces use to transport audio to the Virtual Matrix. The system has no restriction other than reserved ports. If the Virtual Matrix is behind a firewall and external access is required, a Port Forwarding entry must be added to route all traffic on this port to the internal Virtual Matrix IP address.

SIP Server IP Port: The IP Port (default: port 5060) for the integrated SIP Server. In general this value will never be changed as this is an industry standard port number. However, the value must be changed if multiple VCOM Virtual Matrix instances are to be run on the same physical computer.

SIP Server Base IP Port: By default, when set to zero all SIP RTP (Real-time [Audio] Protocol) sessions will establish the IP port number randomly in the range of 10000-42767. In many situations this is perfectly adequate. However, if the audio must transverse a firewall, it is not practical or safe to open such a large range of addresses.

As such, by specifying an RTP Audio Base port the system will assign IP ports sequentially upward from the base port. Once an IP Port is assigned to a SIP client, it will never change unless the Base Port is itself changed.

SIP Server Domain Name The optional SIP Domain for the integrated SIP Server. If the SIP Domain is specified, it can be used as the SIP Proxy Name and the Registrar Name when configuring SIP clients. Regardless of whether the SIP Domain is specified, the Virtual Matrix IP Address can always be used as the Proxy Name and the Registrar Name.

Secondary (Failover) Server Network Settings
If you wish to set up a failover server for a second Virtual Matrix, and have purchased 'Redundancy', enter the relevant values. In an instance of a hardware or connectivity failure client applications will reconnect to the failover server. Refer to Section 6 of the VCOM Virtual Matrix User Guide for a detailed description of the failover capability.

Server IP Address: The IP address of the server hosting the Virtual Matrix.

Server NAT IP Address: The public IP address that is used to route data to the Server's IP address within the LAN. This is only used when Network Address Translation (NAT) is being used on your LAN.

Server IP Port for VCOM Client Data / Audio: The Server IP Port for Client Audio under 'Server IP Port for VCOM Client Data / Audio'.

Server IP Port for Failover Data The port that is used for the two Virtual Matrix servers to communicate with each other.

Failover Settings (visible only if the server is licensed for this feature)
Failover Activation Delay: Set the amount of time to delay the failover from coming online in place of the Primary Server.

Automatic Failback: Define when to restore the Primary Server. Choose the setting that best fits your procedures.

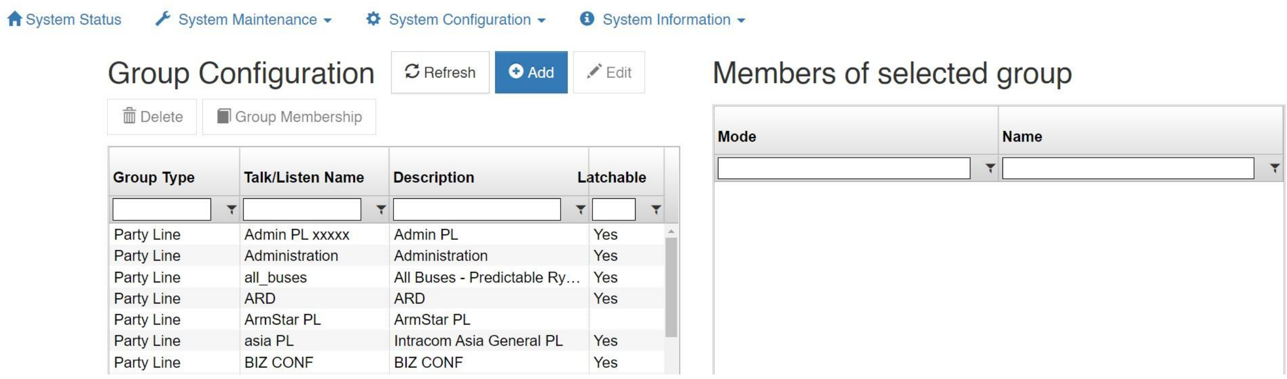
Media Server Settings (visible only if the server is licensed for this feature)
IP Port for Video Application Server WSS: The port that VCOM will use to establish a secure websocket with the Video Application Server.

Hostname for Video Media Server: The hostname of the system running the Video Media Server.

IP Port for Video Media Server WS: The port that VCOM will use to establish an unsecure websocket with the Media Server.

IP Port for Video Media Server WSS: The port that VCOM will use to establish a secure websocket with the Media Server.

6.4.2 Group Configuration



Group Type	Talk/Listen Name	Description	Latchable
Party Line	Admin PL xxxxx	Admin PL	Yes
Party Line	Administration	Administration	Yes
Party Line	all_buses	All Buses - Predictable Ry…	Yes
Party Line	ARD	ARD	Yes
Party Line	ArmStar PL	ArmStar PL	
Party Line	asia PL	Intracom Asia General PL	Yes
Party Line	BIZ CONF	BIZ CONF	Yes

Mode	Name

The ‘Group Configuration’ tab found in the ‘System Configuration’ area is used to add/edit/delete Party Lines and Fixed Groups, change selector names, and change group membership.

The main ‘Group Configuration’ window displays configured Party Lines and Fixed Groups.

To edit a Party Line or Fixed Group, highlight the one desired and click ‘Edit’ to bring up the ‘Group Configuration Add/Edit’ window.

To delete a Party Line or Fixed Group, highlight the one desired and click ‘Delete.’

To add members to a Fixed Group, click ‘Selected Group’ in the lower portion of the ‘Group Configuration’ window. Highlight a non-group member from the list of users and devices in the column on the left and click ‘Insert’ to add as a group member. To remove a group member highlight the user or device from the column on the right and click ‘Remove.’ Click ‘Clear’ to clear all group members.

To add a Party Line or Fixed Group, click the ‘Add’ button.

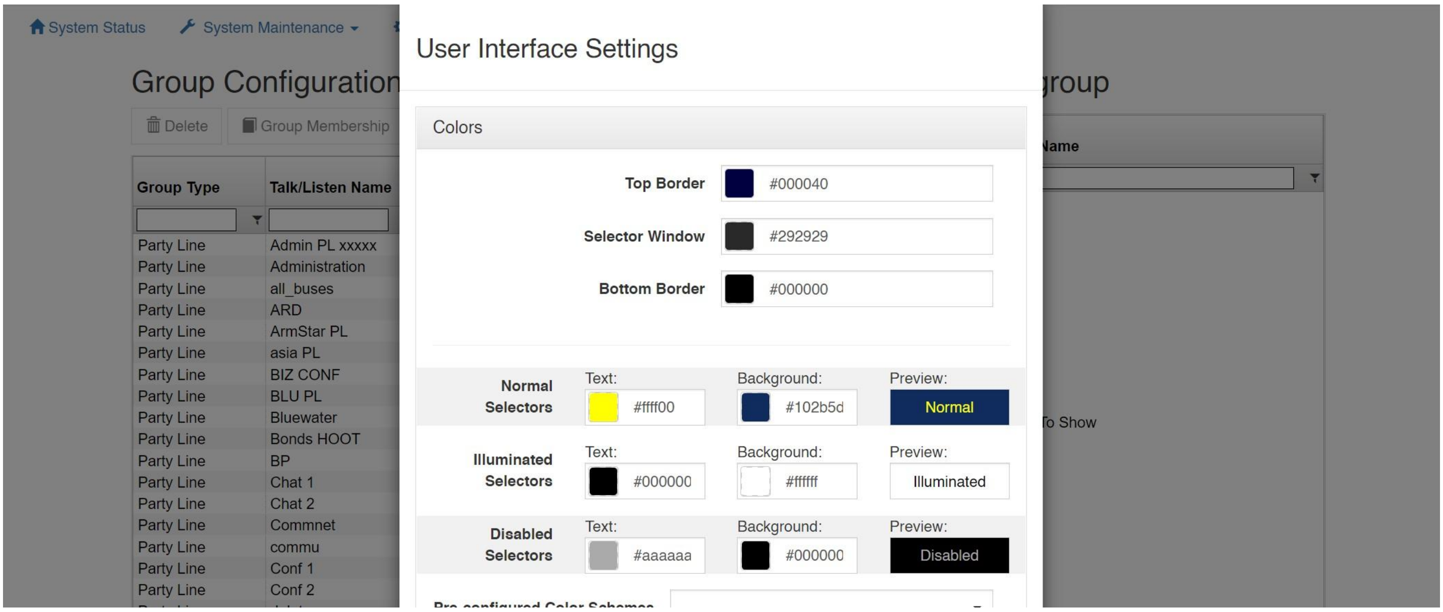
Type: Choose from the drop down box ‘Party Line’ or ‘Fixed Group’

Description: You may add a short description for the Party Line or Fixed Group or leave it blank.

Selector Talk Label: Add a name of up to 10 alphanumerical characters which will appear on the selector.

Latch Disable: Select latch disable to have the selector work as a momentary key.

6.4.3 User Interface Settings



Group Type	Talk/Listen Name
Party Line	Admin PL xxxxx
Party Line	Administration
Party Line	all_buses
Party Line	ARD
Party Line	ArmStar PL
Party Line	asia PL
Party Line	BIZ CONF
Party Line	BLU PL
Party Line	Bluewater
Party Line	Bonds HOOT
Party Line	BP
Party Line	Chat 1
Party Line	Chat 2
Party Line	Commnet
Party Line	commu
Party Line	Conf 1
Party Line	Conf 2

User Interface Settings

Colors

Top Border: #000040

Selector Window: #292929

Bottom Border: #000000

	Text:	Background:	Preview:
Normal Selectors	#ffff00	#102b5d	Normal
Illuminated Selectors	#000000	#ffffff	Illuminated
Disabled Selectors	#aaaaaa	#000000	Disabled

Pre-configured Color Schemes

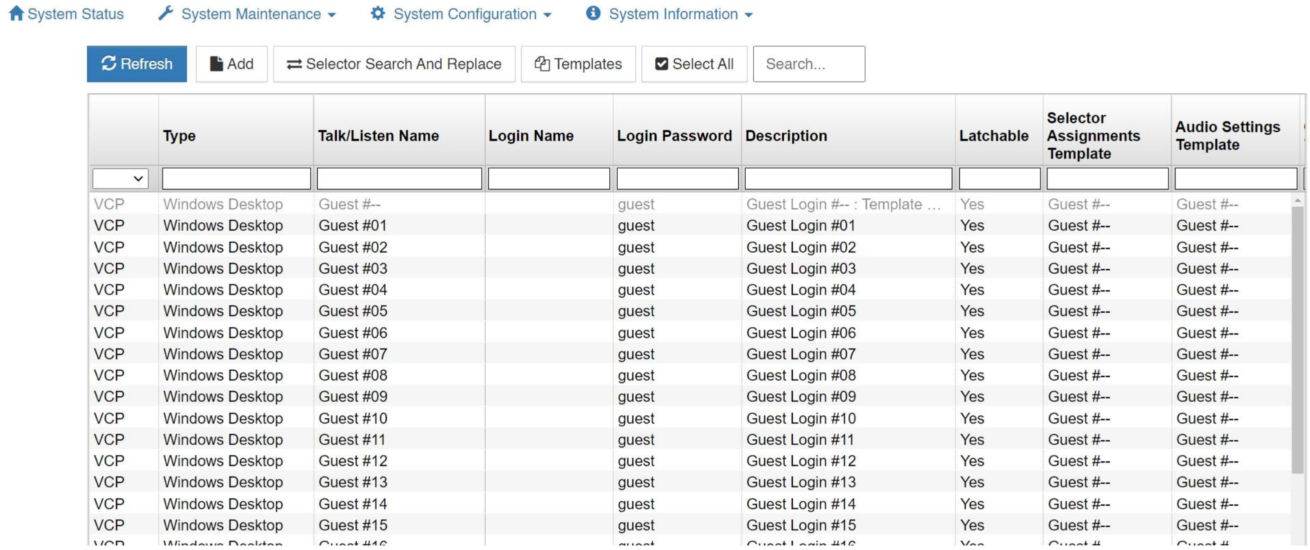
This allows customizations of the VCP GUI such as the Colors (Background and Text), Selector Spacing, and 24-bit PNG graphic files that can be uploaded such as a logo.

6.4.4 Control Rooms

Introduction

The Control Rooms feature provides the ability to configure individual SIP tally pages. More information is available in the Control Rooms documentation.

6.5 Client Configuration



	Type	Talk/Listen Name	Login Name	Login Password	Description	Latchable	Selector Assignments Template	Audio Settings Template
VCP	Windows Desktop	Guest #--		guest	Guest Login #-- : Template ...	Yes	Guest #--	Guest #--
VCP	Windows Desktop	Guest #01		guest	Guest Login #01	Yes	Guest #--	Guest #--
VCP	Windows Desktop	Guest #02		guest	Guest Login #02	Yes	Guest #--	Guest #--
VCP	Windows Desktop	Guest #03		guest	Guest Login #03	Yes	Guest #--	Guest #--
VCP	Windows Desktop	Guest #04		guest	Guest Login #04	Yes	Guest #--	Guest #--
VCP	Windows Desktop	Guest #05		guest	Guest Login #05	Yes	Guest #--	Guest #--
VCP	Windows Desktop	Guest #06		guest	Guest Login #06	Yes	Guest #--	Guest #--
VCP	Windows Desktop	Guest #07		guest	Guest Login #07	Yes	Guest #--	Guest #--
VCP	Windows Desktop	Guest #08		guest	Guest Login #08	Yes	Guest #--	Guest #--
VCP	Windows Desktop	Guest #09		guest	Guest Login #09	Yes	Guest #--	Guest #--
VCP	Windows Desktop	Guest #10		guest	Guest Login #10	Yes	Guest #--	Guest #--
VCP	Windows Desktop	Guest #11		guest	Guest Login #11	Yes	Guest #--	Guest #--
VCP	Windows Desktop	Guest #12		guest	Guest Login #12	Yes	Guest #--	Guest #--
VCP	Windows Desktop	Guest #13		guest	Guest Login #13	Yes	Guest #--	Guest #--
VCP	Windows Desktop	Guest #14		guest	Guest Login #14	Yes	Guest #--	Guest #--
VCP	Windows Desktop	Guest #15		guest	Guest Login #15	Yes	Guest #--	Guest #--
VCP	Windows Desktop	Guest #16		guest	Guest Login #16	Yes	Guest #-	Guest #-

The upper section of the Client Configuration window displays all configured users and devices, log in names, passwords, selector labels, client type, and if the given channel is set as a party line.

Click on a client description name and then Edit to change a parameter, Delete to delete a user or device, Add to create a new client, or Duplicate to copy a client’s settings to a new client.

Client Identification Client Type: Specifies the type of Client that allows the system to modify the internal operational behavior for proper operation of specific, such as VCOM Control Panels, Device Interfaces, Two-Way radios, and SIP devices.

Category	Client Type	Purpose
VCOM Control Panel	VCP: Windows Desktop	For logging into the VCOM (WebRTC) Control Panel on Windows
VCOM Control Panel	VCP: Apple iOS	For logging into the VCOM (WebRTC) Control Panel on iOS
VCOM Control Panel	VCP: Google Android	For logging into the VCOM (WebRTC) Control Panel on Android
VCOM Control Panel	VCP: Apple MAC	For logging into the VCOM (WebRTC) Control Panel on Mac
VCOM Control Panel	VCP: Linux	For logging into the VCOM (WebRTC) Control Panel on Linux
VCOM Control Panel	VCP: TCP-301	Used for the legacy VCOM TCP-301 Hardware Control Panel
VCOM Control Panel	VCP: TCP-401	Used for the legacy VCOM TCP-401 Hardware Control Panel
VCOM Control Panel	VCP: TCP-402	Used for the legacy VCOM TCP-402 Hardware Control Panel
VCOM Control Panel	VCP: TCP-603	Used for the legacy VCOM TCP-603 Hardware Control Panel
VCOM Control Panel	VCP: TCP-701	Used for the legacy VCOM TCP-701 Hardware Control Panel
VCOM Device Interface	VDI: Four-Wire Interface	For logging into the VCOM Device Interface
VCOM Device Interface	VDI: 2-Way Radio Interface	For logging into a VCOM Device Interface that is connect to a 2-Way Radio Interface
SIP	SIP: Telephone Adapter	Analog Telephony Adapter (FXS): also referred to as an “ATA” enables an analog telephone to function as an IP phone, sitting between your network and analog telephone.
SIP	SIP: Telephone Interface	VoIP gateway enables analog phone lines or T-1s with phone service into VCOM
SIP	SIP: Softphone	Enables connection to one of the many available softphones designed for Windows, Mac, etc
SIP	SIP: Hardphone	Enables a connection to a physical IP phone to VCOM
SIP	SIP: Direct IP Trunk	Enables a connection between PBX/SIP Servers and VCOM using IP settings
SIP	SIP: Registered Trunk	Enables a connection between PBX/SIP Servers and VCOM using Registration of clients
SIP	SIP: Four-Wire Interface	Enables connection of a SIP based Four Wire Interface to transport audio into VCOM
VIDEO	VIDEO: HTTP(S) Video Stream	Creates a new video selector. The specified video will be played upon clicking the selector on the WebRTC Control Panel.
RTSP	RTSP Audio Tx/Rx Interface	For transmitting and receiving audio via RTSP feed

Category	Client Type	Purpose
NDI	NDI: Newtek Network Device	For transmitting and receiving audio via NDI feed

Client Description: The description given to identify the client that is used exclusively in the System Administration application. This allows a complete description of a user (typically first and last name) that cannot otherwise be assigned to the selectors due to space restrictions.

Login Name: The name assigned to a user or device and used to login a Control Panel or Device Interface to the Virtual Matrix. Select ‘Allow Anonymous Login’ to allow a user to login a Control Panel by entering any login name he or she chooses followed by the designated password. The chosen login name will appear on the selector.

Login Password: The password assigned to a user or device and used to login a Control Panel or Device Interface to the Virtual Matrix

Selector Talk/Listen Name: The alphanumeric identifier that appears on Control Panel ‘Talk only’ and ‘Talk/Listen’ selectors.

Selector Listen Only Name: The alphanumeric identifier that appears on Control Panel ‘Listen only’ selectors. This is generally only assigned when a client has split functionality for the audio input and output as with a Program Feed input and IFB output.

Use Domain Authentication (LDAP): This is used when a Client is outside the LAN, and your LAN uses authentication to provide secure connections to remote users. If this option is enabled VCOM queries the OS to retrieve the already authenticated Windows user name. It then uses that name along with an encrypted password unique to that client to log in to the VVM. The VCOM Login Password becomes obsolete because the VCOM Control Panel will only permit login if that Windows User Name has been successfully authenticated. The Use Domain Authentication option must also be checked on the Control Panel. VCOM does not communicate with the Domain Controller.

Options Disable Client Login/Connection: This allows the System Administrator to “turn-off” certain clients when they are not needed to login to the system. Always Show Selector when Off-line: Specifies that the selector for this Client will be visible even if off-line on a VCOM Control Panel that is configured to hide the off-line selectors. It is generally used for VCOM Device Interface clients that should, under normal operation, never go off-line thus allowing VCOM Control Panel operators to more easily notice an unanticipated disconnect event.

Latch Disable Talk Selector: Select to operate associated selector as a momentary, meaning that an audio path will only persist as long as the selector is clicked and held. Party Line Operation: This specifies that a given client operates like a Party Line. This means that anyone talking to that client will also talk to anyone listening to that client and anyone listening to that client will also hear everyone talking to that client.

IFB Destination: Designates a client as an IFB Destination that causes the system to interrupt any assigned listen or program feeds to the destination when a Control Panel initiates a talk path to the destination. This setting is typically used with on-air talent who need to be constantly monitoring the on-air program feed but periodically take cues from the director or producer.

ISO Destination: Designates a client as an ISO Destination that causes the system to interrupt any assigned listen or program feeds to the destination when a Control Panel initiates a talk path to the destination and automatically activates a return talk path from the destination back to the Control Panel. Additionally, the talk paths in both directions are isolated so that the conversation is kept private. This setting is typically used with cameras when the director or producer needs to isolate a particular camera from the camera PL to provide private instruction.

Allow Assignment to Multiple Party Lines: Allows a client to be remotely assigned to Party Lines through Party Line Assignment Mode.

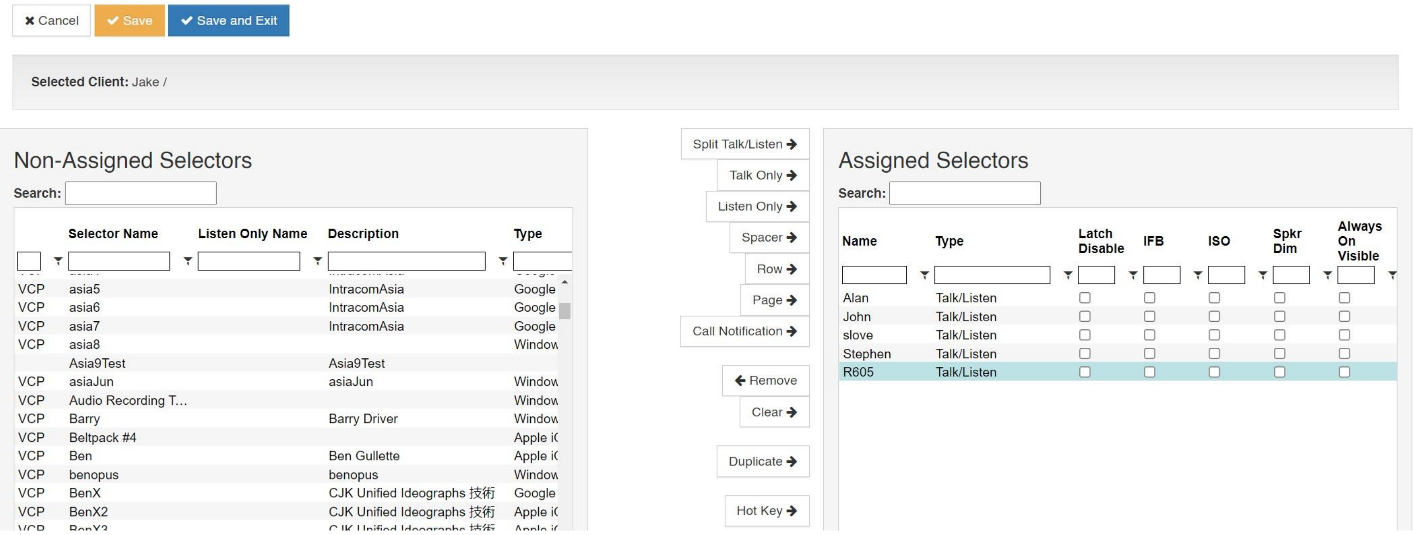
Standard System Administration Privileges: Gives System Administrator privileges to the client.

Master System Administration Privileges: Gives Master System administrator privileges to the client.

Selector Assignment Restrictions No local Assignment By Administrator: This prohibits local assignments to be made by an Administrator. Assignments can only be done through the System Administration application

No Local Assignment By User: This prohibits local assignments to be made by a User. Assignments can only be made by an administrator from the System Administration application

6.5.1 Selector Assignments



Selected Client: Jake /

Non-Assigned Selectors

Search:

	Selector Name	Listen Only Name	Description	Type
VCP	asia5		IntracomAsia	Google
VCP	asia6		IntracomAsia	Google
VCP	asia7		IntracomAsia	Google
VCP	asia8			Window
	Asia9Test		Asia9Test	
VCP	asiaJun		asiaJun	Window
VCP	Audio Recording T…			Window
VCP	Barry		Barry Driver	Window
VCP	Beltpack #4			Apple i
VCP	Ben		Ben Gullette	Apple i
VCP	benopus		benopus	Window
VCP	BenX		CJK Unified Ideographs 技術	Google
VCP	BenX2		CJK Unified Ideographs 技術	Apple i
VCP	BenX3		CJK Unified Ideographs 技術	Apple i

Assigned Selectors

Search:

Name	Type	Latch Disable	IFB	ISO	Spkr Dim	Always On Visible
Alan	Talk/Listen	□	□	□	□	□
John	Talk/Listen	□	□	□	□	□
slove	Talk/Listen	□	□	□	□	□
Stephen	Talk/Listen	□	□	□	□	□
R605	Talk/Listen	□	□	□	□	□

This page allows assignment of a Control Panel’s selectors. Highlight a selector in the left-hand portion of the screen and select one of the configuration options listed below.

Split Talk/Listen: Add the desired selector with both talk and listen paths.

Talk Only: Add the desired selector with only a talk path.

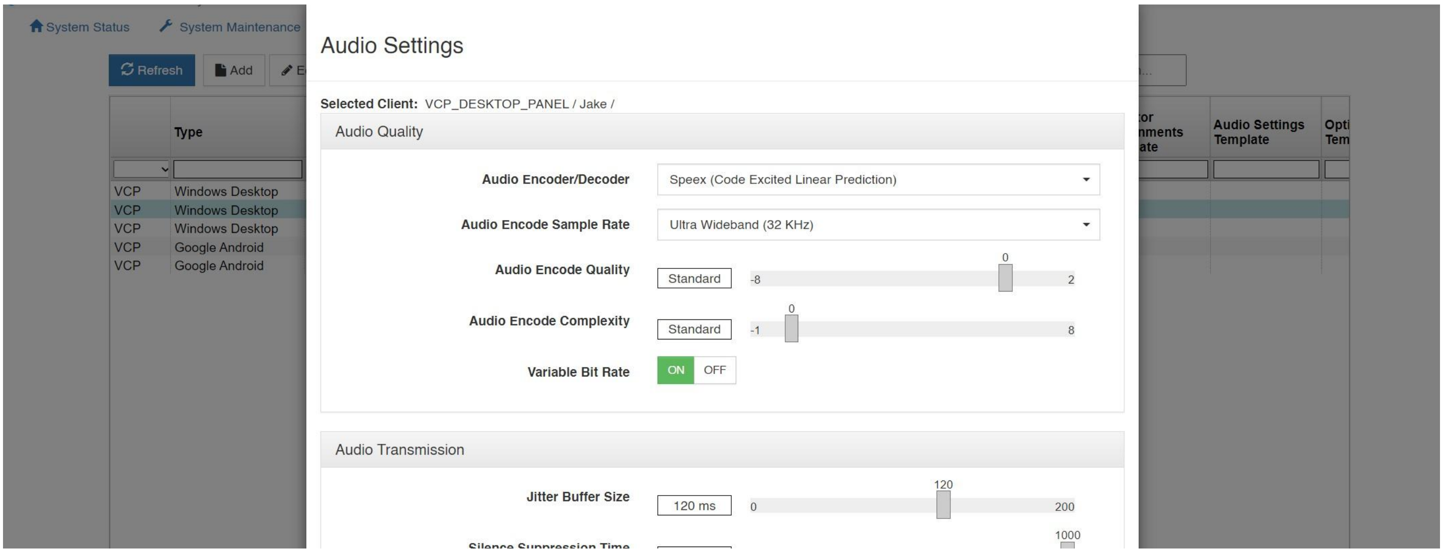
Listen Only: Add the desired selector with a Listen only path.

Remove: Highlight a selector in the right-hand portion of the screen and select ‘Remove’ to delete an assigned selector.

Clear: Delete all assigned selectors.

Hot Key: Assigns a keyboard key to the selected Selector so that the key can be used to activate and deactivate the Selector on a VCOM Control Panel. This option is only supported on the VCOM Control Panel for Windows.

6.5.2 Audio Settings



Audio Settings

Selected Client: VCP_DESKTOP_PANEL / Jake /

Audio Quality

Audio Encoder/Decoder: Speex (Code Excited Linear Prediction)

Audio Encode Sample Rate: Ultra Wideband (32 KHz)

Audio Encode Quality: Standard -8 0 2

Audio Encode Complexity: Standard -1 0 8

Variable Bit Rate: ON OFF

Audio Transmission

Jitter Buffer Size: 120 ms 0 120 200

Silence Suppression Time 1000

Audio Quality Audio Encoder/Decoder: This setting allows selection of a different encoder/decoder. For VCOM Control Panels and VCOM Device Interface clients the choice is between a High Compression / Low Bitrate Codec used for Internet connectivity and a Low Compression / High Bitrate codec that may be used for Local Network connectivity to slightly reduce latency. For SIP Devices the codec specified is preferential codec used when negotiating which codec to use with the SIP Device.

Audio Encode Sample Rate: This setting controls the sampling rate supported by the Clients and thereby dictates default fidelity for the Client connections. This setting is typically the same as the System Audio Sampling rate however it can be specified at lower rate but never at a higher rate (refer to System Audio Sampling Rate for additional detail). Higher audio sampling rates have more significant requirements in computational speed and network bandwidth. Careful consideration must be given when choosing this setting with respect to client hardware and the client network connection.

Audio Encode Quality: The VCOM System codec achieves compression at the expense of fidelity of the input speech signal. Unlike some other speech codecs, it is possible to control the tradeoff made between quality and bit-rate. Audio Encode Complexity: With the VCOM System codec, it is possible to vary the complexity allowed for the encoder. This is done by controlling how the search is performed with an integer ranging from 1 to 10. For normal use, the noise level at complexity 1 is between 1 and 2 dB higher than at complexity 10, but the CPU requirements for complexity 10 is about 5 times higher than for complexity 1. In practice, the best trade-off is between complexity 2 and 4, though higher settings are often useful when encoding non-speech sounds.

Audio Transmission

Variable Bit Rate: Allows the system's codec to dynamically change the bit rate at which audio is being encoded. As sounds like vowels require a higher bit rate to achieve good quality as compared to "s" and "f" sounds, this setting efficiently achieves the best sound quality within the given confines. The system can be set for variable rate or fixed rate. While this setting improves the quality of speech, it conversely degrades the quality of music and should therefore be disabled when using a program feed. Jitter Buffer Size: This setting specifies the depth of the jitter buffer in milliseconds. In network-based communications, the delivery time of audio packets across the network may not be uniform. This characteristic is known as jitter. As such, audio received from a network connection must be buffered to compensate for this so that a continuous, time-relative stream of audio can be delivered to the consumer of the audio. Different network topologies will have different jitter characteristics. For example, a public Internet connection will have significantly more jitter than an internal local network. The effect of a jitter buffer that is too small will result in audio gaps. The value is specified in milliseconds.

Silence Suppression Time: Ceases all transmission of audio data when no voice activity is detected from a Control Panel or Device Interface after the specified time lapse. This virtually eliminates background noise during multiparty conferences. However, it may initially be disconcerting to some individuals as the 'comfort noise' typically associated with analog systems is suppressed. Additionally, this feature minimizes the overall required network bandwidth. The value is specified in milliseconds in the range of 100- 1000 ms or can be turned off entirely.

Packet Re-sequencer Depth: This setting specifies the number of packets that are stored when waiting for an out of sequence audio packet. In some network topologies, even if UDP packets are sent in sequential order, they are received non-sequentially. These packets must be re-sequenced before use. After the maximum re-sequencer depth has been reached, the packet being awaited is declared to be lost and the re-sequencing is re-started at the next earliest received packet. Valid settings are from 2 to 10 packets.

Audio Processing

Automatic Gain Control (AGC): This setting enables or disables AGC on the audio path from Client to the Server. AGC automatically increases or decreases the audio level such that the client presents a uniform audio level to the Virtual Matrix. AGC is primarily appropriate for use with a Control Panel when used with a headset microphone. In some situations where there is a high amount of background noise or some return audio leakage the AGC may incorrectly amplify the noise to normal audio levels.

Automatic Gain Control (AGC) Level: This setting increases or decreases the sensitivity of the AGC. Increasing or decreasing the sensitivity of the ACG changes the behavior of the AGC such that it adapts faster or slower, respectively, to audio levels not considered to be at uniform level. Decreasing the sensitivity may be useful in cases where there is a high amount of background noise or some return audio leakage.

Audio Input Level Gain (Pre-Mix): This setting controls the audio input level sent from the Client to the Virtual Matrix. This setting is typically used only when the client’s audio input device does not provide a sufficiently audible level (as heard by all other clients) and does not have a local gain control to compensate. The value can be adjusted a maximum of +/-18dB in 6dB steps.

Audio Output Level Gain (Post-Mix): This setting controls the audio output level sent to the Client from the Virtual Matrix. This setting is typically used only when the client’s audio output device does not provide a sufficiently audible level and does not have a local gain control to compensate. The value can be adjusted a maximum of +/-18dB in 6dB steps.

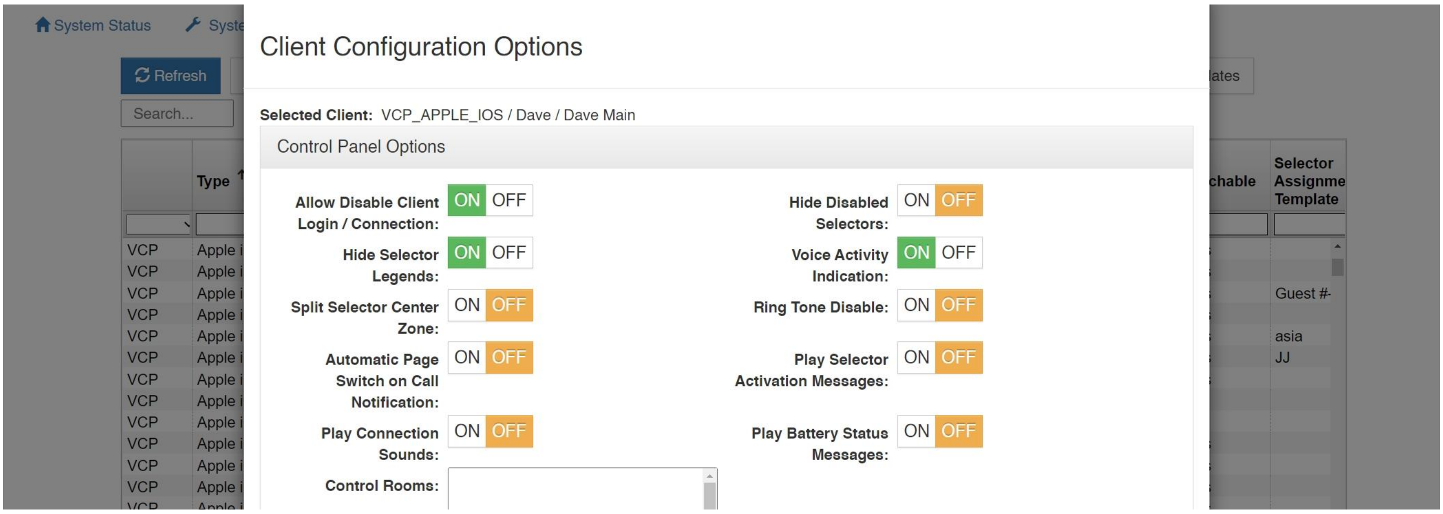
Speakerphone Speaker Dim Reduction: This setting dims the incoming audio output by a configured amount when you activate the talk key.

Echo Cancellation: This setting enables or disables the client’s Echo Cancellation. Echo Cancellation is useful if there is any return audio leakage from the client’s speaker back to his microphone. This may result in an audible echo heard by any other client that is talking and listening to the client with the return audio leakage.

Echo Cancellation Tail Length: This setting controls the duration the echo canceller waits to receive the echo before it begins the cancellation process. The recommended tail length is approximately a third of the room reverberation time. For example, in a small room, reverberation time is in the order of 300ms, so a tail length of 100ms is recommended.

Audio Encryption: This setting is a licensable option for security measures. Clients may choose from following options: No Encryption, AES 128, or AES 256.

6.5.3 VCOM Client Configuration Options



Client Configuration Options

Selected Client: VCP_APPLE_IOS / Dave / Dave Main

Control Panel Options

Allow Disable Client Login / Connection: [✓ ON] OFF

Hide Disabled Selectors: ON [✓ OFF]

Hide Selector Legends: [✓ ON] OFF

Voice Activity Indication: [✓ ON] OFF

Split Selector Center Zone: ON [✓ OFF]

Ring Tone Disable: ON [✓ OFF]

Automatic Page Switch on Call Notification: ON [✓ OFF]

Play Selector Activation Messages: ON [✓ OFF]

Play Connection Sounds: ON [✓ OFF]

Play Battery Status Messages: ON [✓ OFF]

Control Rooms:

Control Panel Options

Allow Disable Client Login/Connection: This setting allows the client’s login capability to be disabled.

Hide Disabled Selectors: This setting hides selectors assigned to other clients that are not logged into the system. When the clients come online, their selector will dynamically appear.

Hide Selector Legends: This setting hides the overlaid selector legends displayed on listen selectors (‘L’) and talk selectors (‘T’).

Voice Activity Indication: This setting is used to visually indicate voice activity on Control Panel selectors, represented by selector text and background color switching between base state (yellow text / navy background) and default activity indication colors (white text / light navy background) or selected activity indication colors (variable). Voice Activity Indication is only available if the Control Panel has the ability to listen to or is being talked to by the client indicating voice activity. Split Selector Center Zone: This setting allows the center of the selector to be used to activate both the talk and listen selectors for split talk/listen selectors.

Ring Tone Disable: Disables Ring Tone loaded in SIP Client Options for the selected user.

Automatic Page Switch on Call Notification: This setting will cause the pages (when multiple pages are used) to switch to the page with the current incoming call from another user.

Play Selector Activation Messages: This setting will cause the unit to announce “Talk on/ Talk Off” or “Listen On/Off” when activating the selectors.

Play Connection Sounds: This setting will cause the unit to play a sound every time you connect or disconnect to the network.

Play Battery Status Messages: This setting will announce the status of the battery depending on the percentage of battery left – (5, 10, 15, 20, 25, 30)

Control Panel Function Buttons

Enable Party Line Assignment Button: This will enable the PL Assignment button on the Control Panel allowing the user the capability of assigning other “devices” to PLs.

Enable Selector Volume Buttons: This enables the “Selector Volume” button that gives the user a quick key to adjust individual selector volumes.

Enable Dial Pad Button: This enables a button that enables the Dial Pad when a SIP device is being accessed to dial out.

Enable Selector Assignment Button: This enables a button that gives the user the capability of assigning selectors through the VCP GUI via a pop-up window.

Enable Selector Relocation Button: This enables a button that allows the user to rearrange the order of their selectors to customize to their particular needs.

Enable Reveal Inactive Selectors Button: This allows the user to disable/enable inactive (not logged in) selectors.

Enable Launch Geo Mapping Button: This enables a button that will launch a web page directed to the Geo Mapping Server to display the Geo Mapping web application.

Control Panel for iOS Options

Restart in Background if Previously Active: This will restart the VCP in the background when the device is restarted.

Operate as a Beltpack: This will use the “Beltpack Template” that allows for oversized buttons on an iOS device such as the iPhone/iPod Touch which can also be used with Screen covers with cutouts for these oversized buttons.

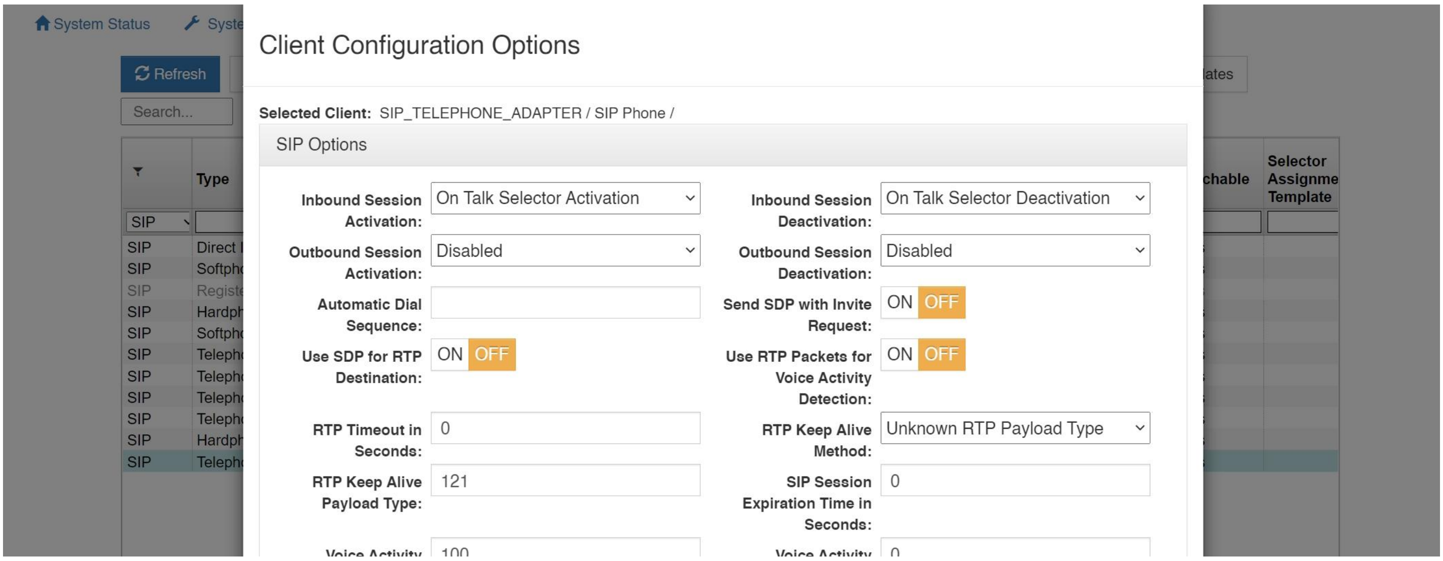
Disable Integrated Mic and Speaker: This will disable the use of an internal mic and speaker on the iOS device.

Control Panel/Device Interface Options Voice Activity Detection Time in Ms: This allows the amount of time to be set for Voice Activity Detection to turn on for the selected user.

Geo Mapping
Geo Mapping Disable: This will disable the selected user’s access and data sent to the Geo Mapping server.

Geo Mapping Latitude/Longitude: This allows the GPS coordinates of the selected user to be set when used as a fixed position. This is not used for mobile devices.

6.5.4 SIP Client Configuration Options



Client Configuration Options

Selected Client: SIP_TELEPHONE_ADAPTER / SIP Phone /

SIP Options

Inbound Session Activation:	On Talk Selector Activation	**Inbound Session Deactivation:**	On Talk Selector Deactivation
Outbound Session Activation:	Disabled	**Outbound Session Deactivation:**	Disabled
Automatic Dial Sequence:		**Send SDP with Invite Request:**	ON OFF
Use SDP for RTP Destination:	ON OFF	**Use RTP Packets for Voice Activity Detection:**	ON OFF
RTP Timeout in Seconds:	0	**RTP Keep Alive Method:**	Unknown RTP Payload Type
RTP Keep Alive Payload Type:	121	**SIP Session Expiration Time in Seconds:**	0
Voice Activity	100	**Voice Activity**	0

Inbound Session Activation: This setting specifies how the Virtual Matrix handles the activation of a call initiated by the SIP client. If configured for ‘Disabled,’ the call initiated by the SIP client is ignored. If configured for ‘On Call Received (Auto Answer),’ the call initiated by the SIP client will be automatically answered by the VCOM Virtual Matrix. If configured for ‘On Talk Selector Activation,’ the call initiated by the SIP Client will be indicated on the associated Control Panel selectors and the call will be answer only if a VCOM Control Panel activates the talk selector associated with the SIP Client.

Inbound Session Deactivation: This setting specifies how the Virtual Matrix handles the deactivation of a call initiated by the SIP client. If configured for ‘Disabled,’ the call initiated by the SIP client can never be disconnected by the Virtual Matrix. If configured for ‘On Forced Disconnect,’ the call initiated by the SIP client can only be disconnected by a VCOM Control Panel using the ‘Disable Client Login’ feature. If configured for ‘On Talk Selector Deactivation,’ the call initiated by the SIP Client will be disconnected when all VCOM Control Panels deactivate the talk selectors associated with the SIP Client.

Outbound Session Activation: This setting specifies how the Virtual Matrix handles the activation of a call initiated to the SIP client. If configured for ‘Disabled,’ the Virtual Matrix cannot initiate any call to the SIP client. If configured for ‘On Registration,’ the Virtual Matrix will initiate a call to the SIP client as soon as the SIP client makes its presence known through a process known as ‘Registration.’ If configured for ‘On Talk Selector Activation,’ the Virtual Matrix will initiate a call to the SIP client when any VCOM Control Panel activates the talk selector associated with the SIP Client.

Outbound Session Deactivation: This setting specifies how the Virtual Matrix handles the deactivation of a call initiated to the SIP client. If configured for ‘Disabled,’ the call initiated to the SIP client can never be disconnected by the Virtual Matrix. If configured for ‘On Forced Disconnect,’ the call initiated to the SIP client can only be disconnected by a VCOM Control Panel using the ‘Disable Client Login’ feature. If configured for ‘On Talk Selector Deactivation,’ the call initiated to the SIP Client will be disconnected when all VCOM Control Panels deactivate the talk selectors associated with the SIP Client.

Automatic Dial Sequence: This setting specifies a dial sequence to be dialed as soon a call is established with a SIP Client. To insert a delay in the dial sequence, use ‘P’ to insert a 5 second delay and ‘p’ to insert a 1 second delay.

Send SDP With Invite Request: This setting changes the default behavior of calls initiated by the Virtual Matrix to allow compatibility with devices that do not conform to proper SIP implementation, specifically the Raytheon ARA-1. Normally when the Virtual Matrix initiates a call to the SIP client, it does so without sending a Session Description Protocol (SDP), so that it can subsequently control the codec selection.

Use SDP for RTP Destination: This setting changes the default behavior of the Virtual Matrix to allow strict conformance with the Real-Time Protocol specification. Normally the Virtual Matrix ignores the RTP IP address specified in the SDP and uses the actually received RTP IP address as the SIP specification as written and does not account for SIP clients behind NAT firewalls that typically alter the IP address of the packet.

Use RTP Packets for Voice Activity Detection: Many SIP device employ Silence Suppression to eliminate unnecessary network traffic. When a device supports silence suppression, this option can be enabled such that Voice Activity will be indicated whenever RTP audio packets are received. If this option is not enabled, The Virtual Matrix will indicate Voice Activity by analyzing the content of the audio stream.

RTP Timeout In Seconds: During an active SIP call, there should be a constant and ongoing flow of RTP audio packets or RTP Keep Alive packets between the client and the server in additional to the SIP control packets. In some cases the RTP audio packets might be blocked even though the SIP control packets are not. This option specifies the time in seconds to wait for RTP audio packets before assuming there must be a problem with the connection and disconnecting the call. Setting this value to zero disables the check for an RTP Timeout.

RTP Keep Alive Method: When a SIP device supports silence suppression, it is often necessary to send RTP keep alive packets when audio is not being sent in order to ensure that no firewalls or routers in between close the associated ports due to inactivity. This option specifies the type of RTP Keep Alive Method as not all SIP devices can accept the RTP Keep Alive Methods specified by RFC 6223.

SIP Session Expiration Time In Seconds: During an active SIP call there is often a constant and ongoing flow of SIP control packets between the client and the server. In some cases the SIP control packets might stop due to a loss of network connectivity. This option specifies the time in seconds to wait for the SIP control packets before assuming there must be a problem with the connection and disconnecting the call. Setting this value to zero disables the check for a SIP Session Expiration.

Voice Activity Detection Validation Time in Ms: This allows the amount of time to be set for Validation Time to register as a Voice Activity event. For example, there needs to be 100ms of audio for Voice Activity Detection to turn on to pass audio in the picture above.

Voice Activity Detection Off Delay Time in Ms: This allows the amount of time to be set for Voice Activity Detection to be turned off. This is the amount of silence allowed after a user is speaking.

Call Notification Ring Tone: A file path can load an audio file to be played when an incoming call is placed.

Auto-Answer Notification Message: This option allows the selection of an audio wave file to be played as the notification message to the caller to indicate that the connection has been established between the SIP client and the VCOM Virtual Matrix. User provided files can be uploaded to the server provided the files are in a 16 bit mono audio format, preferably set to the same Audio Mix Sample Rate of the Virtual Matrix.

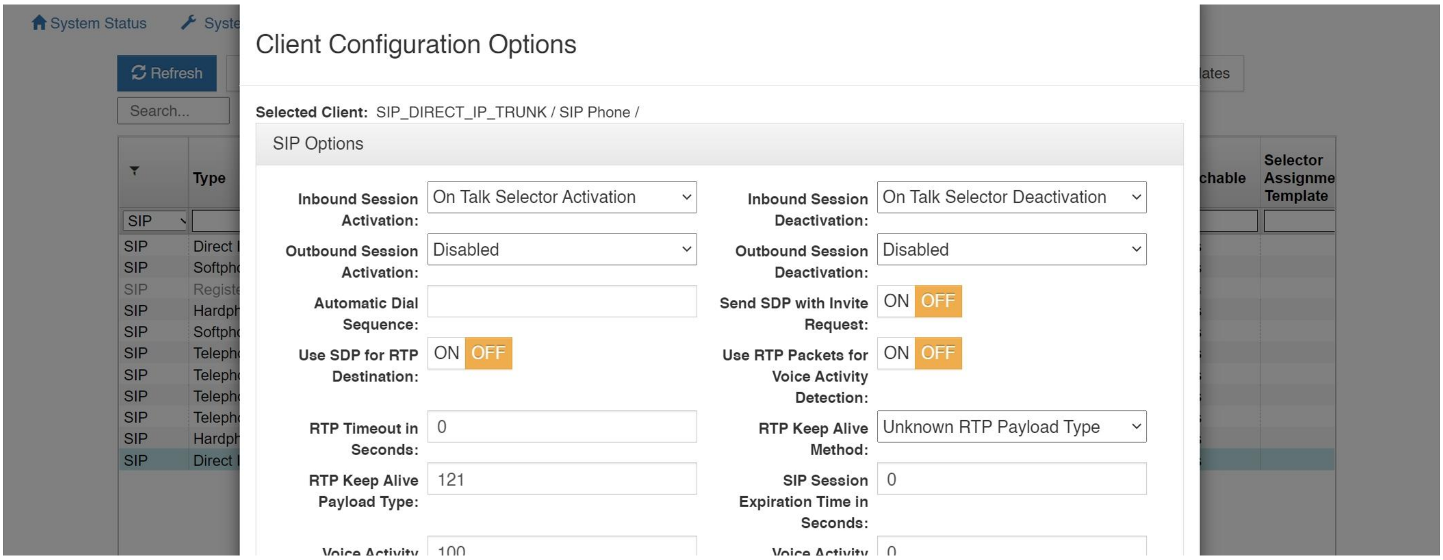
Auto-Answer Delay Time In Ms: This option sets the delay time in milliseconds after which the VCOM Virtual Matrix will automatically answer a received SIP call. Typically this value will be set to zero such that the call is answered immediately. In some situations it is desirable to delay answering the call so that VCOM Control Panels listening to that line will hear a ring signal.

Auto-Answer Access Code: This option enables the requirement that an Access Code must be entered by the caller if the VCOM Virtual Matrix automatically answers a received SIP call. The Access Code may consist of up to 10 digits. When configuring an access code, it is recommended to configure an appropriate Auto-Answer Notification Message which prompts the caller to enter the access code. The provided "AccessCode.wav" message is provided for this purpose.

Use 16kHz for G.722 Timestamp: Sets bandwidth to 16kHz when the G.722 CODEC is used.

Internal SIP Client User Name Prefix: Character placed before the Client’s User Name when dialing, most commonly used is the asterisk.

6.5.5 SIP Direct IP Trunk and Registered Trunk Options



Client Configuration Options

Selected Client: SIP_DIRECT_IP_TRUNK / SIP Phone /

SIP Options

Inbound Session Activation:	On Talk Selector Activation	Inbound Session Deactivation:	On Talk Selector Deactivation
Outbound Session Activation:	Disabled	Outbound Session Deactivation:	Disabled
Automatic Dial Sequence:		Send SDP with Invite Request:	ON OFF
Use SDP for RTP Destination:	ON OFF	Use RTP Packets for Voice Activity Detection:	ON OFF
RTP Timeout in Seconds:	0	RTP Keep Alive Method:	Unknown RTP Payload Type
RTP Keep Alive Payload Type:	121	SIP Session Expiration Time in Seconds:	0
Voice Activity	100	Voice Activity	0

In most situations, the VCOM Virtual Matrix itself acts as the SIP Registrar and SIP Server for SIP Clients to connect to it. However, when connecting to other SIP Registrars and SIP Servers, the VCOM Virtual Matrix can itself act as a SIP Client when a client is configured as a SIP Direct IP Trunk or a SIP Registered Trunk using the following options:

SIP Target User Name: This specifies the fixed user name to use as the Address of Record (AOR) when sending SIP registration and/or SIP invite requests. If using a VCOM Control Panel to dial out through a PBX, this field must be left blank, as the dialed phone number will be User Name.

SIP Target Primary Host Name: This specifies the target primary host name or IP address of the target SIP Registrar or SIP Server to use when sending SIP registration and SIP invite requests.

SIP Target Secondary Host Name: This specifies the target secondary host name or IP address of the target SIP Registrar or SIP Server to use when sending SIP registration and/or SIP invites. The secondary host name will only be used in the case where a secondary (failover) server is available and the primary server is not reachable. If no secondary (failover) server is available, this field must be left blank.

SIP Target Proxy Server IP Address (optional): This specifies the IP address of the SIP Proxy, if a SIP Proxy is used.

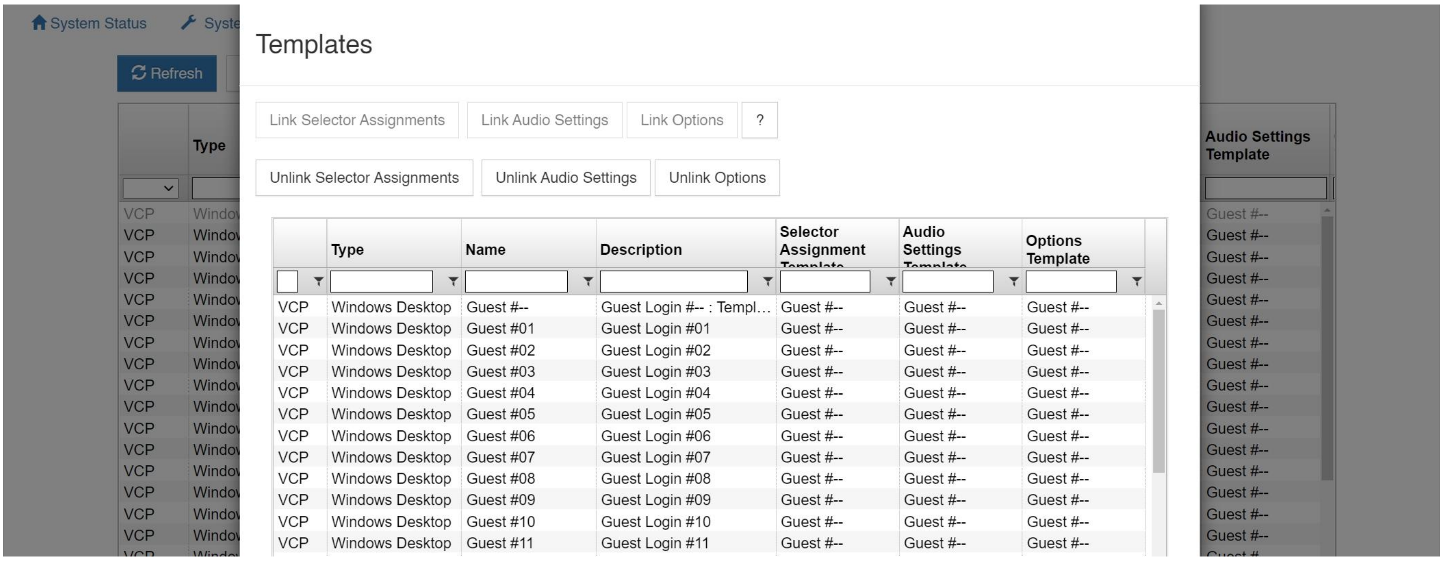
SIP Registration Expiration Time In Seconds: This option specifies the time in seconds that the Virtual Matrix is expected to refresh the registration with the target SIP Registrar. If the registration is not refreshed with the specified time frame, the SIP session will be terminated.

STUN Server or Proxy IP Address: This option enables SIP client transversal through a NAT by specifying the IP address of a STUN Server which will inform the Virtual Matrix of the public IP address of the SIP Client so that it can be included when sending SIP registration and SIP invite requests.

Geo Mapping
Geo Mapping Disable: Check this box to disable the use of geo mapping on any given SIP periphery

Geo Mapping Latitude (Fixed Position): Input the fixed latitude position for a geographically static SIP periphery.

6.5.6 Templates



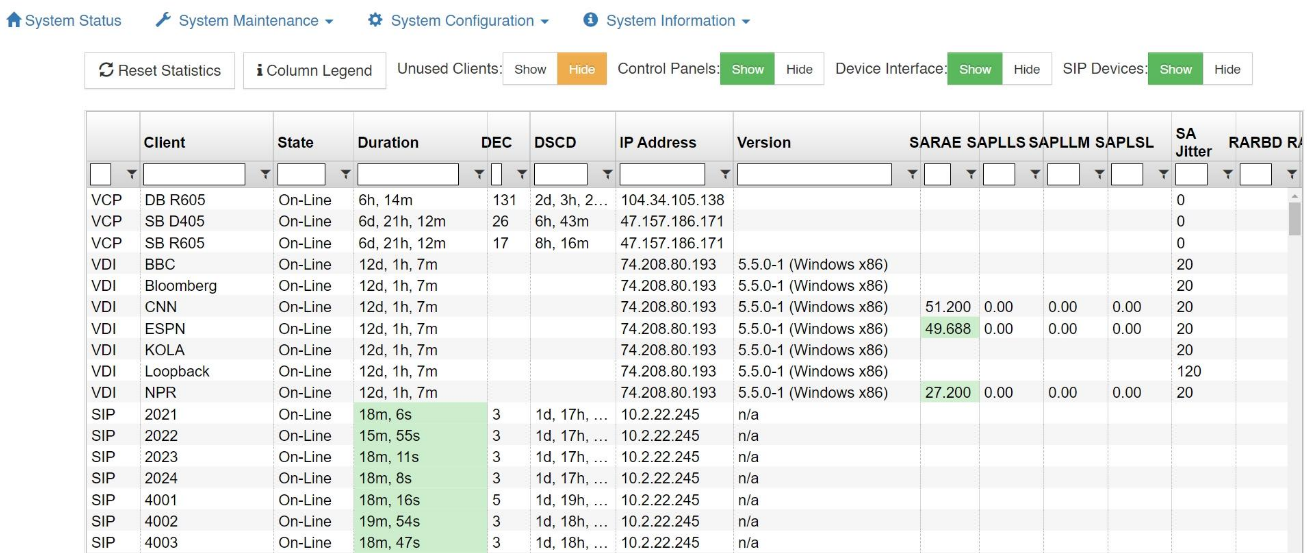
	Type	Name	Description	Selector Assignment	Audio Settings	Options Template
VCP	Windows Desktop	Guest #--	Guest Login #-- : Templ…	Guest #--	Guest #--	Guest #--
VCP	Windows Desktop	Guest #01	Guest Login #01	Guest #--	Guest #--	Guest #--
VCP	Windows Desktop	Guest #02	Guest Login #02	Guest #--	Guest #--	Guest #--
VCP	Windows Desktop	Guest #03	Guest Login #03	Guest #--	Guest #--	Guest #--
VCP	Windows Desktop	Guest #04	Guest Login #04	Guest #--	Guest #--	Guest #--
VCP	Windows Desktop	Guest #05	Guest Login #05	Guest #--	Guest #--	Guest #--
VCP	Windows Desktop	Guest #06	Guest Login #06	Guest #--	Guest #--	Guest #--
VCP	Windows Desktop	Guest #07	Guest Login #07	Guest #--	Guest #--	Guest #--
VCP	Windows Desktop	Guest #08	Guest Login #08	Guest #--	Guest #--	Guest #--
VCP	Windows Desktop	Guest #09	Guest Login #09	Guest #--	Guest #--	Guest #--
VCP	Windows Desktop	Guest #10	Guest Login #10	Guest #--	Guest #--	Guest #--
VCP	Windows Desktop	Guest #11	Guest Login #11	Guest #--	Guest #--	Guest #--

Templates allow you to apply a given client’s selector assignments, audio settings, and/or options to one or more other clients.

First select the client you want to use as the template and then using the CTRL key, select one or more other clients you want to apply your template’s settings to. You will see the Templates section become enabled. Click on the appropriate Link button to populate selector assignments, audio settings, and/or options from your template to your other selected clients. If you later want to remove applied client settings from your template, use the appropriate Unlink button.

6.6 System Information

6.6.1 Client Statistics



	Client	State	Duration	DEC	DSCD	IP Address	Version	SARAE	SAPLLS	SAPLLM	SAPLSL	SA Jitter	RARBD	RA
VCP	DB R605	On-Line	6h, 14m	131	2d, 3h, 2…	104.34.105.138						0		
VCP	SB D405	On-Line	6d, 21h, 12m	26	6h, 43m	47.157.186.171						0		
VCP	SB R605	On-Line	6d, 21h, 12m	17	8h, 16m	47.157.186.171						0		
VDI	BBC	On-Line	12d, 1h, 7m			74.208.80.193	5.5.0-1 (Windows x86)					20		
VDI	Bloomberg	On-Line	12d, 1h, 7m			74.208.80.193	5.5.0-1 (Windows x86)					20		
VDI	CNN	On-Line	12d, 1h, 7m			74.208.80.193	5.5.0-1 (Windows x86)	51.200	0.00	0.00	0.00	20		
VDI	ESPN	On-Line	12d, 1h, 7m			74.208.80.193	5.5.0-1 (Windows x86)	49.688	0.00	0.00	0.00	20		
VDI	KOLA	On-Line	12d, 1h, 7m			74.208.80.193	5.5.0-1 (Windows x86)					20		
VDI	Loopback	On-Line	12d, 1h, 7m			74.208.80.193	5.5.0-1 (Windows x86)					120		
VDI	NPR	On-Line	12d, 1h, 7m			74.208.80.193	5.5.0-1 (Windows x86)	27.200	0.00	0.00	0.00	20		
SIP	2021	On-Line	18m, 6s	3	1d, 17h, …	10.2.22.245	n/a							
SIP	2022	On-Line	15m, 55s	3	1d, 17h, …	10.2.22.245	n/a							
SIP	2023	On-Line	18m, 11s	3	1d, 17h, …	10.2.22.245	n/a							
SIP	2024	On-Line	18m, 8s	3	1d, 17h, …	10.2.22.245	n/a							
SIP	4001	On-Line	18m, 16s	5	1d, 19h, …	10.2.22.245	n/a							
SIP	4002	On-Line	19m, 54s	3	1d, 18h, …	10.2.22.245	n/a							
SIP	4003	On-Line	18m, 47s	3	1d, 18h, …	10.2.22.245	n/a							

Client Statistics: Displays individual send and receive audio and packet loss statistics for all client connections.

Click the ‘Reset Statistics’ button in the upper, left-hand corner to reset all client statistics or highlight a user or device and then click ‘Reset Statistics’ to reset the statistics of an individual user or device.

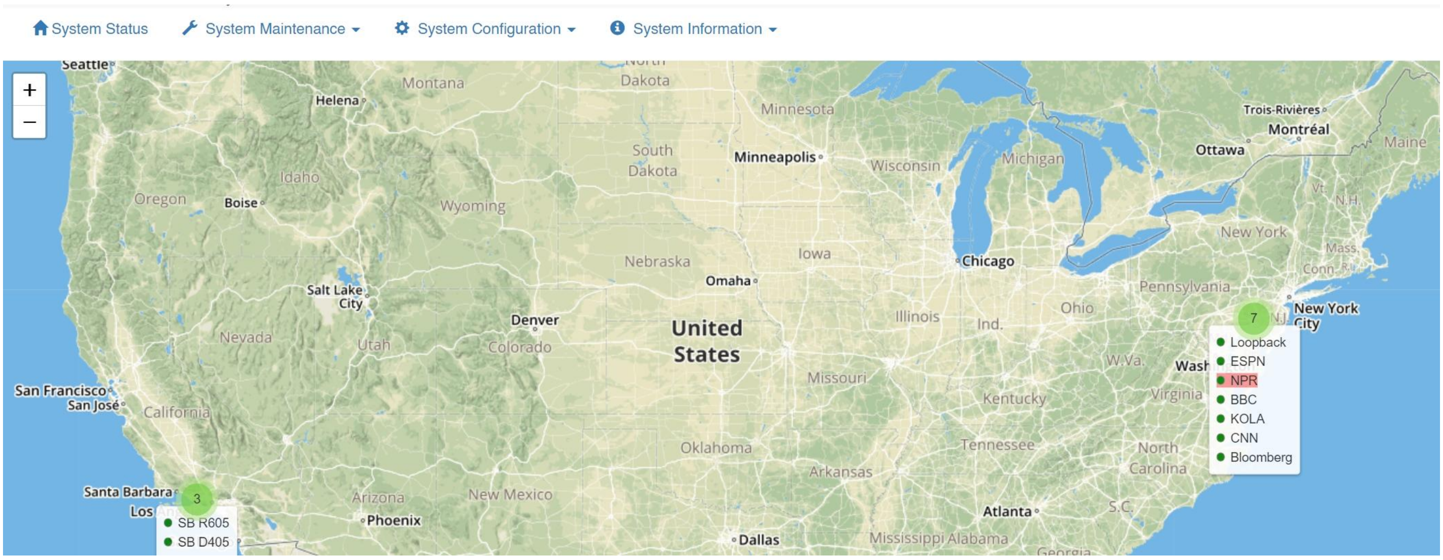
Select ‘Show Unused Clients’ to display users and devices programmed for your system but that are off-line.

Click the ‘Column Legend’ button in the upper, left-hand side of the ‘Client Statistics’ page to display the legend.

6.6.2 SIP Registrations

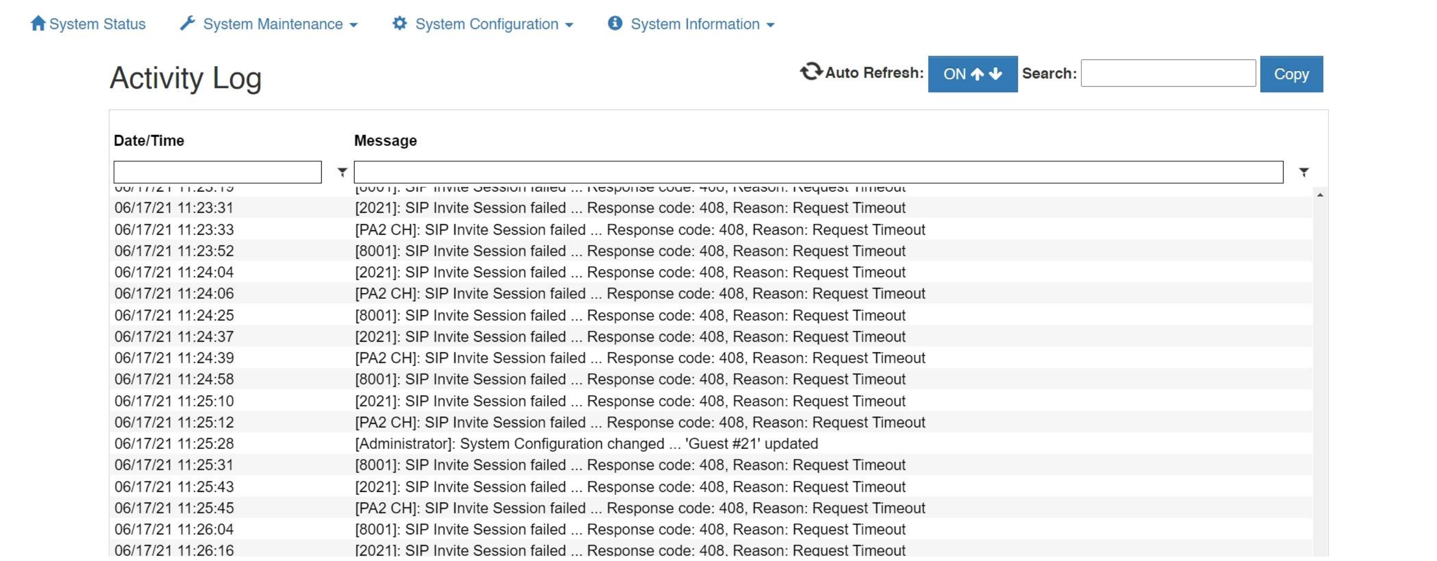
Displays all VCOM SIP registrations including user names, address of record, and contact detail.

6.6.3 Geolocation



Displays the approximate locations of clients on the system. For VCOM Control Panel clients on Android and iOS, this is based on GPS information if the required permission is granted for the app. Location is determined based on IP address for all other clients types.

6.6.4 Activity Log



```
06/17/21 11:23:19   [8001]: SIP Invite Session failed ... Response code: 408, Reason: Request Timeout
06/17/21 11:23:31   [2021]: SIP Invite Session failed ... Response code: 408, Reason: Request Timeout
06/17/21 11:23:33   [PA2 CH]: SIP Invite Session failed ... Response code: 408, Reason: Request Timeout
06/17/21 11:23:52   [8001]: SIP Invite Session failed ... Response code: 408, Reason: Request Timeout
06/17/21 11:24:04   [2021]: SIP Invite Session failed ... Response code: 408, Reason: Request Timeout
06/17/21 11:24:06   [PA2 CH]: SIP Invite Session failed ... Response code: 408, Reason: Request Timeout
06/17/21 11:24:25   [8001]: SIP Invite Session failed ... Response code: 408, Reason: Request Timeout
06/17/21 11:24:37   [2021]: SIP Invite Session failed ... Response code: 408, Reason: Request Timeout
06/17/21 11:24:39   [PA2 CH]: SIP Invite Session failed ... Response code: 408, Reason: Request Timeout
06/17/21 11:24:58   [8001]: SIP Invite Session failed ... Response code: 408, Reason: Request Timeout
06/17/21 11:25:10   [2021]: SIP Invite Session failed ... Response code: 408, Reason: Request Timeout
06/17/21 11:25:12   [PA2 CH]: SIP Invite Session failed ... Response code: 408, Reason: Request Timeout
06/17/21 11:25:28   [Administrator]: System Configuration changed ... 'Guest #21' updated
06/17/21 11:25:31   [8001]: SIP Invite Session failed ... Response code: 408, Reason: Request Timeout
06/17/21 11:25:43   [2021]: SIP Invite Session failed ... Response code: 408, Reason: Request Timeout
06/17/21 11:25:45   [PA2 CH]: SIP Invite Session failed ... Response code: 408, Reason: Request Timeout
06/17/21 11:26:04   [8001]: SIP Invite Session failed ... Response code: 408, Reason: Request Timeout
06/17/21 11:26:16   [2021]: SIP Invite Session failed ... Response code: 408, Reason: Request Timeout
```

During system operation the logging feature displays a time-stamped entry for each client connection/disconnection and key changes.

7. Failover Capability

In any mission critical communications system it is imperative to have built in redundancy. VCOM supports this function with a Failover capability. Failover by definition is the ability to automatically switch over from a primary working server to a secondary backup server should there be any catastrophic failure in operation of the primary server or its associated network.

7.1 Implementation

In the primary server, the IP address of the secondary server is configured. When the primary server starts, a connection to the secondary server is immediately established. Through this connection the primary server shares its licensing information to the secondary server. Additionally, the primary server conveys any operational changes to the system configuration to secondary server in real time so that the system configurations remain synchronized. This connection will remain active as long as both servers are running. If this connection is lost, the secondary server will immediately assume it is an active server allowing VCOM clients to connect. However in some cases even if the connection is not lost, the complexities of some network failures may still warrant the secondary server becoming the active server. When any VCOM client logs into the primary server, the secondary server IP address is automatically provided to it. In the event that communications with the primary server is lost, the client will automatically attempt to connect to the secondary server. If the secondary server is available and active, the VCOM client will log into the secondary server.

Once the secondary server becomes the active server, switching back to the primary server generally will require a manual authorization as the condition that caused the failover would need to be properly evaluated to ensure there is no possibility for reoccurrence of that event which would unnecessarily disrupt active communications. The manual switchover can be controlled through the System Administration application.

7.2 Failover Criteria

In normal operations, the primary server is always the active server. In general as long as the communications link between the primary and secondary server is connected, the primary server will remain as the active server. When a server is not the active server, logins will not be allowed. There are many different scenarios that can result in a failover event. The most common are as follows:

Communication link between primary and secondary servers lost due to primary server failure:
In this simplest scenario, the secondary server would recognize the loss of the primary server and immediately become the active server. All clients would also recognize the loss of the primary server and would immediately reconnect to the secondary server.

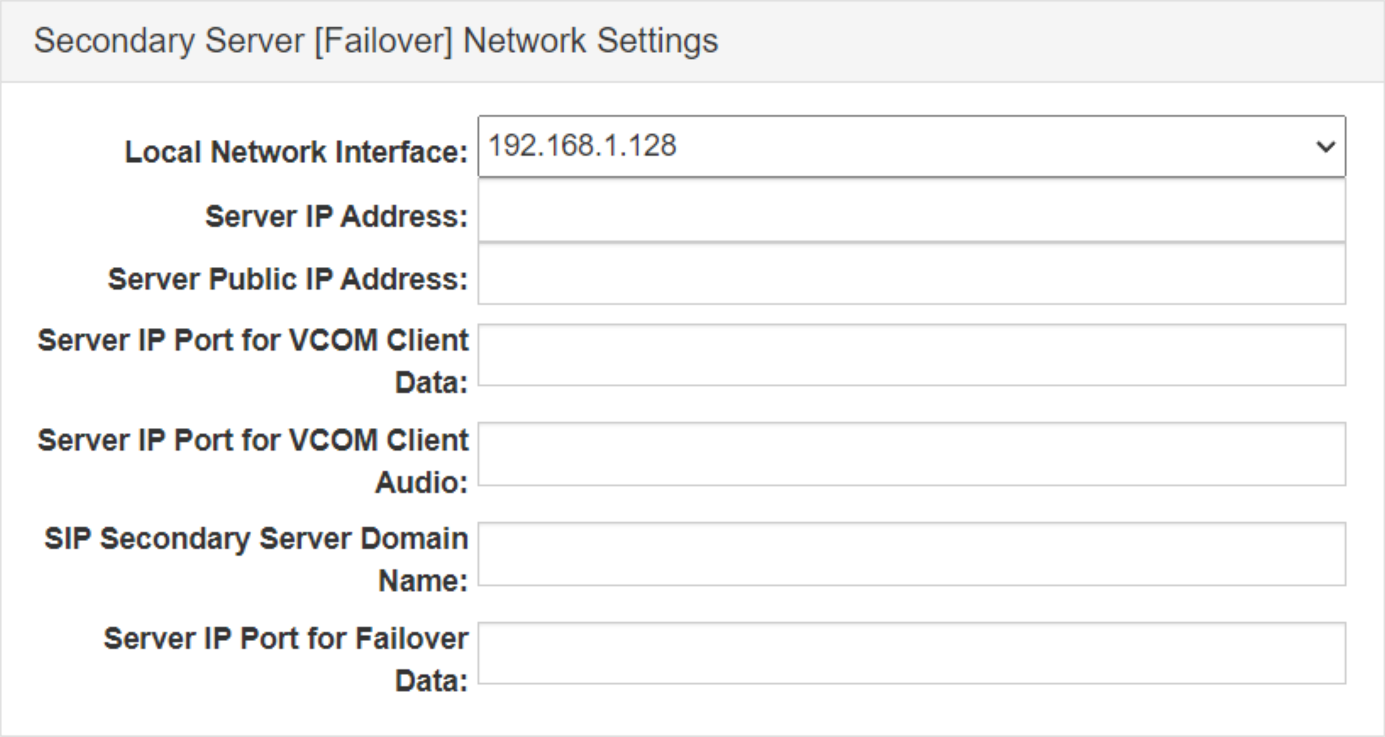
Communication link between primary and secondary servers lost due to failure of network infrastructure:
In this scenario, the secondary server would recognize the loss of the primary server and immediately become the active server. Since the primary server is still running, it too would also still consider itself to be the active server. However, if the network failure also resulted in the simultaneous loss of the majority of connected VCOM clients the primary server will deactivate itself forcing all remaining clients to connect to the secondary server.

Communication link between primary and secondary servers is not lost but partial failure of network infrastructure:
In this scenario, the partial network failure may result in the loss of a large portion of the VCOM clients. In this case the primary server will inform the secondary server to activate allowing connections to be made. If the secondary server reports the client connection were established the primary server will deactivate itself forcing all remaining clients to connect to the secondary server.

7.3 Other Considerations

Many SIP clients also support a failover server however the IP address of the secondary server often must be manually configured. The primary and secondary servers should never be co-located so as to eliminate the risk of simultaneous server failure due to environmental issues.

7.4 Setup



Secondary Server [Failover] Network Settings

Local Network Interface: 192.168.1.128

Server IP Address:

Server Public IP Address:

Server IP Port for VCOM Client Data:

Server IP Port for VCOM Client Audio:

SIP Secondary Server Domain Name:

Server IP Port for Failover Data:

On the primary server log into the System Administration and from the System Configuration tab select System Settings. In the Secondary Server [Failover] Network Settings click the Local Network Interface dropdown and select the IP address to use for communication between the Primary Server and the Secondary Server. In the Server IP Address field enter the IP address of the Secondary Server. In the Server IP Port for VCOM Client Data and Server IP Port for VCOM Client Audio fields type 1000. In the Server IP Port for Failover Data field type 1001.

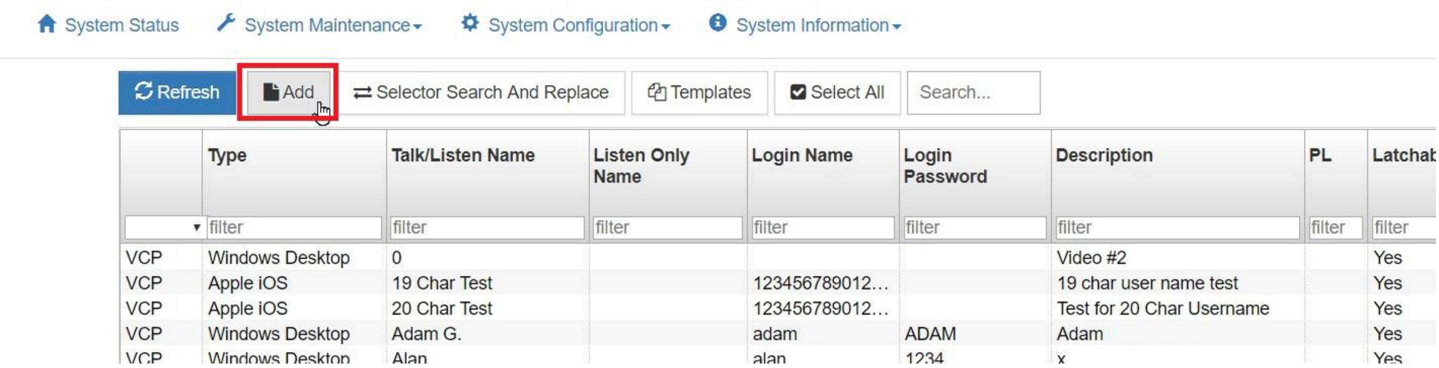
No configuration is necessary on the secondary server. The system license and all settings will be synced with the secondary when the connection is established.

Upon clicking save a connection between the primary server and secondary server will be established. Navigate to the System Status page and in the Failover Status section you will see the message "Primary Active, Secondary Standby" if the connection was established successfully. Once the connection is established the System Administration will not be accessible from the secondary server.

8. Connecting SIP Lines

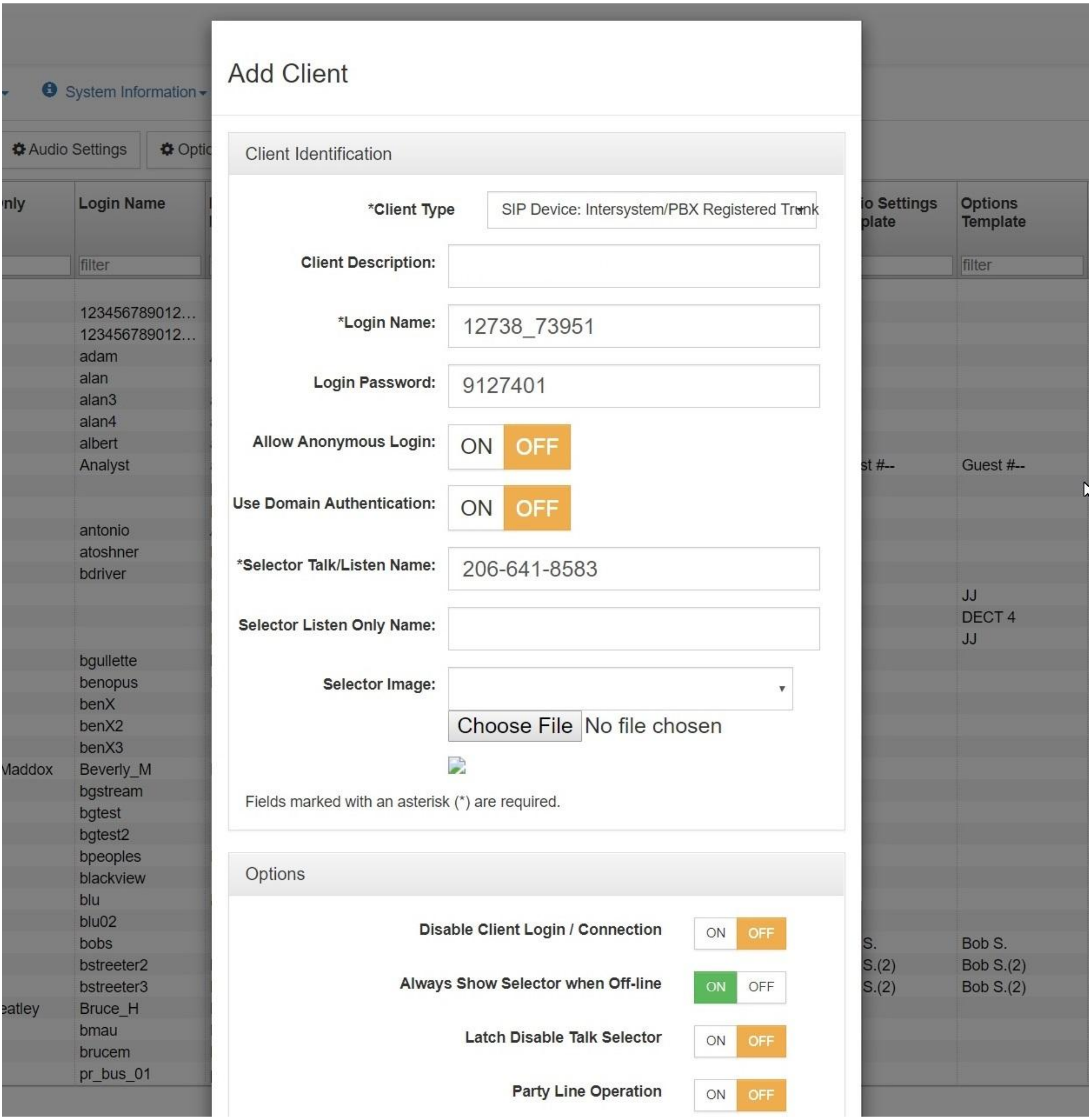
Purchasing SIP Lines
Intracom Systems does not provide SIP lines. The lines must be purchased through a 3rd party phone line provider. VCOM can connect to SIP lines using a Direct IP Trunk or a Registered Trunk. If you use a Direct IP Trunk SIP Server Domain Authentication must be disabled in the System Settings. A Registered Trunk is the preferred method and will be covered in this guide. VCOM requires 1 trunk per DID. Once a SIP line is purchased you will be provided a phone number, username, PBX IP, and you will set up a password.

Creating a SIP Client After logging into the VCOM System Administration under the System Configuration tab click Client Configuration.



	Type	Talk/Listen Name	Listen Only Name	Login Name	Login Password	Description	PL	Latchab
▾	filter	filter	filter	filter	filter	filter	filter	filter
VCP	Windows Desktop	0				Video #2		Yes
VCP	Apple iOS	19 Char Test		123456789012…		19 char user name test		Yes
VCP	Apple iOS	20 Char Test		123456789012…		Test for 20 Char Username		Yes
VCP	Windows Desktop	Adam G.		adam	ADAM	Adam		Yes
VCP	Windows Desktop	Alan		alan	1234	x		Yes

Click Add.



Add Client

Client Identification

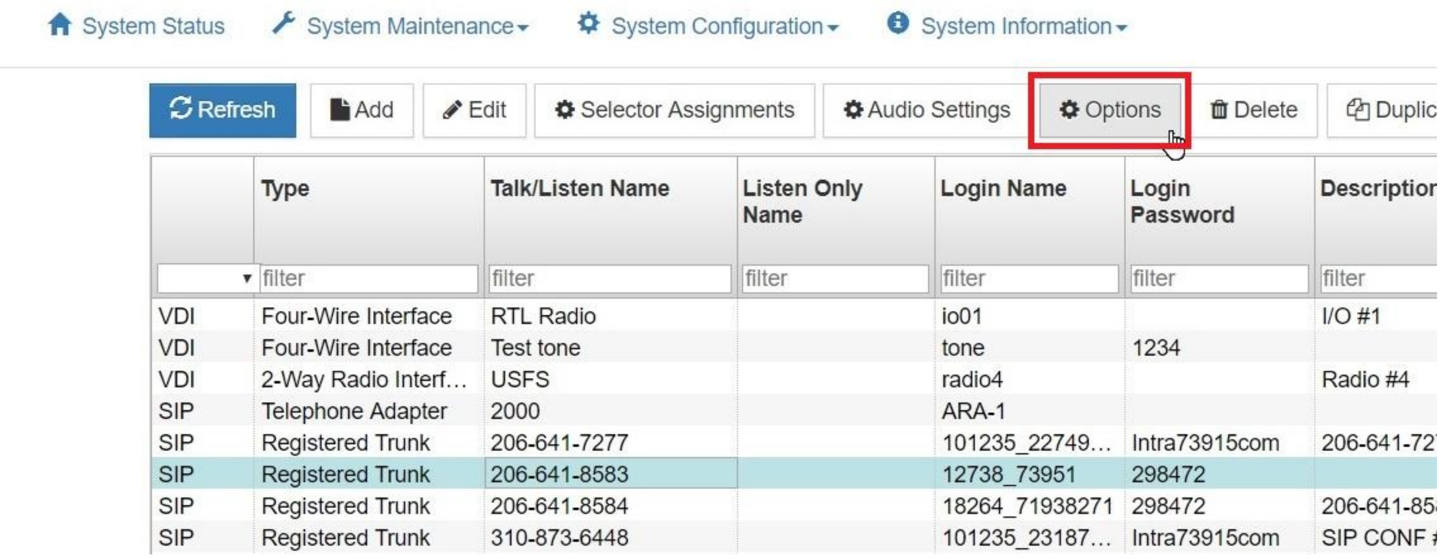
*Client Type	SIP Device: Intersystem/PBX Registered Trunk
Client Description:	
*Login Name:	12738_73951
Login Password:	9127401
Allow Anonymous Login:	ON [✓ OFF]
Use Domain Authentication:	ON [✓ OFF]
*Selector Talk/Listen Name:	206-641-8583
Selector Listen Only Name:	
Selector Image:	Choose File No file chosen

Fields marked with an asterisk (*) are required.

Options

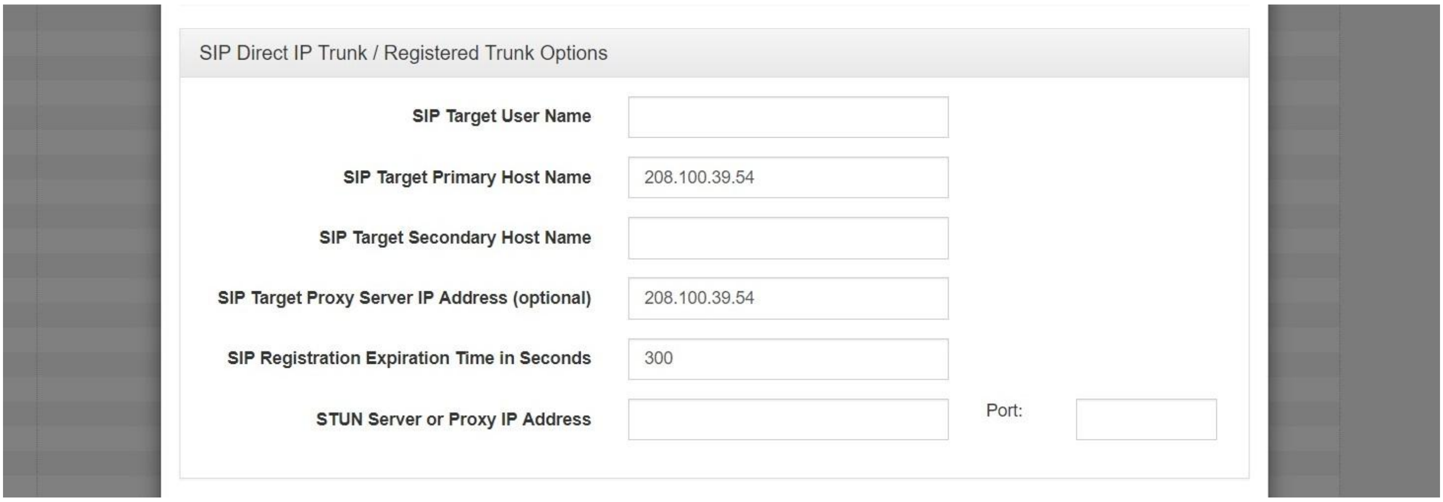
Disable Client Login / Connection	ON [✓ OFF]
Always Show Selector when Off-line	[✓ ON] OFF
Latch Disable Talk Selector	ON [✓ OFF]
Party Line Operation	ON [✓ OFF]

On the Client Type drop-down menu select “SIP Device: Intersystem/PBX Registered Trunk”. For Login Name enter in the username given by your SIP provider. The Login Password will be the password you set up with the SIP provider. In the screenshot above the Selector Talk/Listen Name is set to the phone number but this is not required. In the options panel below enable “Always Show Selector when Off-line”. Click save at the bottom of the menu.



	Type	Talk/Listen Name	Listen Only Name	Login Name	Login Password	Descriptior
	filter	filter	filter	filter	filter	filter
VDI	Four-Wire Interface	RTL Radio		io01		I/O #1
VDI	Four-Wire Interface	Test tone		tone	1234	
VDI	2-Way Radio Interf…	USFS		radio4		Radio #4
SIP	Telephone Adapter	2000		ARA-1		
SIP	Registered Trunk	206-641-7277		101235_22749…	Intra73915com	206-641-72
SIP	Registered Trunk	206-641-8583		12738_73951	298472	
SIP	Registered Trunk	206-641-8584		18264_71938271	298472	206-641-85
SIP	Registered Trunk	310-873-6448		101235_23187…	Intra73915com	SIP CONF #

Click on the client you just made to highlight it then click Options.



SIP Direct IP Trunk / Registered Trunk Options

SIP Target User Name	
SIP Target Primary Host Name	208.100.39.54
SIP Target Secondary Host Name	
SIP Target Proxy Server IP Address (optional)	208.100.39.54
SIP Registration Expiration Time in Seconds	300
STUN Server or Proxy IP Address	Port:

Scroll down to the bottom of the menu. For the SIP Target Primary Host Name enter in the PBX IP given by your SIP provider. You can also enter in the SIP Target Proxy Server IP Address, although this step is optional.

The settings show above can be left default but it is likely that you will want to change them. Below is a description of what each option does.

Call Notification Ring Tone: A file path can load an audio file to be played when an incoming call is placed.

Auto-Answer Notification Message: This option allows the selection of an audio wave file to be played as the notification message to the caller to indicate that the connection has been established between the SIP client and the VCOM Virtual Matrix. User provided files can be uploaded to the server provided the files are in a 16 bit mono audio format, preferably set to the same Audio Mix Sample Rate of the Virtual Matrix.

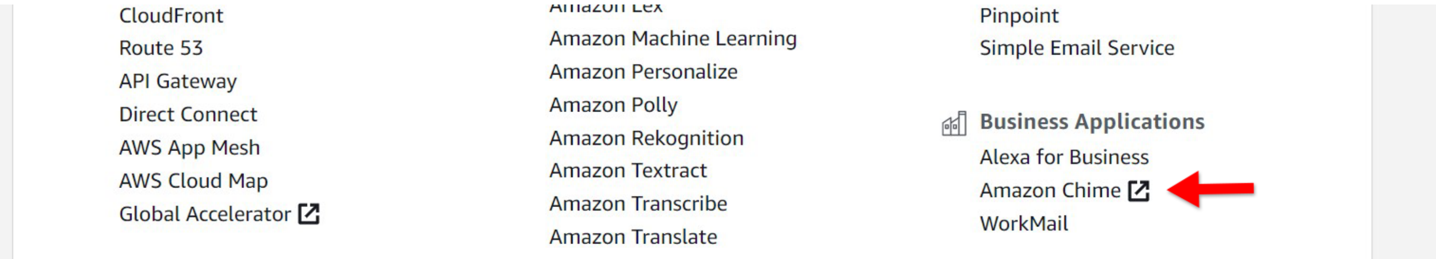
Auto-Answer Delay Time In Ms: This option sets the delay time in milliseconds after which the VCOM Virtual Matrix will automatically answer a received SIP call. Typically this value will be set to zero such that the call is answered immediately. In some situations it is desirable to delay answering the call so that VCOM Control Panels listening to that line will hear a ring signal.

Using the SIP Client You will need to assign the SIP client's selector to a Control Panel in order to talk or listen on the SIP line. Documentation on how to do this is available here. In order to dial out on the SIP line you will also need to set Enable Dial Pad Buttons to On in the client Options.

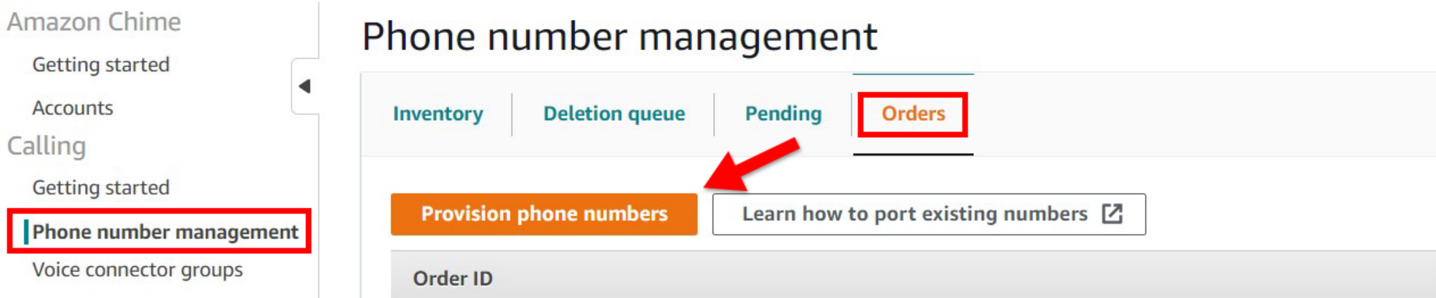
9. Connecting AWS Chime SIP Lines

9.1 AWS Settings

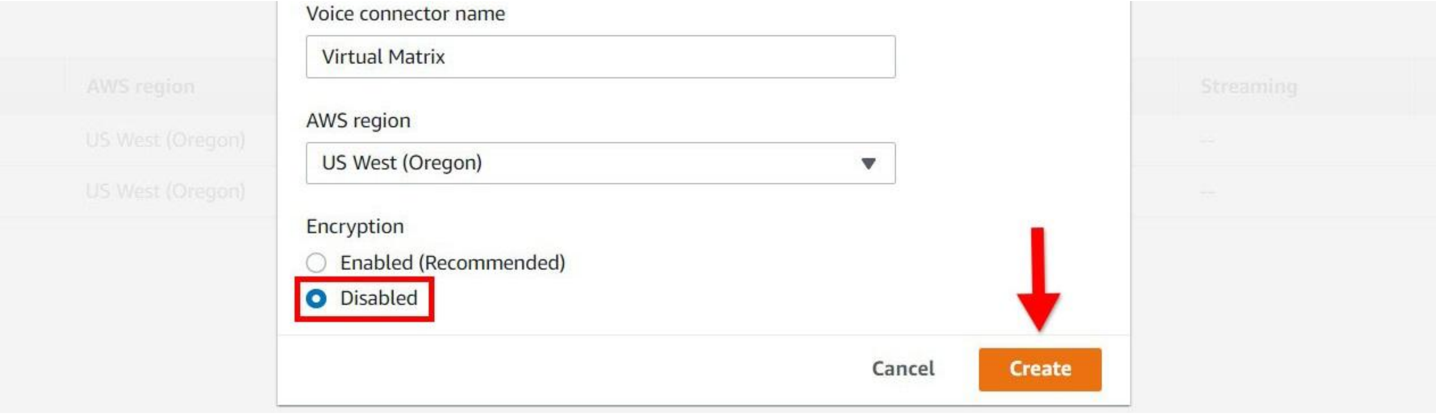
This portion of the guide will show how to create an AWS Chime Voice Connector and purchase phone lines for use with VCOM Virtual Matrix.



From the AWS Management Console navigate to the Business Applications section and select Amazon Chime.



On the left select Phone number management, select the Orders tab and then click Provision phone numbers.

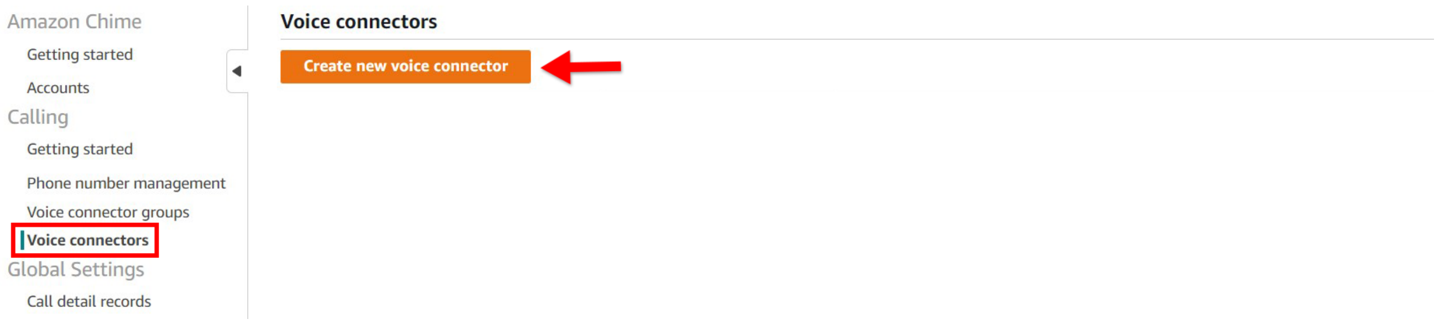


Voice connector name: Virtual Matrix

AWS region: US West (Oregon)

Encryption: ○ Enabled (Recommended) ● Disabled

Select Voice Connector and then click Next. Follow the prompts to purchase a phone number.



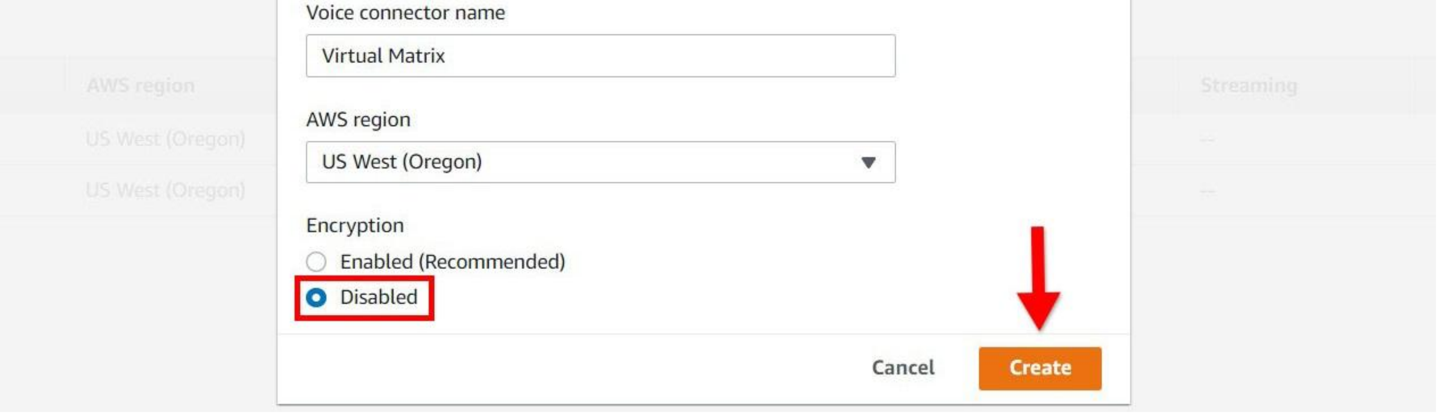
Amazon Chime
- Getting started
- Accounts

Calling
- Getting started
- Phone number management
- Voice connector groups
- Voice connectors

Global Settings
- Call detail records

Voice connectors

On the left select Voice connectors and then click Create new voice connector.

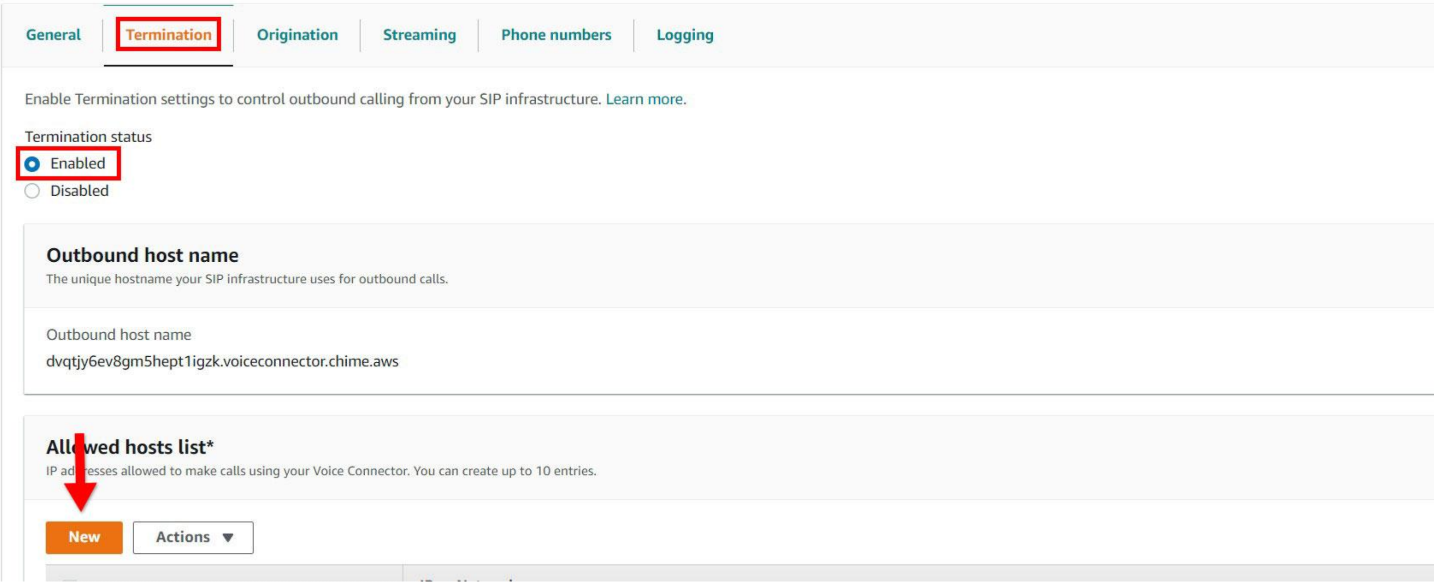


Voice connector name: Virtual Matrix

AWS region: US West (Oregon)

Encryption
- ○ Enabled (Recommended)
- ● Disabled

Enter a name for your Voice Connector and Disable Encryption then click Create.



Enable Termination settings to control outbound calling from your SIP infrastructure. Learn more.

Termination status
- ● Enabled
- ○ Disabled

Outbound host name

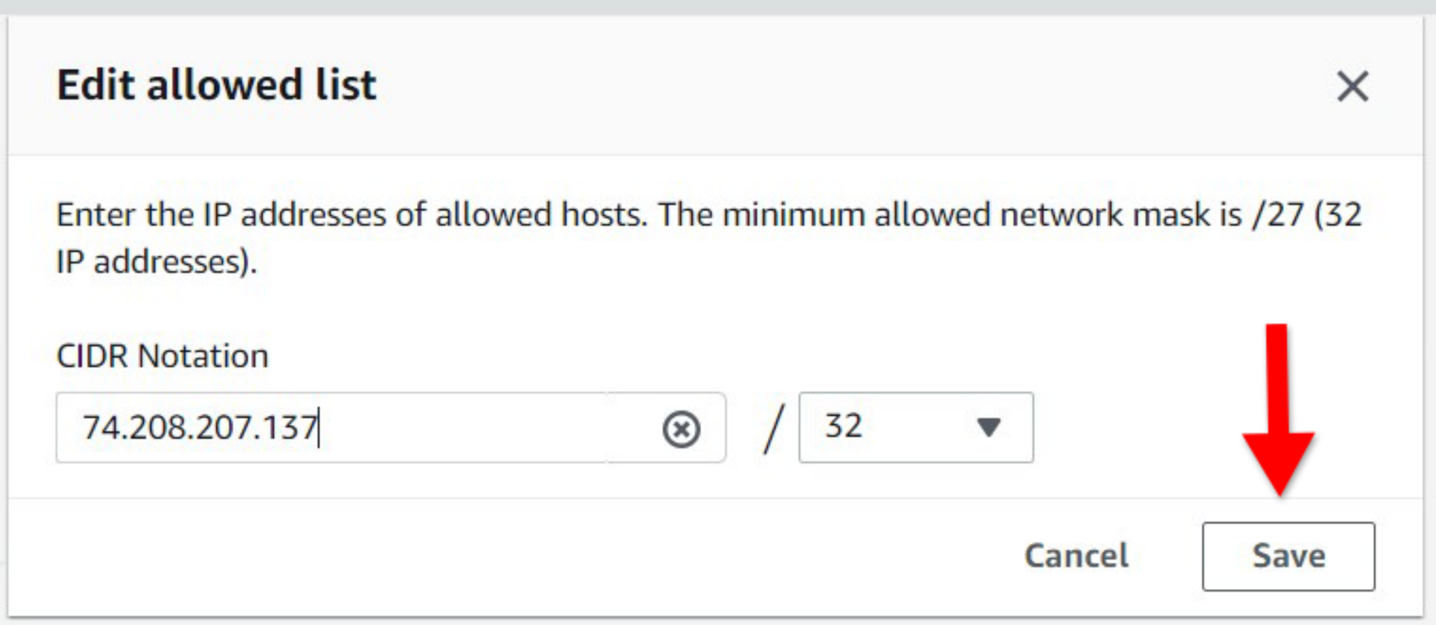
The unique hostname your SIP infrastructure uses for outbound calls.

Outbound host name: dvqtjy6ev8gm5hept1igzk.voiceconnector.chime.aws

All wed hosts list*

IP ad esses allowed to make calls using your Voice Connector. You can create up to 10 entries.

Select your new Voice Connector and navigate to the Termination tab. Set Termination status to enabled and then click New in the Allowed hosts list section.



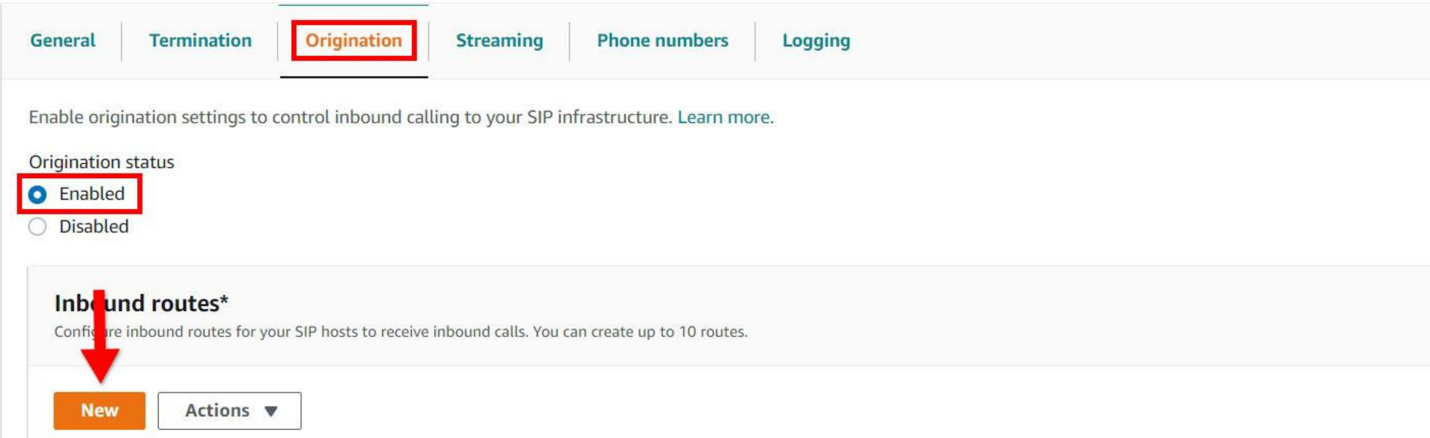
Edit allowed list

Enter the IP addresses of allowed hosts. The minimum allowed network mask is /27 (32 IP addresses).

CIDR Notation

74.208.207.137 / 32

Enter the IP address of your VCOM Virtual Matrix server and then click Save. Scroll down to the bottom of the Termination page and click Save.



Enable origination settings to control inbound calling to your SIP infrastructure. Learn more.

Origination status

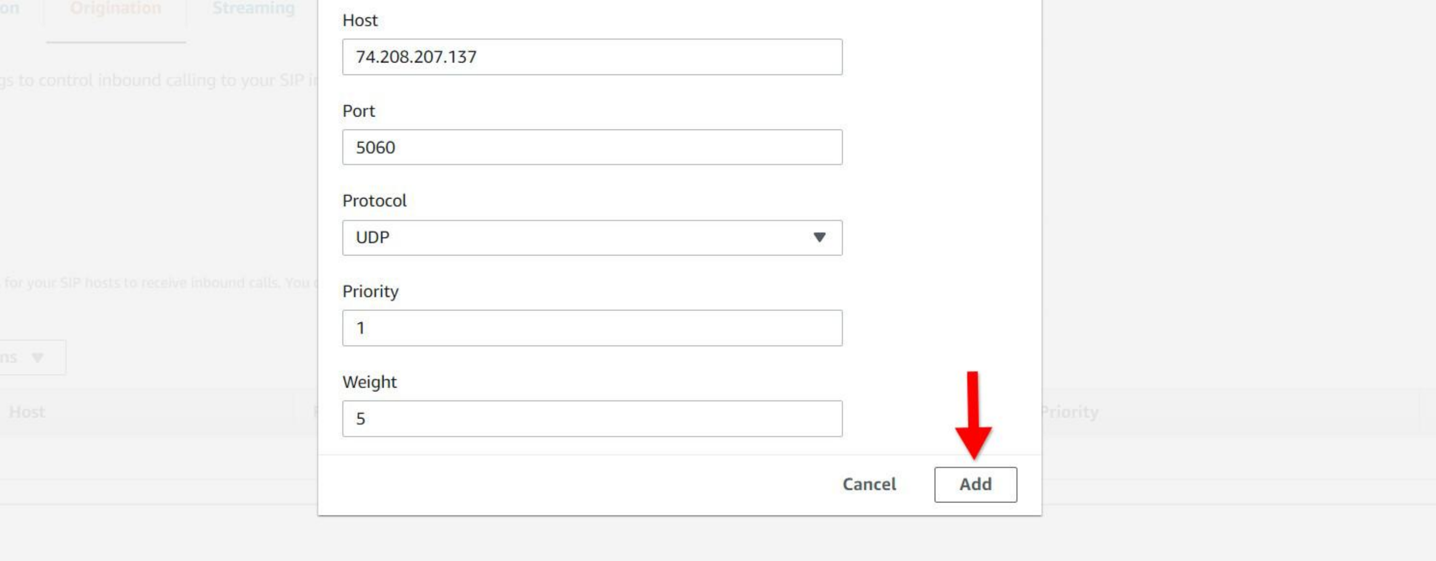
● Enabled

○ Disabled

Inbound routes*

Configure inbound routes for your SIP hosts to receive inbound calls. You can create up to 10 routes.

Navigate to the Origination page and under Origination status select Enabled. Click New under the Inbound routes section.



Host: 74.208.207.137

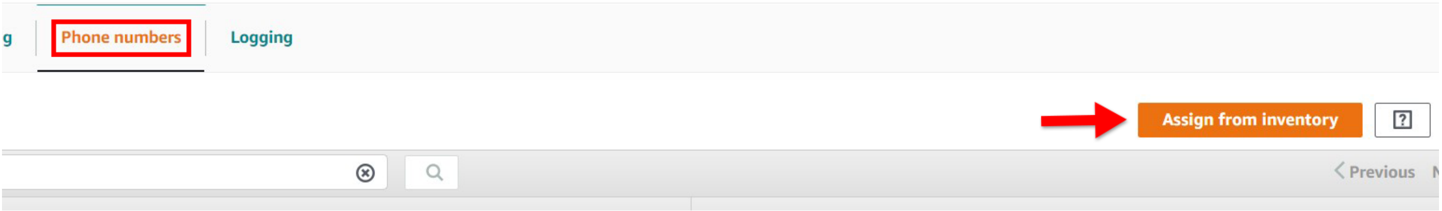
Port: 5060

Protocol: UDP

Priority: 1

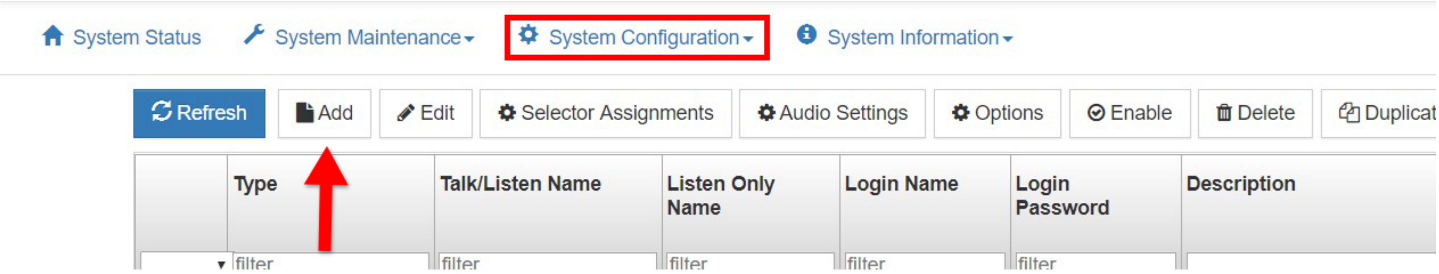
Weight: 5

In the Host section enter the IP address of your VCOM Virtual Matrix server then fill out the remaining fields as shown then click Add. Scroll down to the bottom of the page and click Save.



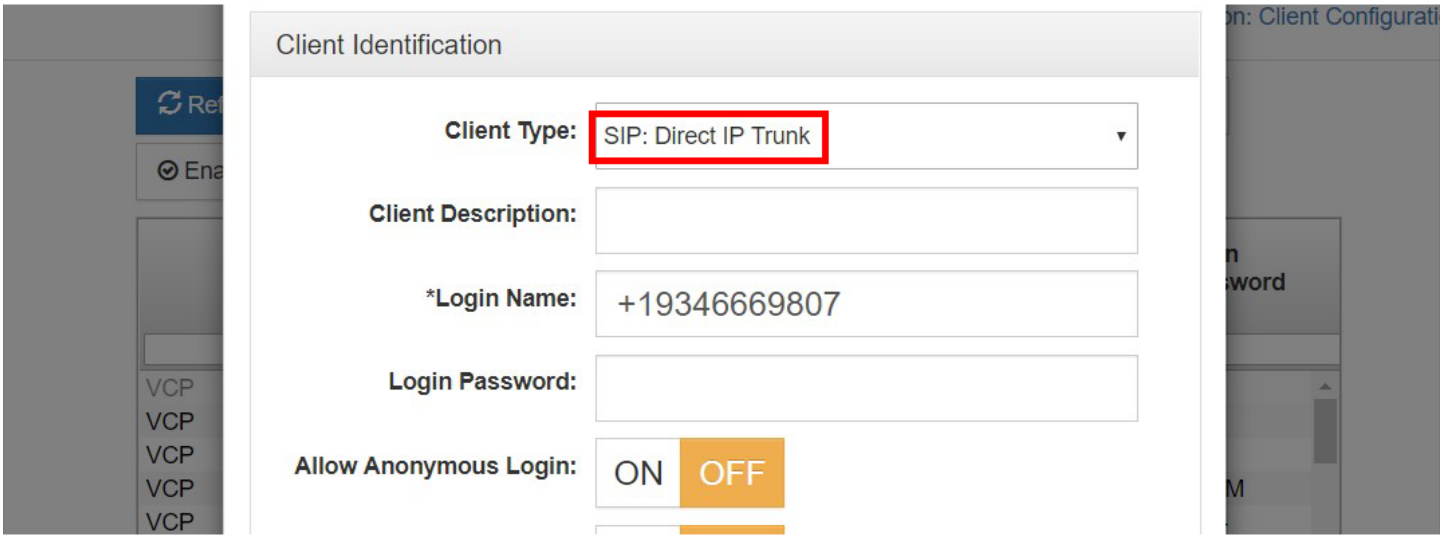
Navigate to the Phone numbers section and then click Assign from inventory. Select your desired phone number and then click Assign from inventory to add the line to the Voice Connector.

9.2 VCOM Settings



	Type	Talk/Listen Name	Listen Only Name	Login Name	Login Password	Description
	filter	filter	filter	filter	filter	

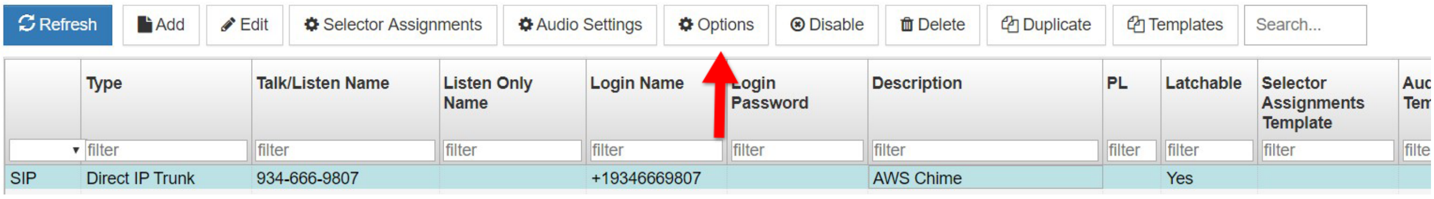
Access the System Administration application either by clicking on the desktop shortcut or by entering the IP address of the VCOM server in your browser’s address bar. From the System Configuration tab select Client Configuration then click Add.



Client Identification

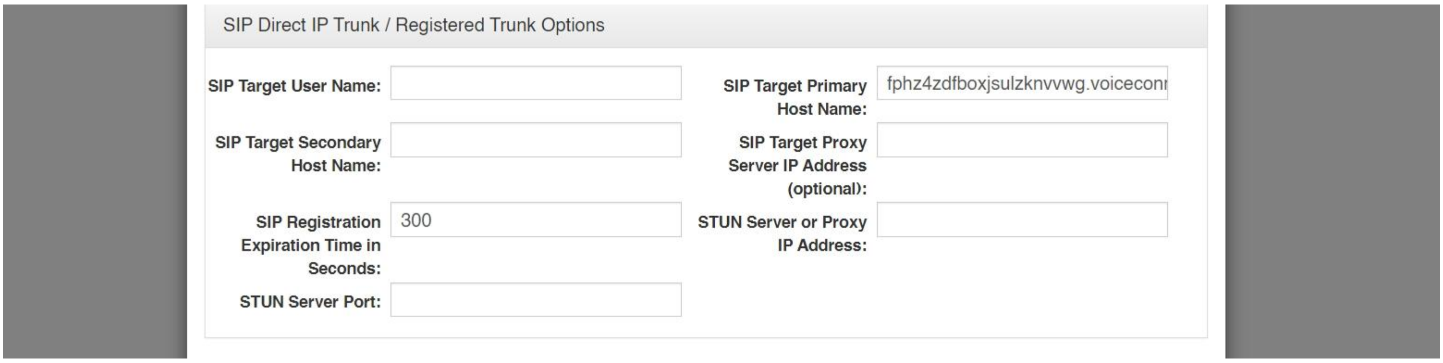
Client Type:	SIP: Direct IP Trunk
Client Description:	
*Login Name:	+19346669807
Login Password:	
Allow Anonymous Login:	ON [✓ OFF]

For the Client Type select SIP: Direct IP Trunk and enter the Login Name in the format shown above. Add a Selector Talk/Listen name and then click Save.



	Type	Talk/Listen Name	Listen Only Name	Login Name	Login Password	Description	PL	Latchable	Selector Assignments Template	Auc Tem
SIP	Direct IP Trunk	934-666-9807		+19346669807		AWS Chime		Yes		

Highlight the client you just created and then select Options from the menu.


SIP Direct IP Trunk / Registered Trunk Options

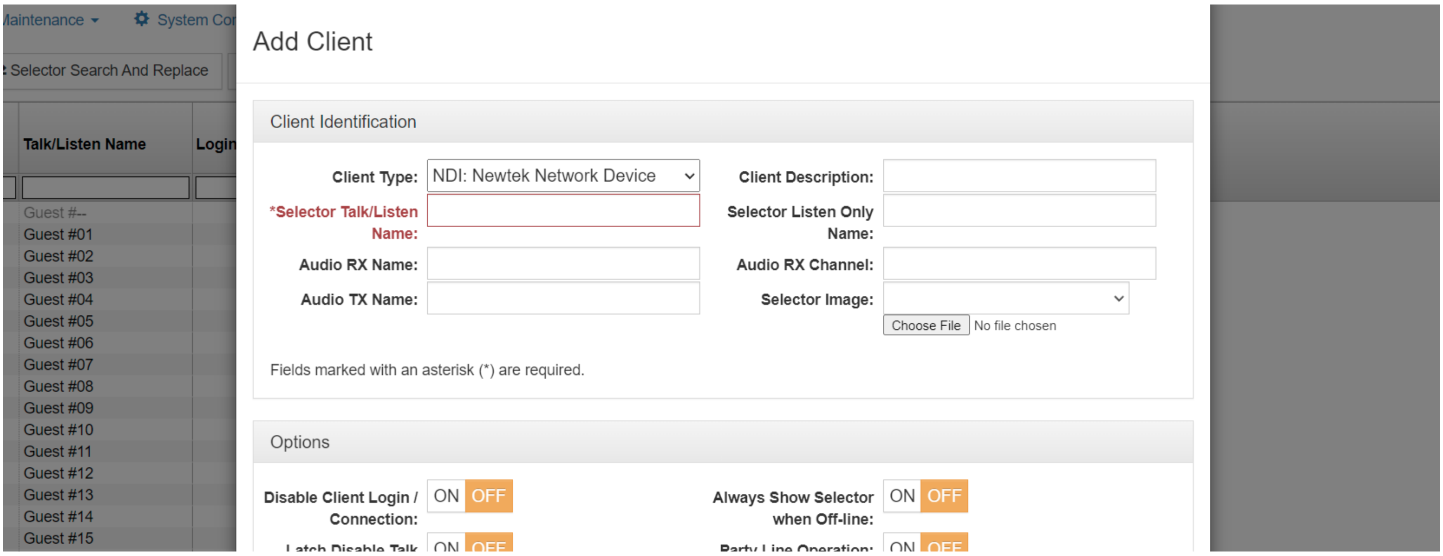
SIP Target User Name:		SIP Target Primary Host Name:	fphz4zdfboxjsulzknvvwg.voiceconn
SIP Target Secondary Host Name:		SIP Target Proxy Server IP Address (optional):	
SIP Registration Expiration Time in Seconds:	300	STUN Server or Proxy IP Address:	
STUN Server Port:			

In the SIP Target Primary Host Name field enter your Voice Connector ID in the format your-voice-connector-id.voiceconnector.chime.aws.

Note: When making an outbound call from VCOM you will need to precede the phone number with +1.

To use Direct IP Trunks such as AWS Chime SIP lines it is necessary to disable SIP Server Domain Authentication in the System Settings.

10. Connecting NDI Audio Streams



Add Client

Client Identification

Client Type:	NDI: Newtek Network Device	Client Description:	
*Selector Talk/Listen Name:		Selector Listen Only Name:	
Audio RX Name:		Audio RX Channel:	
Audio TX Name:		Selector Image:	Choose File No file chosen

Fields marked with an asterisk (*) are required.

Options

Disable Client Login / Connection:	ON OFF	Always Show Selector when Off-line:	ON OFF
Latch Disable Talk	ON OFF	Party Line Operation:	ON OFF

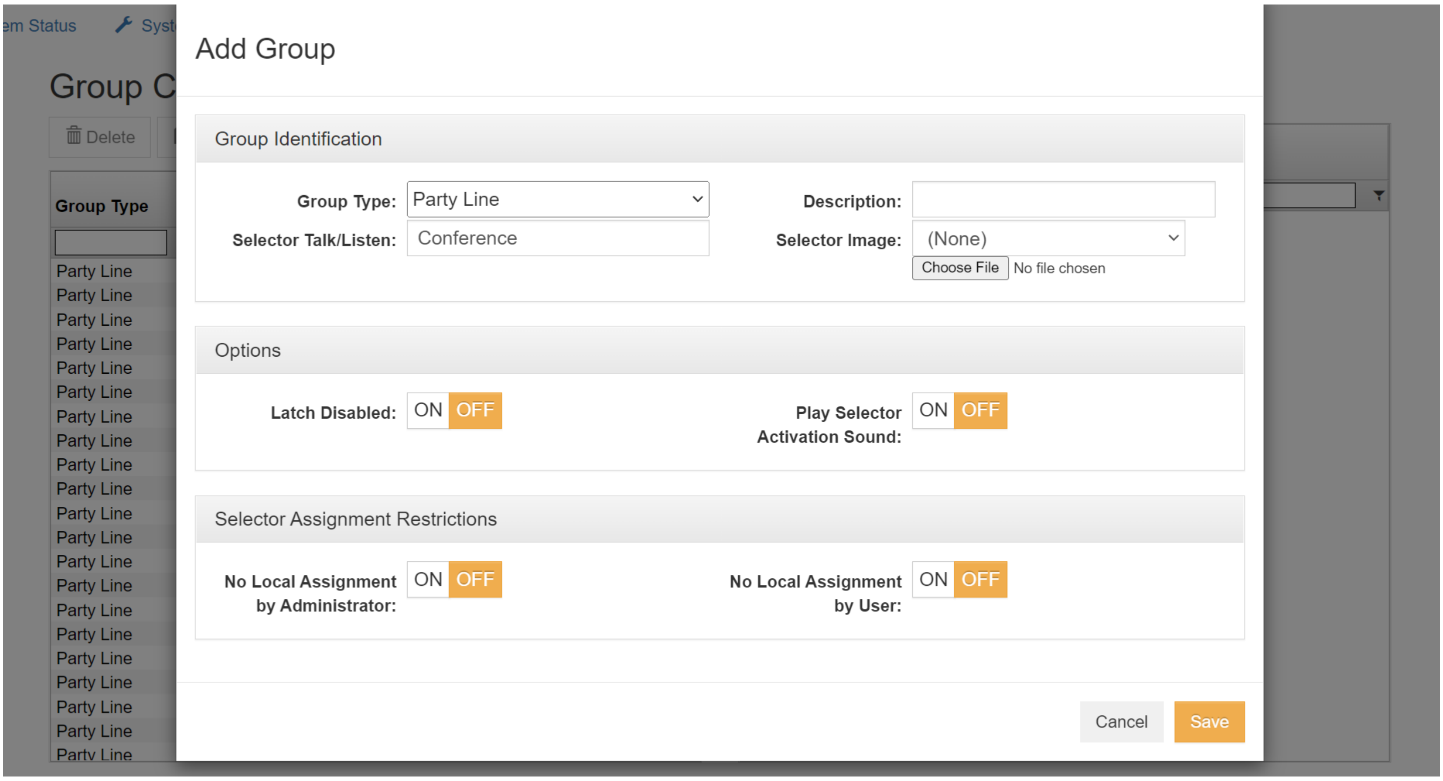
Log into the System Administration and from the System Configuration menu select Client Configuration. Click Add and select NDI: Newtek Network Device from the Client Type dropdown. The Audio RX Name shouldbe in the format `<machine_name> (<stream_name>)`. The Audio TX Name field should only contain the stream name.

When the server starts it will immediately begin pulling audio from the Audio RX Name/ Channel and be ready to send audio to anyone making a request for the Audio Tx Name. The video component if present is discarded.

11. Connecting to Conferencing Platforms

VCOM can be used to dial into virtually any conferencing platform. The majority of conferencing platforms such as Microsoft Teams, Google Meet, and Zoom support dialing into meetings via a designated phone number and conference pin code. In order to dial into a meeting you must first provision and configure a SIP phone line for VCOM. Follow the Connecting SIP Lines or Connecting AWS Chime SIP Lines documentation before continuing with this guide.

It is possible to connect multiple VCOM users / channels to a meeting using a single SIP phone line. This can be done using a Party Line. To create a Party Line log into the System Administration and select Group Configuration from the System Configuration dropdown.



Add Group

Group Identification

Group Type: Party Line

Description:

Selector Talk/Listen: Conference

Selector Image: (None)

Choose File No file chosen

Options

Latch Disabled: ON OFF

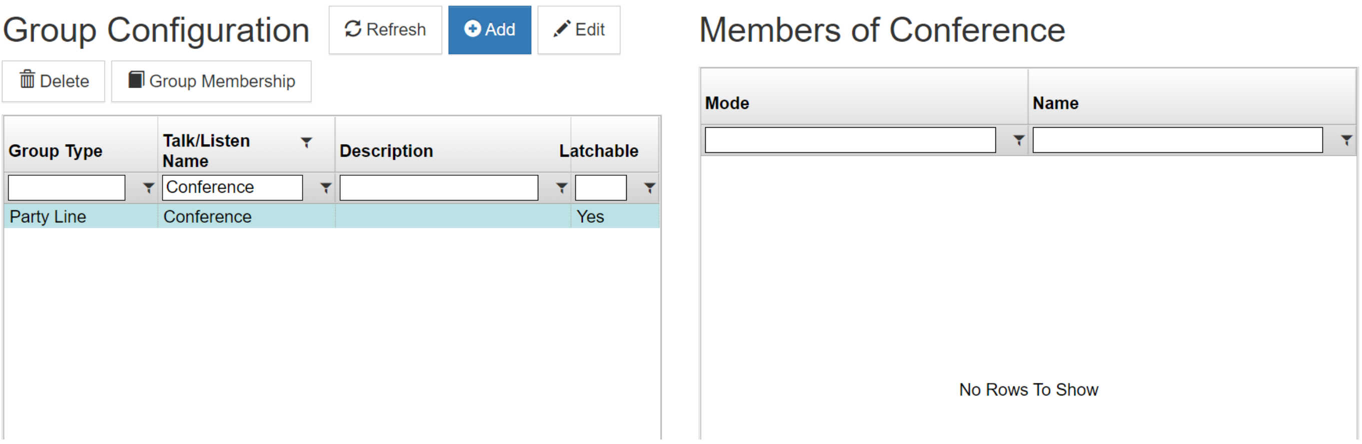
Play Selector Activation Sound: ON OFF

Selector Assignment Restrictions

No Local Assignment by Administrator: ON OFF

No Local Assignment by User: ON OFF

Click the blue Add button at the top of the screen. In the Add Group menu change Group Type to Party Line, enter a Selector Talk/Listen name and click Save.

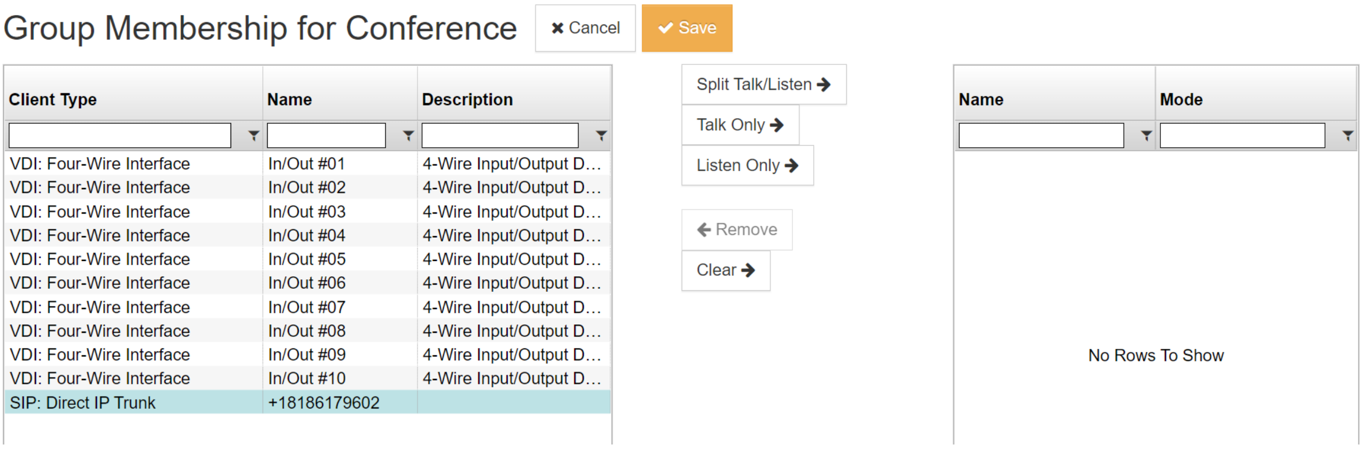


Group Type	Talk/Listen Name	Description	Latchable
	Conference		
Party Line	Conference		Yes

Mode	Name

No Rows To Show

Select the Party Line you just created and then click the Group Membership button.

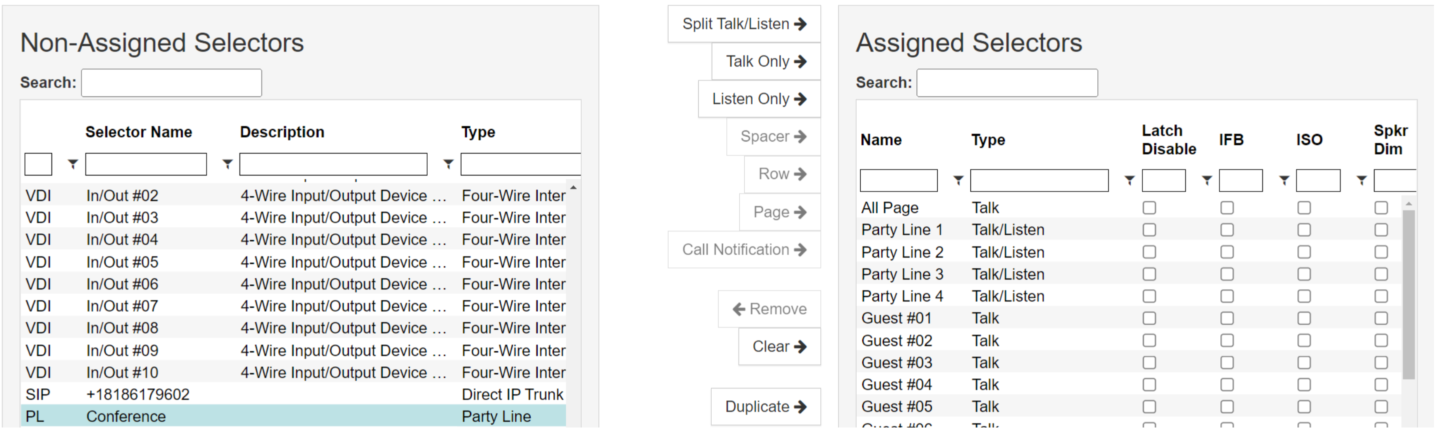


Client Type	Name	Description
VDI: Four-Wire Interface	In/Out #01	4-Wire Input/Output D…
VDI: Four-Wire Interface	In/Out #02	4-Wire Input/Output D…
VDI: Four-Wire Interface	In/Out #03	4-Wire Input/Output D…
VDI: Four-Wire Interface	In/Out #04	4-Wire Input/Output D…
VDI: Four-Wire Interface	In/Out #05	4-Wire Input/Output D…
VDI: Four-Wire Interface	In/Out #06	4-Wire Input/Output D…
VDI: Four-Wire Interface	In/Out #07	4-Wire Input/Output D…
VDI: Four-Wire Interface	In/Out #08	4-Wire Input/Output D…
VDI: Four-Wire Interface	In/Out #09	4-Wire Input/Output D…
VDI: Four-Wire Interface	In/Out #10	4-Wire Input/Output D…
SIP: Direct IP Trunk	+18186179602	

Name	Mode

No Rows To Show

On the left side menu select your SIP phone line and click the Split Talk/Listen button. Select any additional client whose audio I/O you wish to tie into the conference line then click Save.

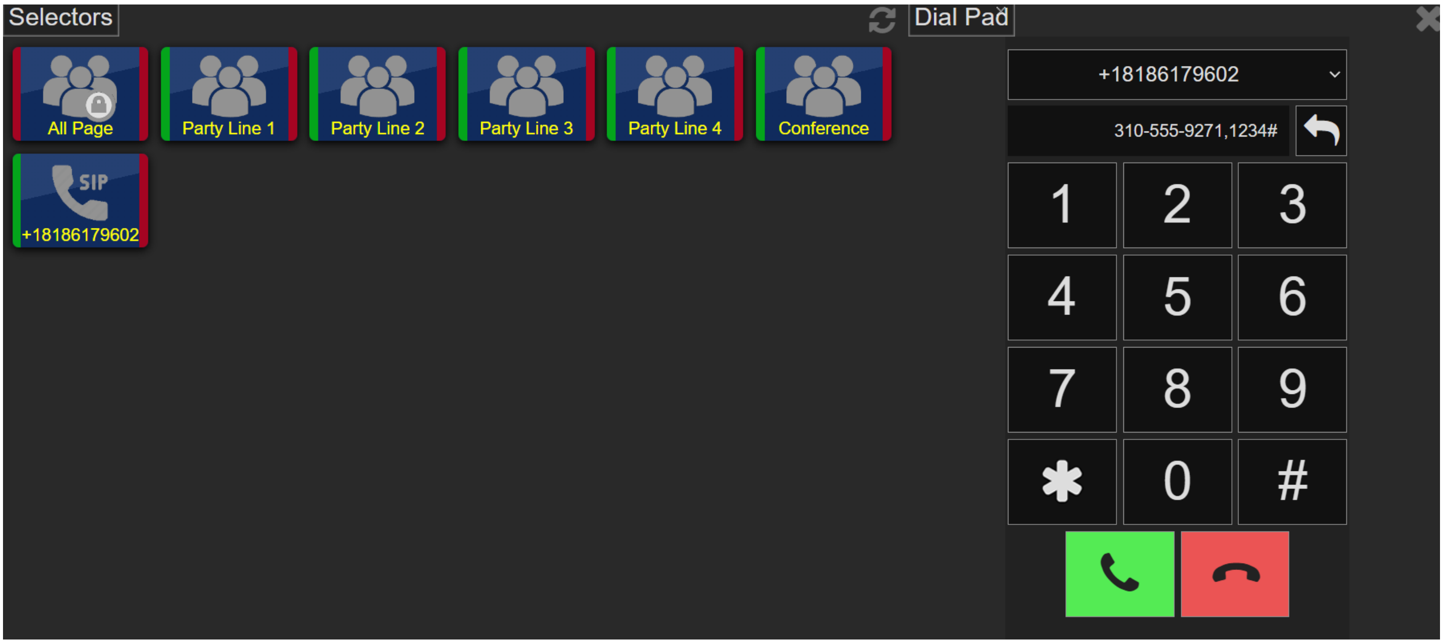


	Selector Name	Description	Type
VDI	In/Out #02	4-Wire Input/Output Device …	Four-Wire Inter
VDI	In/Out #03	4-Wire Input/Output Device …	Four-Wire Inter
VDI	In/Out #04	4-Wire Input/Output Device …	Four-Wire Inter
VDI	In/Out #05	4-Wire Input/Output Device …	Four-Wire Inter
VDI	In/Out #06	4-Wire Input/Output Device …	Four-Wire Inter
VDI	In/Out #07	4-Wire Input/Output Device …	Four-Wire Inter
VDI	In/Out #08	4-Wire Input/Output Device …	Four-Wire Inter
VDI	In/Out #09	4-Wire Input/Output Device …	Four-Wire Inter
VDI	In/Out #10	4-Wire Input/Output Device …	Four-Wire Inter
SIP	+18186179602		Direct IP Trunk
PL	Conference		Party Line

Name	Type	Latch Disable	IFB	ISO	Spkr Dim
All Page	Talk	□	□	□	□
Party Line 1	Talk/Listen	□	□	□	□
Party Line 2	Talk/Listen	□	□	□	□
Party Line 3	Talk/Listen	□	□	□	□
Party Line 4	Talk/Listen	□	□	□	□
Guest #01	Talk	□	□	□	□
Guest #02	Talk	□	□	□	□
Guest #03	Talk	□	□	□	□
Guest #04	Talk	□	□	□	□
Guest #05	Talk	□	□	□	□

From the System Configuration menu select Client Configuration. Select the client that you want to be able to access the Party Line and click the Selector Assignments button. Select the Party Line on the left side of the screen and click the Split Talk/Listen button then click Save.

You will also need to assign the SIP phone line to at least one client. This will allow the client to dial into the meeting.



310-555-9271,1234#

To connect to a meeting log into a client that has the SIP phone line assigned as a selector and click the handset icon at the top of the screen. Enter the meeting phone number followed by a comma and then the meeting pin. Click the green handset icon to dial into the meeting.

12. VCOM Device Interface

The VCOM Device Interface is a software application that bridges VCOM with multiple external communications systems. This document provides information on how to install, configure, and use the VCOM Device Interface.

Note: A hardware audio/logic interface is required to convert 4-wire and 2-wire analog signals into digital to bridge with the IP world, typically via USB connection. To bridge a telephone system a hybrid is also required or a PC/server card which accepts analog phone lines or T-1(s) directly.

12.1 Installation

System Requirements
Processor (dedicated server): 3 Ghz or greater
Processor (multi-purpose server): 3.4 GHz or greater
Memory: Follow OS requirements
Storage: Follow OS requirements
OS: Windows 7, 8, 10, Windows Server 2019

Bandwidth Requirements
Recommended configuration: 100BaseT connection over private LAN

Bandwidth Utilization per client:

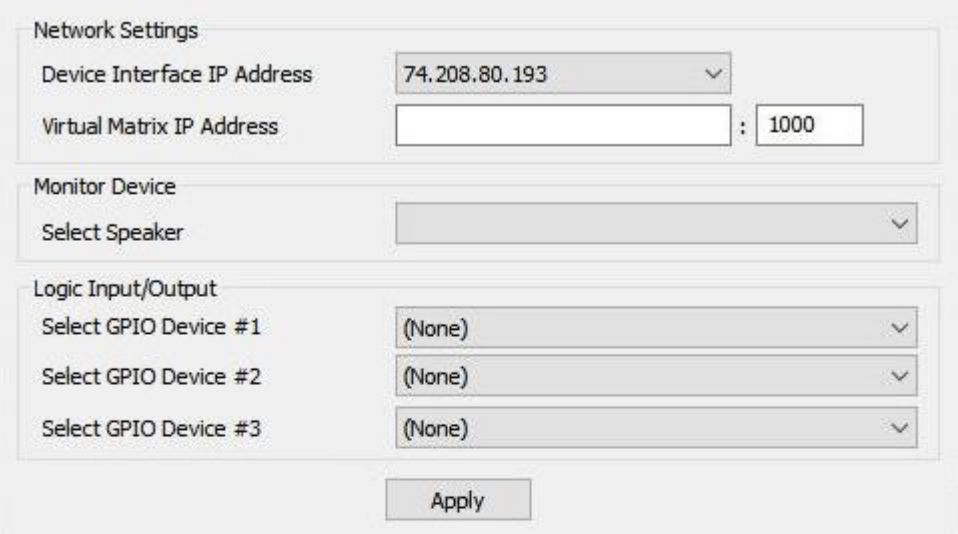
Audio Sample Rate	Data Rate (Kbps) [ATS=20ms*] (Default)	Data Rate (Kbps) [ATS=40ms*]	Data Rate (Kbps) [ATS=60ms*]	Data Rate (Kbps) [ATS=80ms*]	Data Rate (Kbps) [ATS=100ms*]
8 KHz	32	23.6	20.8	19.4	18.56
16 KHz	44.8	36.4	33.6	32.2	31.36
32 KHz	46.8	38.4	35.6	34.2	33.36

*ATS = Audio Time Slice per packet which controls how many 20ms audio frames are transmitted within a single UDP packet. As each UDP packet requires a fixed amount of overhead, the more frames sent at the same time, the less the UDP overhead which conserves network bandwidth. Conversely, the more audio frames sent per transmission, the greater the system latency and the potential audible consequence of a lost packet. The default is 20ms.

Firewall Requirements
Allow TCP connection for data and UDP connection for audio on port 1000

Installation
Download VCOM Device Interface from our downloads page and unzip the installer. Run the installer and follow the prompts. You will need to accept Intracom Systems’ License Agreement to install the software.

12.2 Configuration



Network Settings

Device Interface IP Address: 74.208.80.193

Virtual Matrix IP Address: : 1000

Monitor Device

Select Speaker:

Logic Input/Output

Select GPIO Device #1: (None)

Select GPIO Device #2: (None)

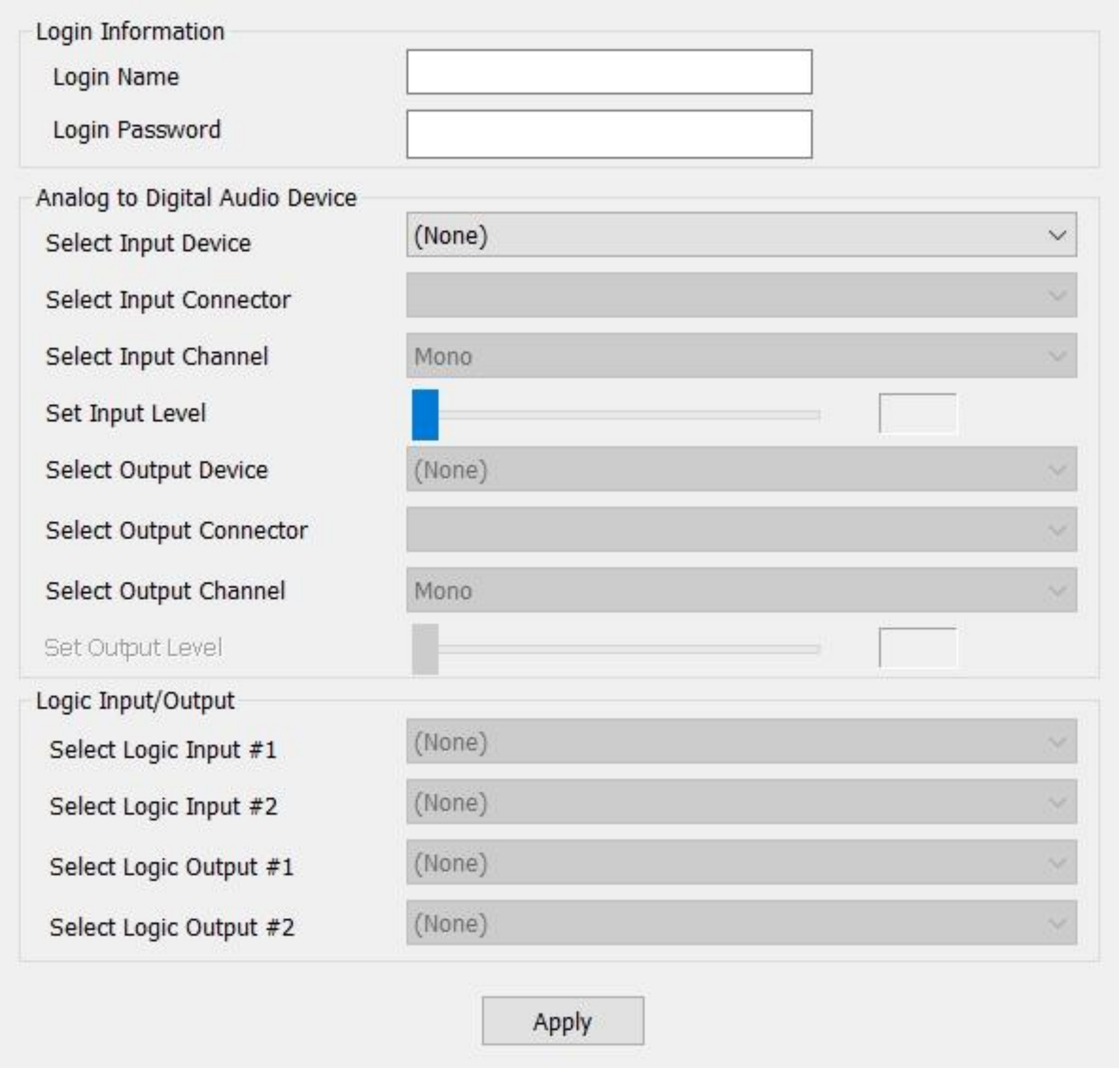
Select GPIO Device #3: (None)

The Configuration menu will be displayed upon first launch.

Device Interface IP Address: The IP address of your computer. This setting may need to be changed if you have multiple network adapters.

Logic Input/Output: Optionally select the GPIO(s) device that you will use to control your audio device(s).

Click Add to configure a new device connection.



Login Information

Login Name

Login Password

Analog to Digital Audio Device

Select Input Device: (None)

Select Input Connector:

Select Input Channel: Mono

Set Input Level

Select Output Device: (None)

Select Output Connector:

Select Output Channel: Mono

Set Output Level

Logic Input/Output

Select Logic Input #1: (None)

Select Logic Input #2: (None)

Select Logic Output #1: (None)

Select Logic Output #2: (None)

Enter the Login Name and Login Password for the device as pre-configured in the VCOM System Configuration application.

Select Input/Output Device: Allows selection of the audio input/output device you wish to use.

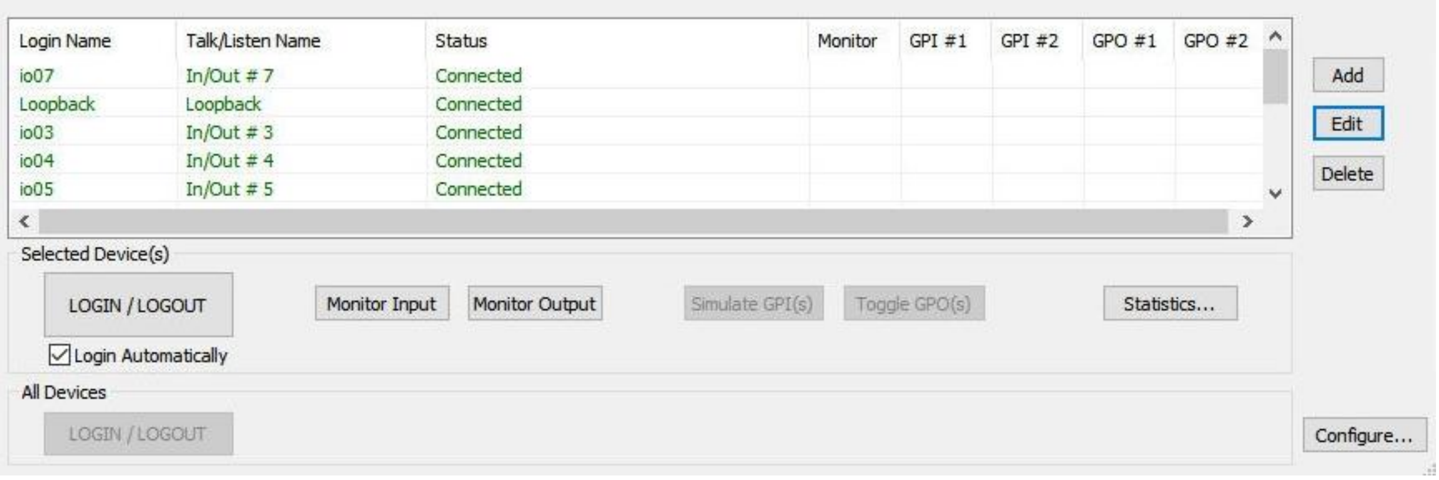
Select Input/Output Connector: Allows selection of which input/output jack the audio input device is to use.

Select Input/Output Channel: Allows selection of Mono, Stereo – Left, or Stereo – Right.

Set Input Level: Allows adjustment of the input audio level.

Under **Logic Input/Output** , select the logic protocol and input(s)/output(s) that you wish to use for the given audio device. In most circumstances you will only have one logic input and output

12.3 Operation



Login Name	Talk/Listen Name	Status	Monitor	GPI #1	GPI #2	GPO #1	GPO #2
io07	In/Out # 7	Connected					
Loopback	Loopback	Connected					
io03	In/Out # 3	Connected					
io04	In/Out # 4	Connected					
io05	In/Out # 5	Connected					

☑ Login Automatically

Login / Logout: Connects or disconnects all clients. If a client is highlighted then the button will only affect that client.

Simulate GPI(s): Demonstrates the effect of activating the configured General Purpose Inputs and is for testing purposes only.

Toggle GPO(s): Forces activation of the configured General Purpose Outputs and is for testing purposes only.

Statistics: Displays the send and receive audio rates and packet loss data

12.4 Troubleshooting

Q: When attempting to login to the Virtual Matrix, why do I get a “Cannot connect to Virtual Matrix” message? A: The Control Panel is unable to establish a TCP/IP data connection with the Virtual Matrix. Check the Control Panel Configuration to ensure the ‘Control Panel IP Address’ is valid and represents a valid and active network connection. Ensure that the ‘Virtual Matrix IP Address’ is entered exactly as provided with the designated port number. Check to ensure a corporate firewall is not intentionally blocking the designated TCP/IP data port.

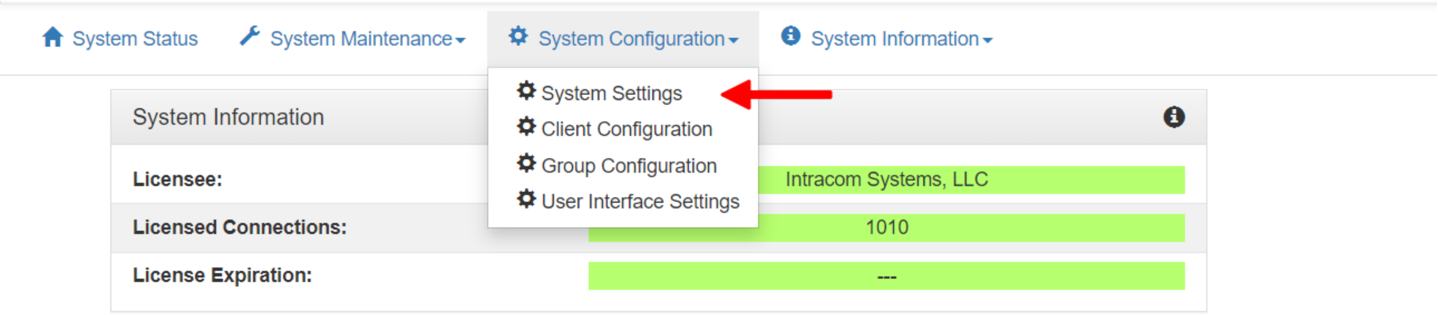
Q: When attempting to login to the Virtual Matrix, why do I get an “Unable to establish return audio path” message?
A: The Control Panel is unable to establish a UDP audio connection with the Virtual Matrix. Check to ensure a corporate firewall is not intentionally blocking the designated UDP audio port, which is typically the same as the TCP/IP data port.

Q: When attempting to login to the Virtual Matrix, why do I get a “Provided user name and/or password is invalid!” message?
A: The Control Panel is unable to validate the username and password. Check to ensure the name is typed exactly as provided as the username and password are both case sensitive. Check to ensure the correct TCP/IP data port is specified to ensure you are logging in to the correct system.

13. Audio Recording

Two different models of recording are supported in VCOM. The first is file based recording where each endpoint to be recorded is outputted to time a stamped WAV file. The second is based on industry standard SIPREC for interfacing to the third party SIPREC recording platforms. Control Panels, Device Interfaces, SIP connections, and/or Party Lines can be recorded.

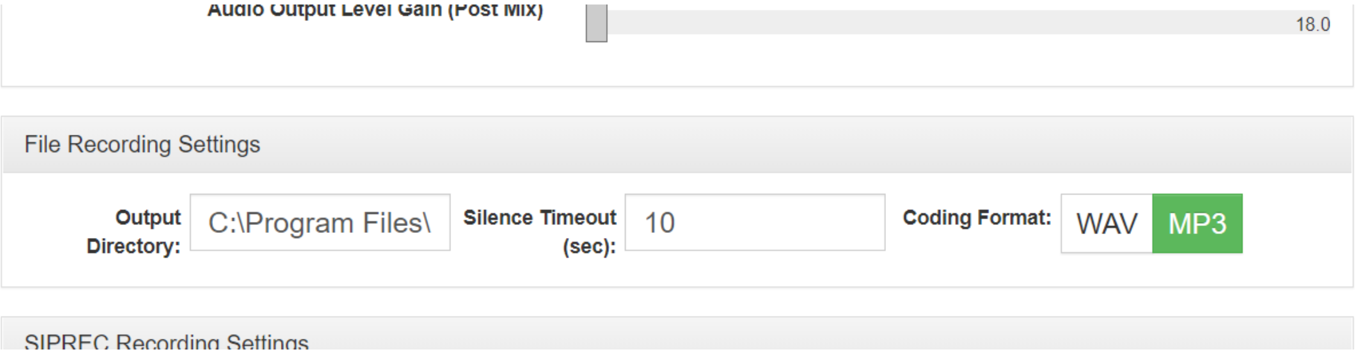
13.1 File-based Audio Recording



System Information

Licensee:	Intracom Systems, LLC
Licensed Connections:	1010
License Expiration:	---

Log into the System Administration and select System Settings from the System Configuration menu.



File Recording Settings

Output Directory: C:\Program Files\
Silence Timeout (sec): 10
Coding Format: WAV [✓ MP3]

Scroll down to the File Recording Settings section.

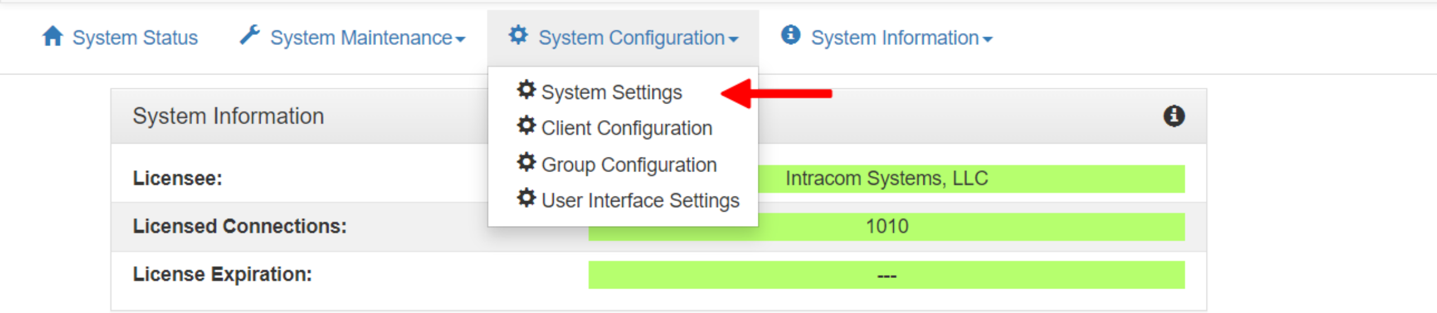
Output Directory: The directory in which the audio recordings are stored.

Silence Timeout (sec): The duration after silence is detected on the Client that the system will wait to end the audio recording file. The default is 10 seconds.

Adjust the settings if needed then click the Save button.

Note: The recording functionality must be enabled in the system's license. You will not see the File Recording Settings if the feature is not licensed.

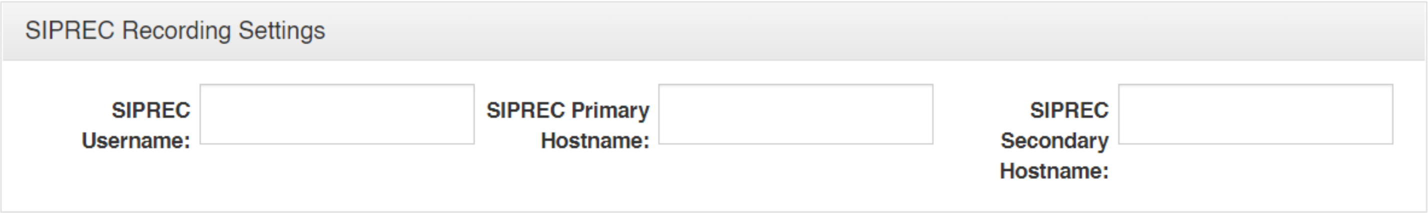
13.2 SIPREC Audio Recording



System Information

Licensee:	Intracom Systems, LLC
Licensed Connections:	1010
License Expiration:	---

Log into the System Administration and select System Settings from the System Configuration menu.


SIPREC Recording Settings

SIPREC Username:

SIPREC Primary Hostname:

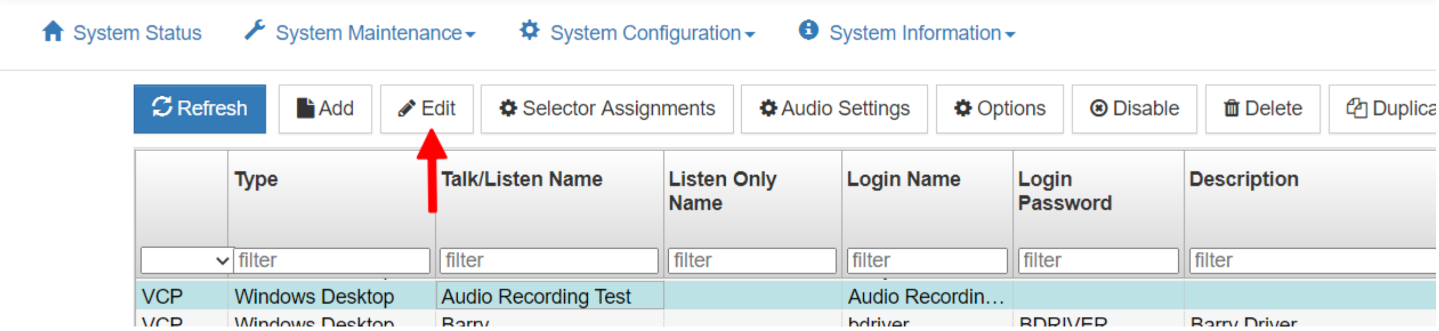
SIPREC Secondary Hostname:

Scroll down to the SIPREC Recording Settings section and fill out the requisite fields to allow VCOM Virtual Matrix to connect to your SIPREC server.

Note: The recording functionality must be enabled in the system's license. You will not see the SIPREC Recording Settings if the feature is not licensed.

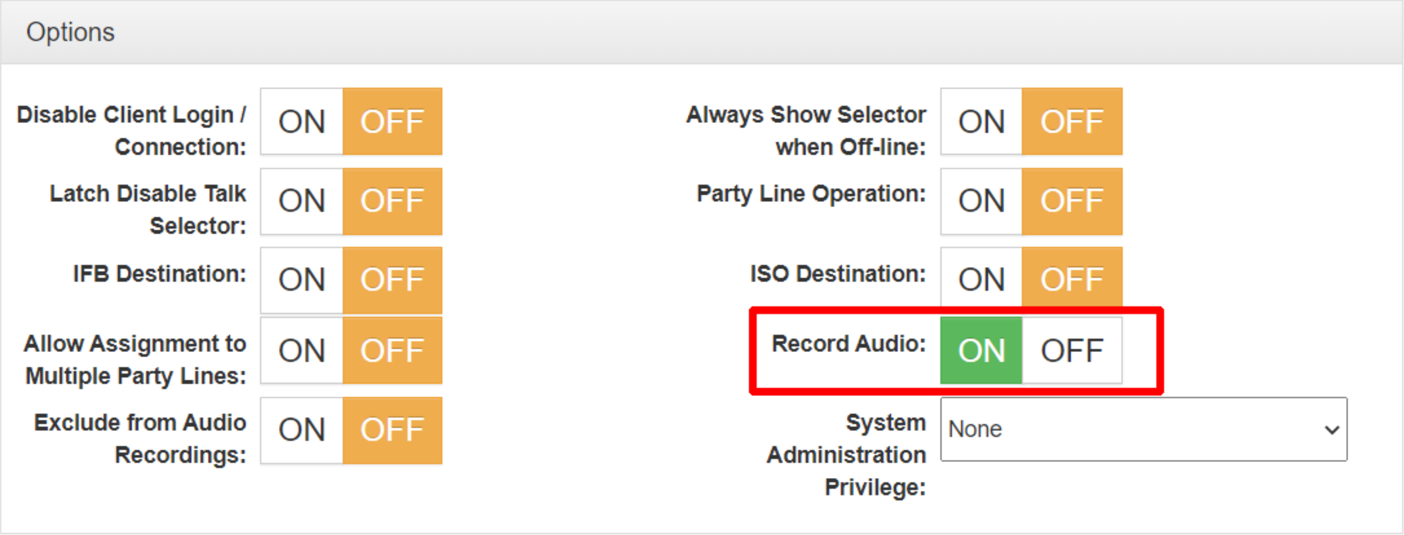
13.3 Enable Audio Recording

From the System Configuration menu select Client Configuration.



	Type	Talk/Listen Name	Listen Only Name	Login Name	Login Password	Description
	filter	filter	filter	filter	filter	filter
VCP	Windows Desktop	Audio Recording Test		Audio Recordin…		
VCP	Windows Desktop	Barry		bdriver	BDRIVER	Barry Driver

Select the client that you want to enable audio recording for and click the Edit button.



Options

Disable Client Login / Connection:	ON [✓ OFF]	Always Show Selector when Off-line:	ON [✓ OFF]
Latch Disable Talk Selector:	ON [✓ OFF]	Party Line Operation:	ON [✓ OFF]
IFB Destination:	ON [✓ OFF]	ISO Destination:	ON [✓ OFF]
Allow Assignment to Multiple Party Lines:	ON [✓ OFF]	Record Audio:	[✓ ON] OFF
Exclude from Audio Recordings:	ON [✓ OFF]	System Administration Privilege:	None

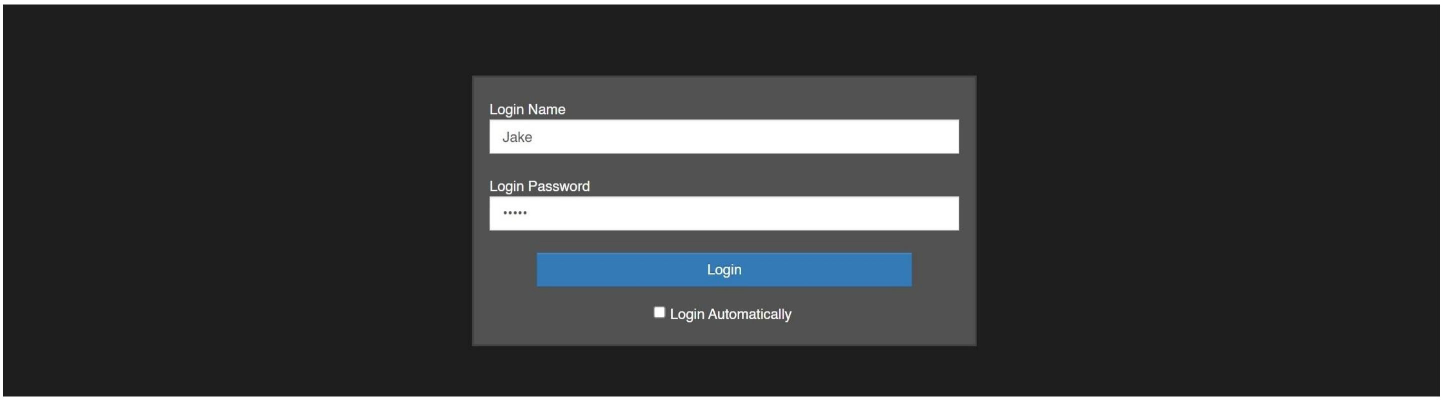
Scroll down to the Options menu and turn on the Record Audio option. Click the save button at the bottom of the menu. All audio going to and coming from the client will be recorded.

Note: The Exclude from Audio Recordings option allows a client to be excluded from recording such as a program feed so that if one is recording a client that is listening to the program feed it will record every else except the program feed.

14. VCOM WebRTC Control Panel

Logging In

To access the VCOM WebRTC Control Panel open a web browser (Google Chrome is recommended) and enter the IP address or domain name of the VCOM Virtual Matrix server. There are also VCOM WebRTC Control Panel apps available for all major platforms. If you are using the app, enter the IP address or domain name of the VCOM Virtual Matrix in the Virtual Matrix Hostname field.



Login Name: Jake

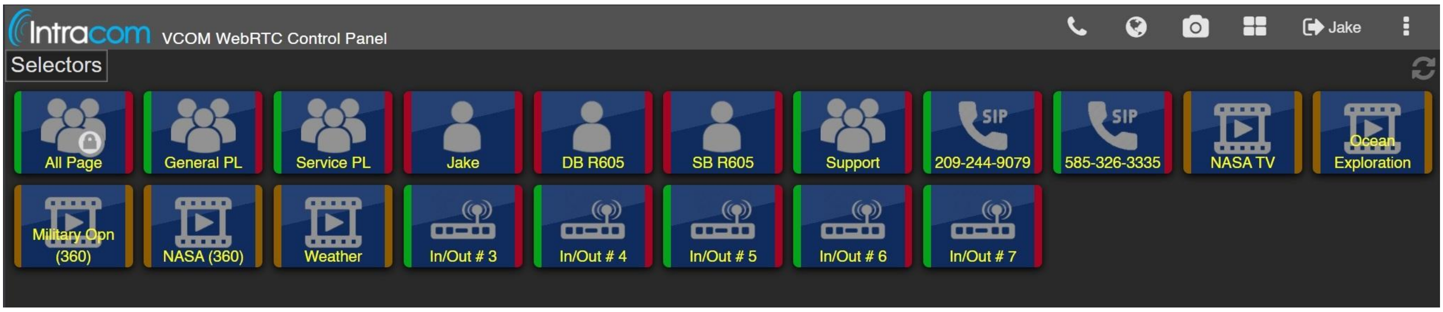
Login Password: •••••

Login

□ Login Automatically

VCOM comes with 20 guest logins in the default configuration. Anything can be entered into the Login Name field as long as the Login Password "guest" is used. Custom logins can be made using the VCOM System Administrator.

Control Panel

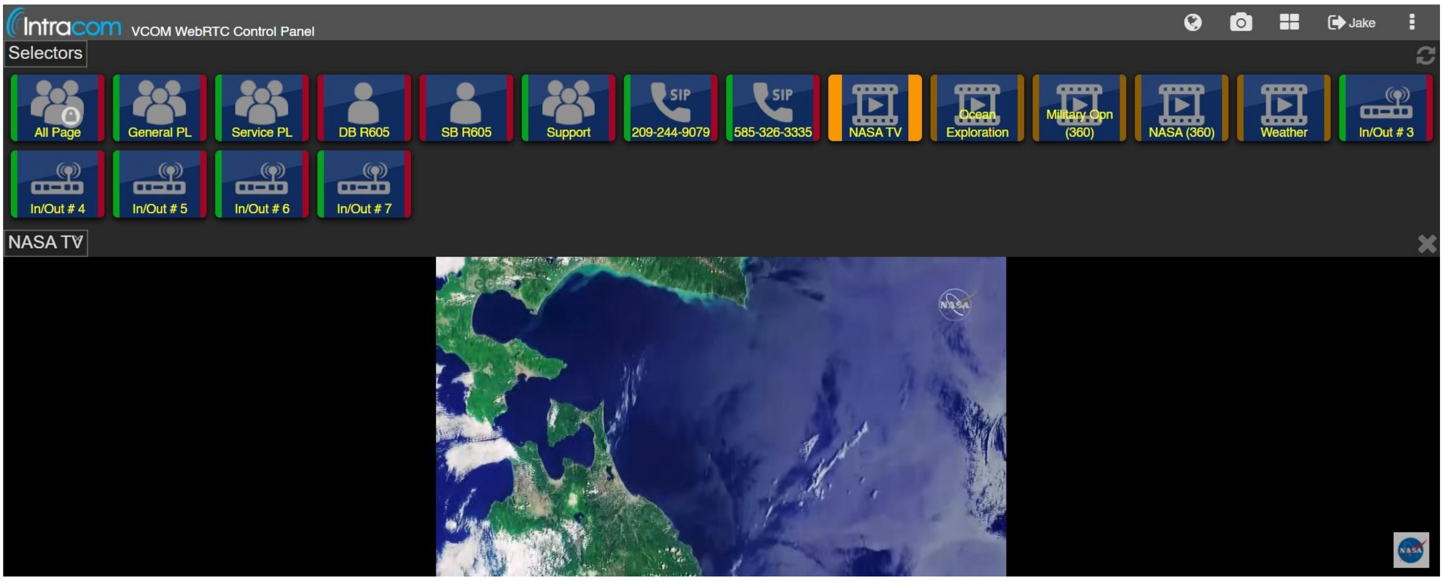


The Control Panel provides a series of buttons referred to as Talk and Listen selectors. An available Talk selector is red and an available Listen selector is green. Some selectors provide for dual Talk/Listen selector operation. If a selector is grayed out, this indicates that the source or destination is not connected to the system and not available for selecting a talk or listen. To activate a Listen to a particular source tap a green selector. When active the selector will be white. To deactivate a listen to a particular source tap the selector again. To activate a Talk to a particular destination tap a red selector. To deactivate a talk to a particular source tap the selector again. To use a selector in momentary mode tap and hold the selector; it will deactivate when you release.

Selectors display channel state using the following patterns: Voice activity: Color oscillation of selector background Incoming call: Fast flash of talk selector

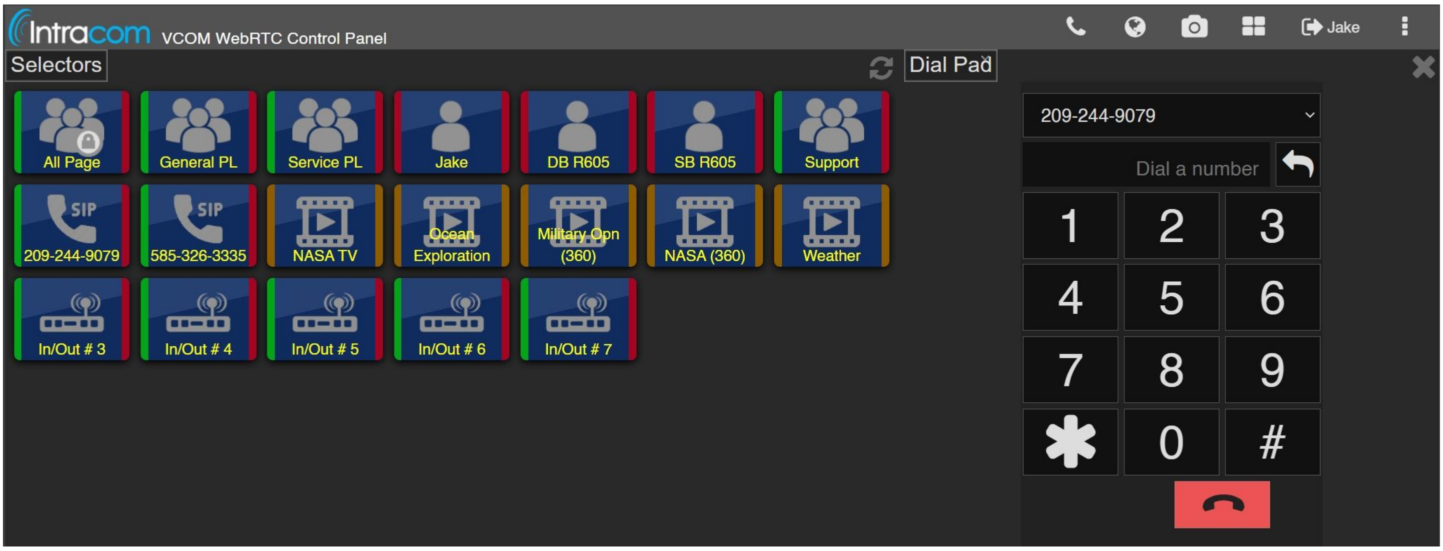
A selector can refer to either an individual source or destination or to a Group Call or Party Line. A Group Call is a single selector that activates a Talk and Listen to multiple destinations. A Party Line is a dynamic conference whereby activation of the associated selector automatically makes you a participant of the selected conference. When talking to a Party Line you talk to everyone who is listening to that Party Line. When listening to a Party Line, you listen to everyone who is talking to that Party Line.

Video Selectors



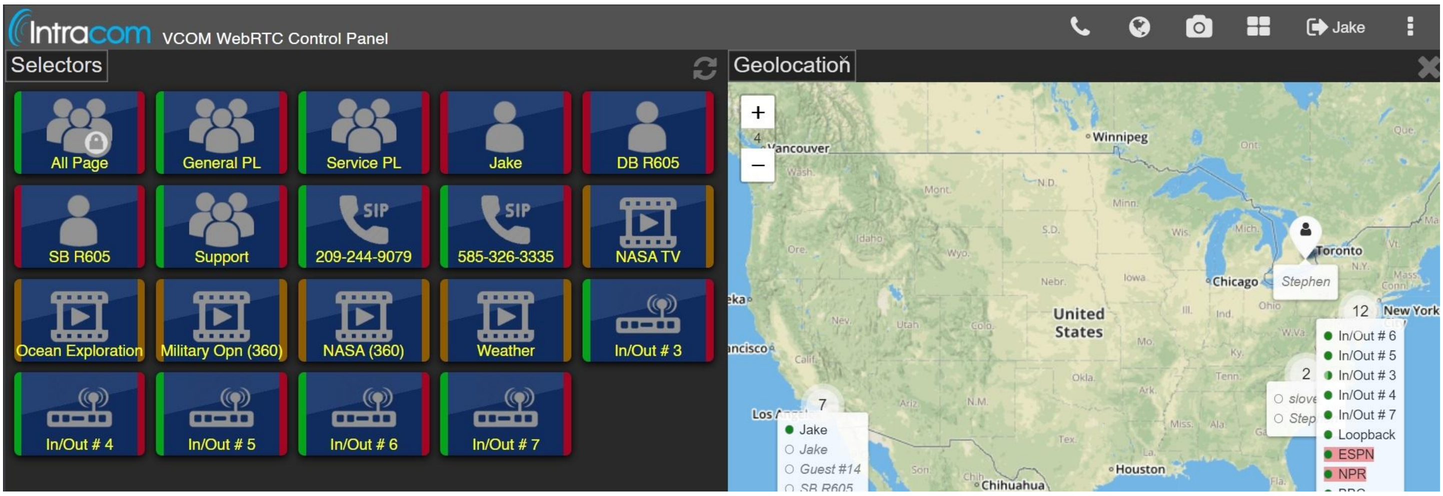
Clicking on an orange selector will display its corresponding video.

Dialpad



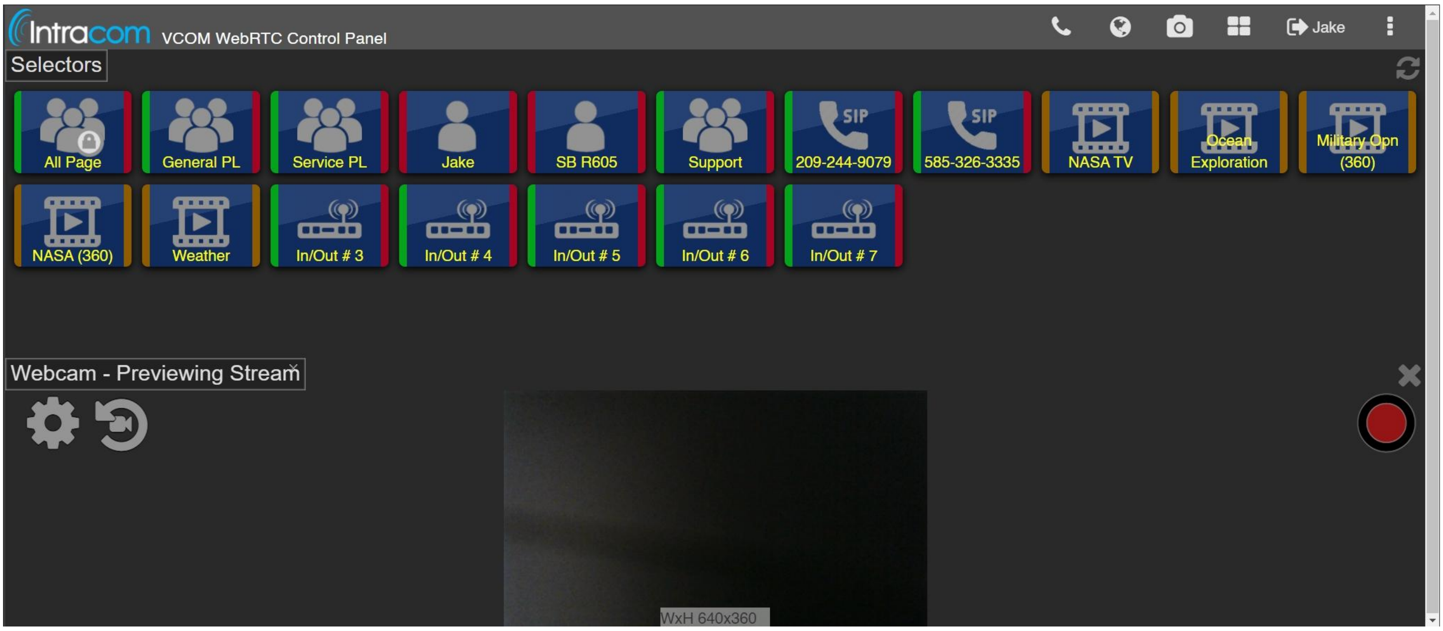
If the Client is configured in the System Administration with the "Enable Dial Pad Buttons" option set to On and has a SIP line as one of its selectors then a handset icon will be shown in the top bar. Pressing this button will display a dialpad from which phone numbers can be called.

Geolocation

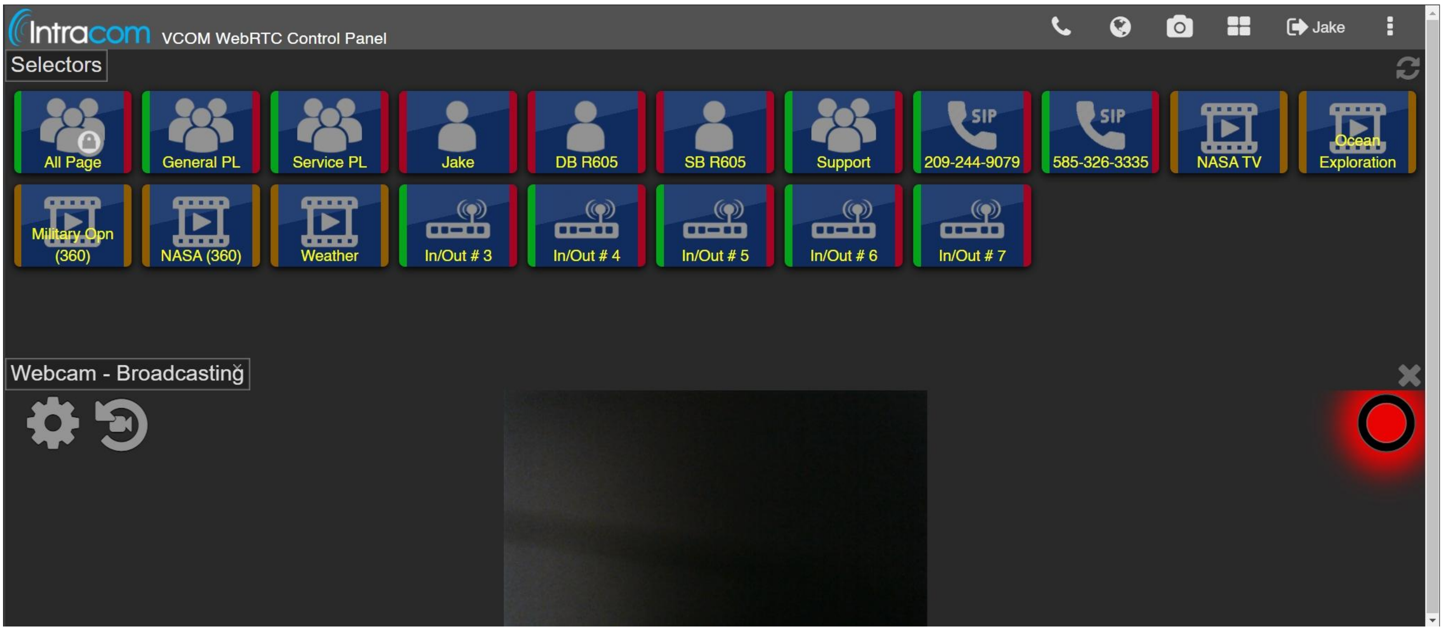


If the Client is configured in the System Administration with the "Enable Geolocation Button" set to On then a globe icon will be shown in the top bar. Pressing this button will display a global-scale map with other users appearing as pin-points beside their name along with longitude/latitude coordinates.

Video Streaming



If VCOM is licensed for video streaming and a Media Server has been provisioned and connected via the System Administration then a camera icon will be shown in the top bar. Pressing this button will open a preview of your webcam.



Press the red button to being streaming. Other clients will be able to view the stream.

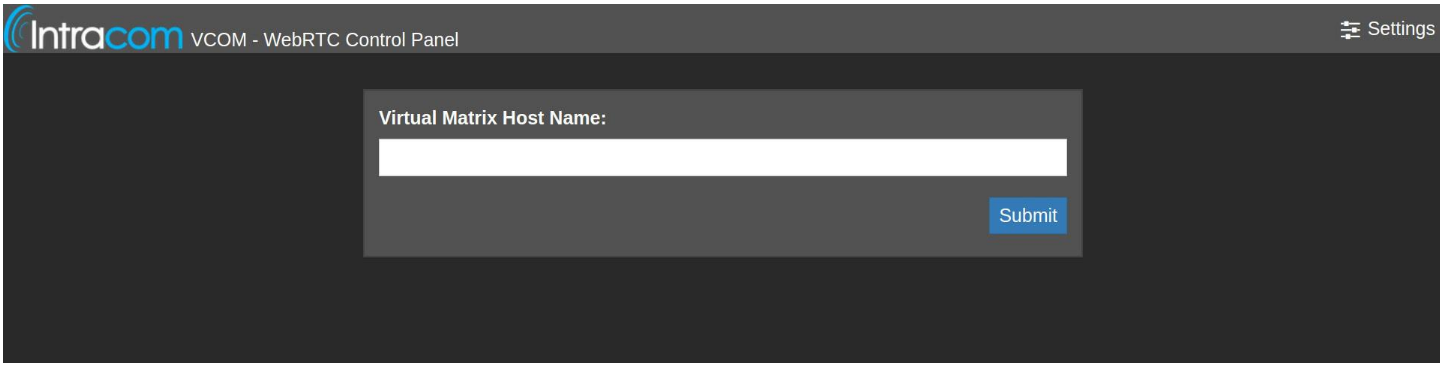
15. Hardware Control Panels

15.1 Network Requirements

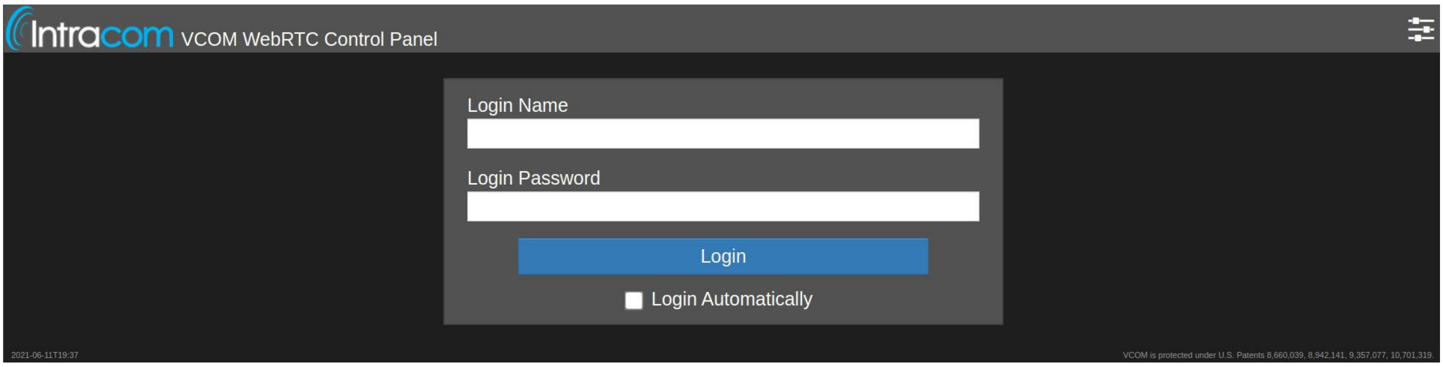
The Control Panel requires a 200 Kbps network connection or greater for basic talk/listen functionality. The following ports should be open between the server and the Control Panel.

Port	TCP/UDP	Description
80	TCP	System Administration and WebRTC Control Panel data (Unsecure)
443	TCP	System Administration and WebRTC Control Panel data (Secure)
81	TCP	WebRTC Control Panel Signaling data (Unsecure)
444	TCP	WebRTC Control Panel Signaling data (Secure)
49152 to 65535	UDP	WebRTC Control Panel audio
8888	TCP/UDP	(Optional) Media Server

15.2 Log In and Basic Usage


Intracom VCOM - WebRTC Control Panel
Settings
Virtual Matrix Host Name:
Submit

Upon turning on the Control Panel you will see the above screen. The Virtual Matrix Host Name is the domain name or IP address of the server that is running VCOM Virtual Matrix. Tap the field to enter the host name and then press submit. The configuration will be saved and will not have to be entered again.



Intracom VCOM WebRTC Control Panel

Login Name

Login Password

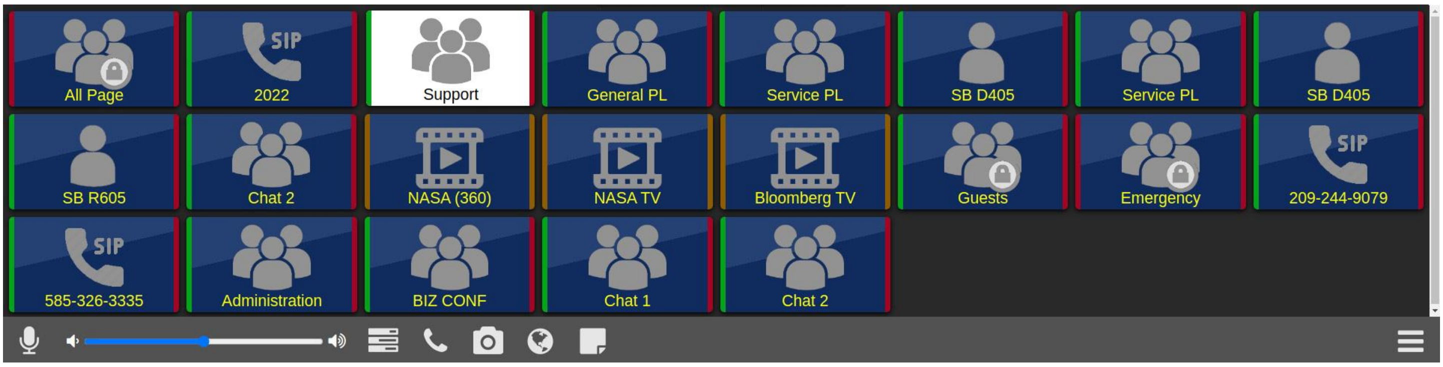
Login

□ Login Automatically

2021-06-11T19:37

VCOM is protected under U.S. Patents 8,660,039, 8,942,141, 9,357,077, 10,701,319.

Enter you Login Name and Login Password and then press Login. For information on how to create logins please refer to the VCOM System Administration documentation.



Selectors

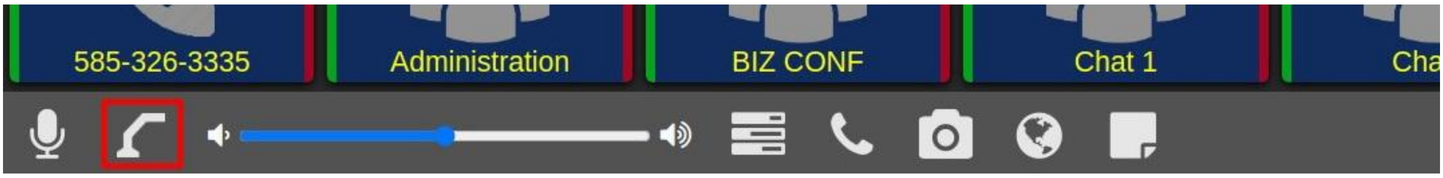
The Control Panel provides a series of buttons referred to as Talk and Listen selectors. An available Talk selector is red and an available Listen selector is green. Some selectors provide for dual Talk/Listen selector operation. If a selector is grayed out, this indicates that the source or destination is not connected to the system and not available for selecting a talk or listen. To activate a Listen to a particular source tap a green selector. When active the selector will be white. To deactivate a listen to a particular source tap the selector again. To activate a Talk to a particular destination tap a red selector. To deactivate a talk to a particular source tap the selector again. To use a selector in momentary mode tap and hold the selector; it will deactivate when you release.

Selectors display channel state using the following patterns:
Voice activity: Color oscillation of selector background
Incoming call: Fast flash of talk selector

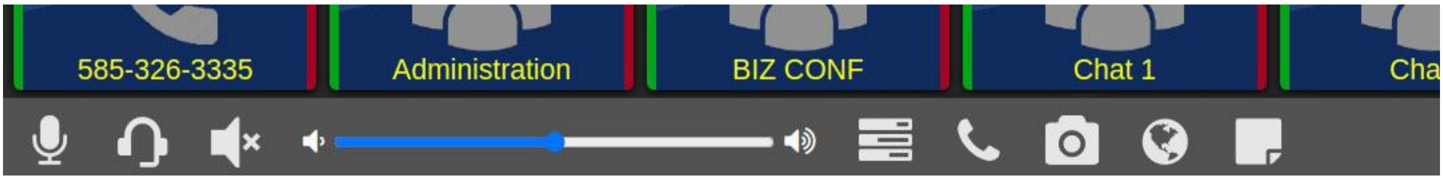
A selector can refer to either an individual source or destination or to a Group Call or Party Line. A Group Call is a single selector that activates a Talk and Listen to multiple destinations. A Party Line is a dynamic conference whereby activation of the associated selector automatically makes you a participant of the selected conference. When talking to a Party Line you talk to everyone who is listening to that Party Line. When listening to a Party Line, you listen to everyone who is talking to that Party Line.

Controls
The bar at the bottom of the screen includes a variety of audio controls as well as options to open a the dialpad, geolocation window, etc. depending on how the system is configured.

15.3 Headsets



The Control Panel has support for USB headsets. After plugging in a headset, a new button showing a gooseneck mic will appear towards the bottom of the screen. This icon indicates that the internal mic/speaker is being used. To begin using the headset, tap the button.



A headset icon will now be displayed to indicate that the headset is being used. Additionally, a speaker button will appear. The speaker button enables/disables the internal speaker.

16. VCOM Interoperability with Simple Network Management Protocol (SNMP)

16.1 Installation

Prior to installing the VCOM Virtual Matrix it is important to ensure that the Microsoft SNMP Service is installed. If installed, a running service called 'SNMP Service' can be found in the Services dialog. If SNMP Services are not installed, follow the directions here to install it.

From the Services Dialog, With the 'SNMP service' running, right click on the SNMP Service Configuration and select the 'Security' tab and ensure an Accepted Community is defined to with a name of 'Public' and the rights of Read-Only. Next select the 'Traps' tab. In this dialog, enter the IP address of the SNMP Monitoring tool that will be receiving the SNMP Trap messages.

With the SNMP services enabled, the installation process of the VCOM Virtual Matrix will automatically install and configure VCOM SNMP Agent for use by the SNMP Service.

Lastly, the provided MIB file may be added to the SNMP Monitoring Tool environment. In some cases, the SNMP Monitoring Tool must be configured with the IP address of the source of the incoming SNMP messages which would be the address(es) of the VCOM Virtual Matrix (both Primary and Secondary).

16.2 Operation

The SNMP implementation is limited only to the generation of SNMP Trap messages. There is no VCOM configuration required for the SNMP as the system will always generate the SNMP Trap messages for specific events if SNMP is installed and licensed. The SNMP Trap messages that are supported are:

- VDI/SIP Client Disconnect - An SNMP Trap will be generated for every VCOM Device Interface or SIP Client disconnect. The VDI and SIP Clients generally support critical system functionality and their disconnect is considered an event that should be investigated. The SNMP Trap message includes the VCOM Talk/Listen Selector Name of the VDI/SIP client that disconnected

- Failover Status Change - An SNMP Trap will be generated for every change in the Failover Status. In normal operation there should be no changes in the Failover state and as such any change is considered an event that should be noted. The most significant events that require investigation are any events that indicate that Secondary server or Primary server have gone offline.

16.3 SNMP TRAP Message Detail

MIB Object Identifier	Message Function	Data Type (bytes)	Data Length	Data Description
1.3.6.1.4.1.41961.0.0.2	VDI/SIP Client Disconnect	Octet String	variable	Selector Name as configured in VVM
1.3.6.1.4.1.41961.0.0.3	Failover Status Change	Integer	4	0 - Failover is not licensed 1 - Failover is not configured 2 - Primary server is active, Failover server is offline 3 - Primary server is active, Failover server is ready 4 - Failover server is active, Primary server is offline 5 - Failover server is active, Primary server is ready

16.4 Control Rooms

Introduction
For businesses leveraging the VCOM SIP/TIF system, visibility into the operational state of numerous connected phone lines is crucial. These organizations prioritize the ability to monitor line statuses in real-time, aiming to enhance awareness of which lines are actively in use.

Screenshot of the vcom tif

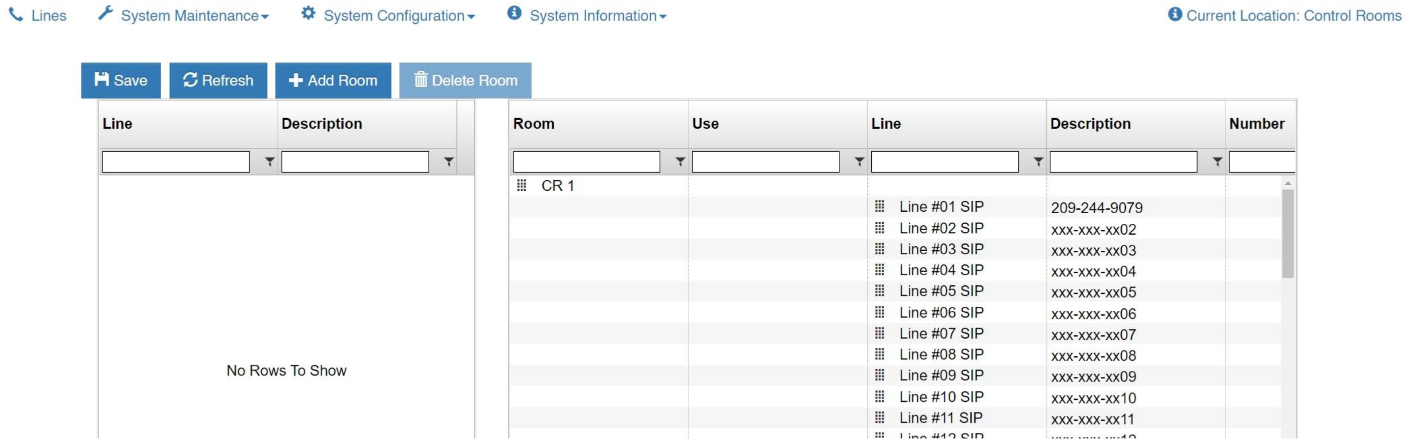
Introducing the VCOM Control Rooms feature, designed to simplify your communication network. This innovative solution allows you to organize multiple phone lines into designated "rooms," each customizable with its unique name. This organization method transforms how you manage your lines, making it easier to oversee and control your communication infrastructure effectively.

Screenshot of a vcom control room menu

Experience unmatched monitoring ease with the VCOM WebRTC Control Panel. Each room, organized into tabs, offers a streamlined view of your phone lines, allowing for quick access and real-time monitoring. This intuitive interface ensures that every call is managed efficiently, providing you with the control you need to maintain superior communication standards.

To utilize the Control Rooms feature, users must first access the VCOM WebRTC Control Panel. This requires an available Control Panel port on the system. It's important to note that VCOM SIP/TIF systems typically do not include Control Panel ports in their default licensing. As such, most customers will need to acquire additional ports to leverage the Control Rooms functionality.

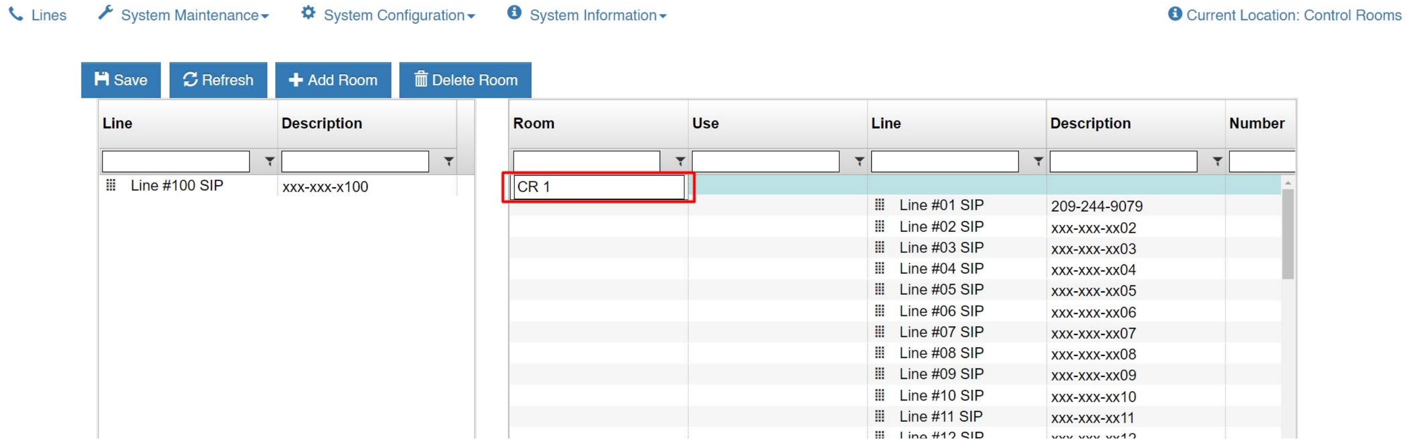
Creating the Control Room



Line	Description
No Rows To Show	

Room	Use	Line	Description	Number
CR 1				
		Line #01 SIP	209-244-9079	
		Line #02 SIP	xxx-xxx-xx02	
		Line #03 SIP	xxx-xxx-xx03	
		Line #04 SIP	xxx-xxx-xx04	
		Line #05 SIP	xxx-xxx-xx05	
		Line #06 SIP	xxx-xxx-xx06	
		Line #07 SIP	xxx-xxx-xx07	
		Line #08 SIP	xxx-xxx-xx08	
		Line #09 SIP	xxx-xxx-xx09	
		Line #10 SIP	xxx-xxx-xx10	
		Line #11 SIP	xxx-xxx-xx11	
		Line #12 SIP	xxx-xxx-xx12	

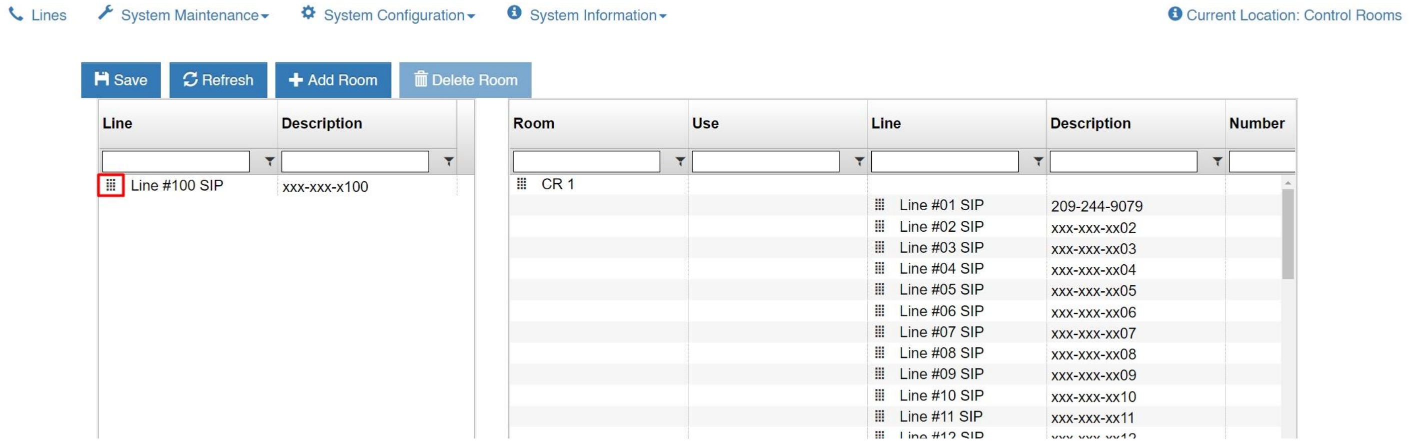
Click the Add Room button to create a new Control Room.



Line	Description
Line #100 SIP	xxx-xxx-x100

Room	Use	Line	Description	Number
CR 1				
		Line #01 SIP	209-244-9079	
		Line #02 SIP	xxx-xxx-xx02	
		Line #03 SIP	xxx-xxx-xx03	
		Line #04 SIP	xxx-xxx-xx04	
		Line #05 SIP	xxx-xxx-xx05	
		Line #06 SIP	xxx-xxx-xx06	
		Line #07 SIP	xxx-xxx-xx07	
		Line #08 SIP	xxx-xxx-xx08	
		Line #09 SIP	xxx-xxx-xx09	
		Line #10 SIP	xxx-xxx-xx10	
		Line #11 SIP	xxx-xxx-xx11	
		Line #12 SIP	xxx-xxx-xx12	

Double click the name of the Control Room to edit its name.

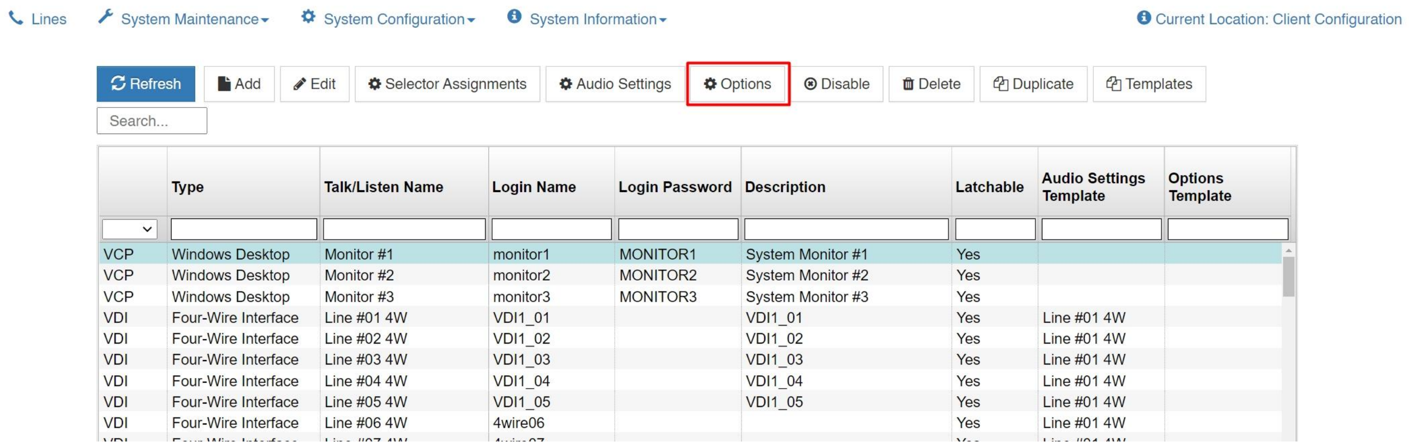


Line	Description
Line #100 SIP	xxx-xxx-x100

Room	Use	Line	Description	Number
CR 1				
		Line #01 SIP	209-244-9079	
		Line #02 SIP	xxx-xxx-xx02	
		Line #03 SIP	xxx-xxx-xx03	
		Line #04 SIP	xxx-xxx-xx04	
		Line #05 SIP	xxx-xxx-xx05	
		Line #06 SIP	xxx-xxx-xx06	
		Line #07 SIP	xxx-xxx-xx07	
		Line #08 SIP	xxx-xxx-xx08	
		Line #09 SIP	xxx-xxx-xx09	
		Line #10 SIP	xxx-xxx-xx10	
		Line #11 SIP	xxx-xxx-xx11	
		Line #12 SIP	xxx-xxx-xx12	

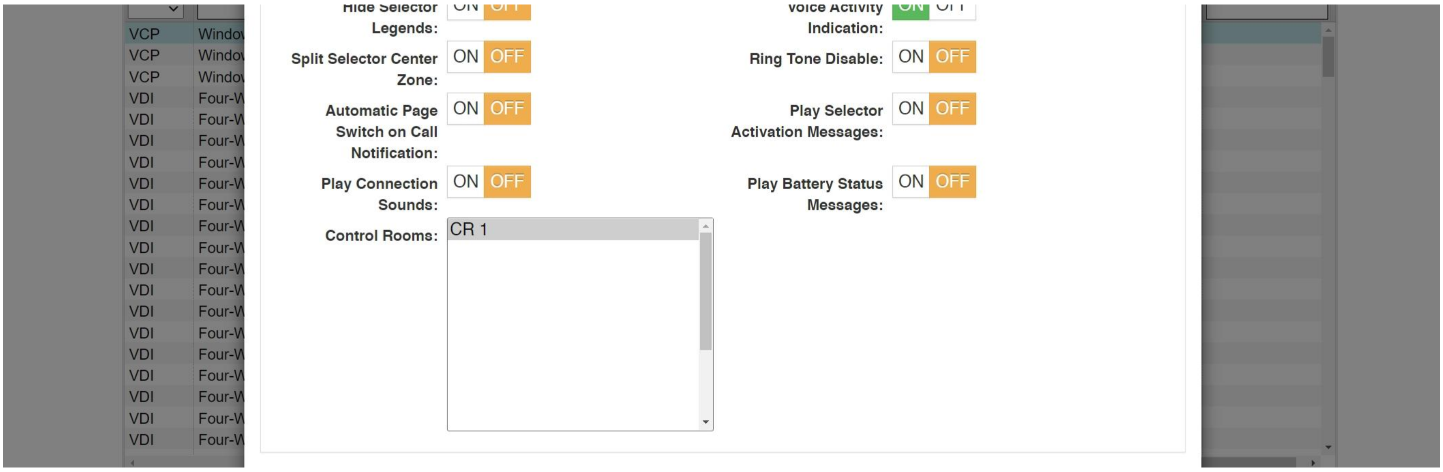
Drag a SIP line from the left side of the screen over the name of the Control Room to assign it to the room.

Assigning and Viewing the Control Room



	Type	Talk/Listen Name	Login Name	Login Password	Description	Latchable	Audio Settings Template	Options Template
VCP	Windows Desktop	Monitor #1	monitor1	MONITOR1	System Monitor #1	Yes		
VCP	Windows Desktop	Monitor #2	monitor2	MONITOR2	System Monitor #2	Yes		
VCP	Windows Desktop	Monitor #3	monitor3	MONITOR3	System Monitor #3	Yes		
VDI	Four-Wire Interface	Line #01 4W	VDI1_01		VDI1_01	Yes	Line #01 4W	
VDI	Four-Wire Interface	Line #02 4W	VDI1_02		VDI1_02	Yes	Line #01 4W	
VDI	Four-Wire Interface	Line #03 4W	VDI1_03		VDI1_03	Yes	Line #01 4W	
VDI	Four-Wire Interface	Line #04 4W	VDI1_04		VDI1_04	Yes	Line #01 4W	
VDI	Four-Wire Interface	Line #05 4W	VDI1_05		VDI1_05	Yes	Line #01 4W	
VDI	Four-Wire Interface	Line #06 4W	4wire06			Yes	Line #01 4W	

From the System Configuration dropdown select Client Configuration. Select the client that you want to be able to view the room and then click the Options button.



Hide Selector Legends: ON OFF

Voice Activity Indication: ON OFF

Split Selector Center Zone: ON OFF

Ring Tone Disable: ON OFF

Automatic Page Switch on Call Notification: ON OFF

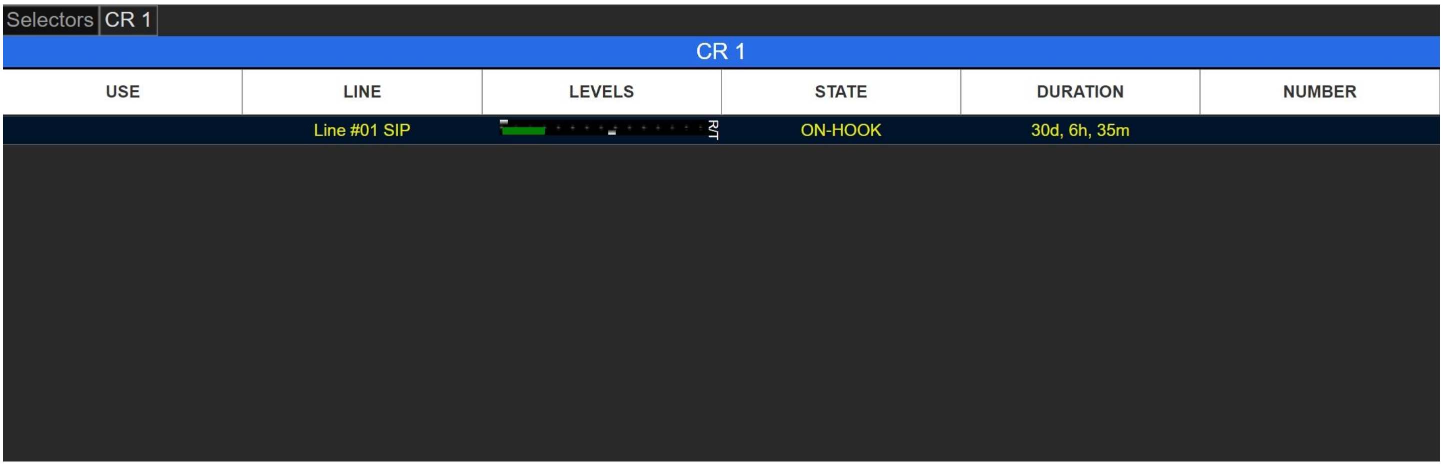
Play Selector Activation Messages: ON OFF

Play Connection Sounds: ON OFF

Play Battery Status Messages: ON OFF

Control Rooms: CR 1

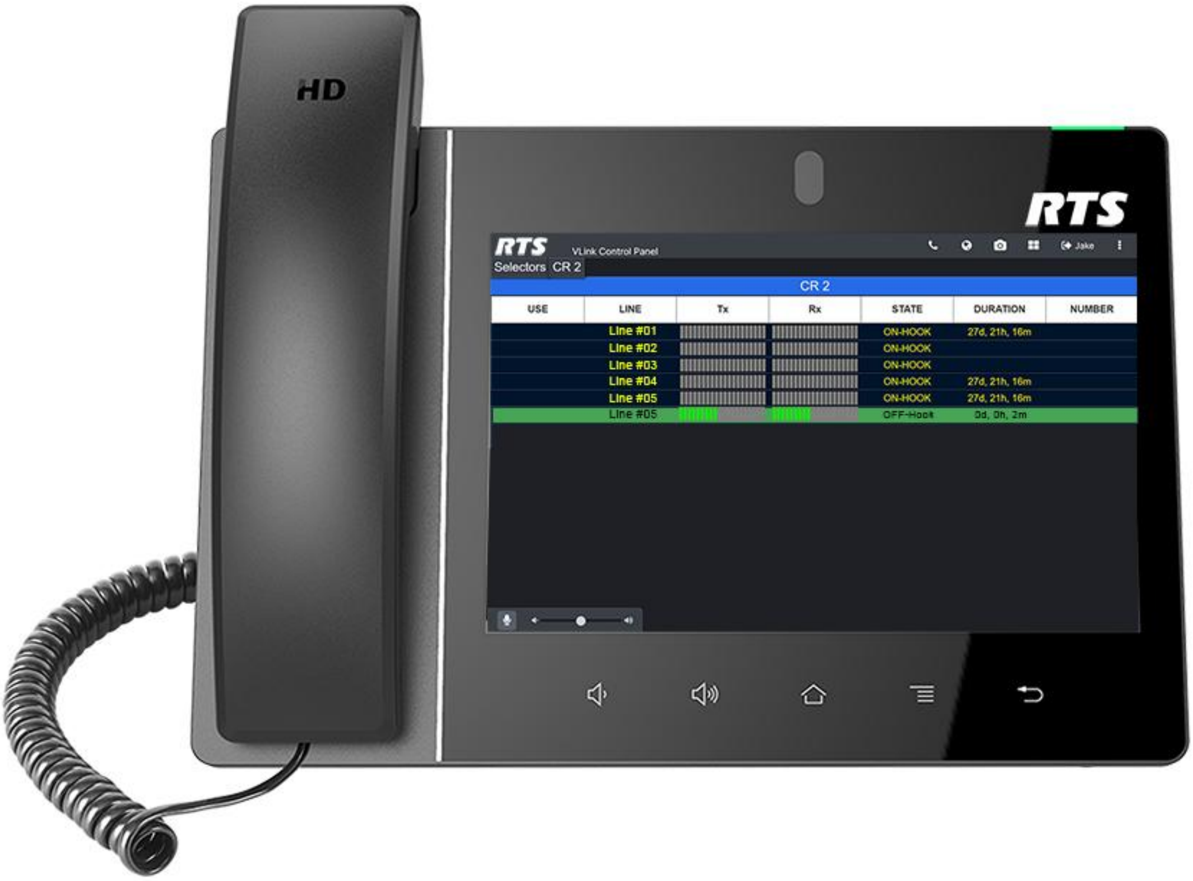
From the Control Rooms list select the room(s) that you want the client to be able to access then click the Save button.



CR 1

USE	LINE	LEVELS	STATE	DURATION	NUMBER
	Line #01 SIP	R/T	ON-HOOK	30d, 6h, 35m	

Control Rooms can be monitored from the VCOM WebRTC Control Panel on your smartphone or computer. To view the room, log in and select the desired room's tab.



CR 2

USE	LINE	Tx	Rx	STATE	DURATION	NUMBER
	Line #01			ON-HOOK	27d, 21h, 16m	
	Line #02			ON-HOOK		
	Line #03			ON-HOOK		
	Line #04			ON-HOOK	27d, 21h, 16m	
	Line #05			ON-HOOK	27d, 21h, 16m	
	Line #05			OFF-Hook	0d, 0h, 2m	

Control Rooms can also be monitored on Comscreen hardphones.