VLink Virtual Matrix

Documentation for VLink Virtual Matrix

Bosch Security Systems

Copyright Bosch Security Systems

Table of contents

1. Installation 5
    1.1 Hardware Requirements 5
    1.2 Network Requirements 7
    1.3 WebRTC Audio Connection 10
    1.4 Software Installation 11
    1.5 Licensing 11
    1.6 SSL Introduction 13
    1.7 SSL (CA Certificate) 14
    1.8 SSL (Self-Signed Certificate) 17
2. AWS Installation 18
    2.1 AWS Security Group (firewall) Configuration 19
    2.2 Static IP Address Configuration (recommended) 21
    2.3 Connecting to the EC2 Instance 23
    2.4 Configuring the EC2 Instance 25
3. Azure Installation 28
    3.1 Firewall Configuration 29
    3.2 Connecting to the server instance 30
    3.3 Configuring the server instance 30
4. VLink TIF 33
    4.1 Introduction 33
    4.2 Phone Switch SIP Line Planning 33
    4.3 Phone Switch / PBX Connect Method 33
    4.4 IP Network Considerations 34
    4.5 Dante Virtual Soundcard (DVS) 34
    4.6 RTS Intercom Port Planning 35
    4.7 VLink Configuration 36
    4.8 Internal server Dante Virtual Soundcard Channel Connections 38

Copyright Bosch Security Systems

4.9 Setup of Audio Channels Between VLink and Omneo Cards 39
4.10 Intercom Port to SIP Line Association 42
4.11 Testing 45
5. TURN Server Provisioning 49
5.1 Minimum Server Requirements 49
5.2 Software Installation 49
6. Video Media Server 51
6.1 Installation 51
6.2 STUN Server 52
6.3 Configuration 52
7. System Administration 53
7.1 Logging In 53
7.2 System Status 54
7.3 System Maintenance 56
7.4 System Configuration 58
7.5 Client Configuration 63
7.6 System Information 79
8. Failover Capability 81
8.1 Implementation 81
8.2 Failover Criteria 82
8.3 Other Considerations 82
8.4 Setup 83
9. Connecting SIP Lines 84
10. Connecting AWS Chime SIP Lines 88
10.1 AWS Settings 88
10.2 VLink Settings 92
11. Connecting NDI Audio Streams 94
12. VLink Device Interface 95
12.1 Installation 95
12.2 Configuration 96

Copyright Bosch Security Systems

12.3 Operation 98

12.4 Troubleshooting 98

13. Audio Recording 100

13.1 File-based Audio Recording 100

13.2 SIPREC Audio Recording 101

13.3 Enable Audio Recording 101

14. VLink WebRTC Control Panel 103

15. VLink Interoperability with Simple Network Management Protocol (SNMP) 107

15.1 Installation 107

15.2 Operation 107

15.3 SNMP TRAP Message Detail 108

15.4 Control Rooms 109

Copyright Bosch Security Systems

1. Installation

1.1 Hardware Requirements

Operating System Requirements
The VLink 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 VLink 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 VLink 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 VLink 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

Copyright Bosch Security Systems

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.

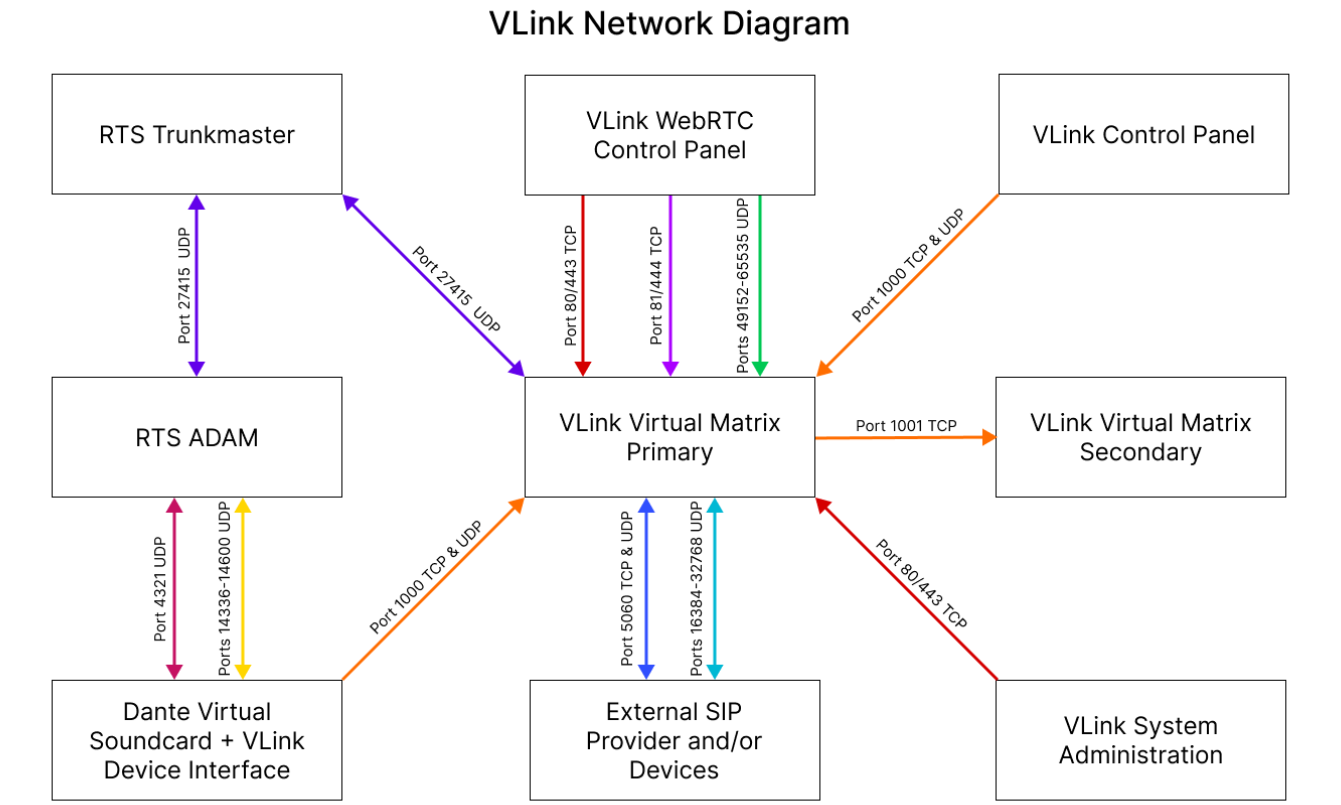
For reference, the standard server provided by RTS has an Intel Core i7-8700 with 12 cores and a PassMark benchmark of 15222 or an average of 1268 per core. With the above recommendations, the server can support 600+ connections in a “Heavy” use configuration, 900+ connections in a “Moderate” configuration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

Copyright Bosch Security Systems

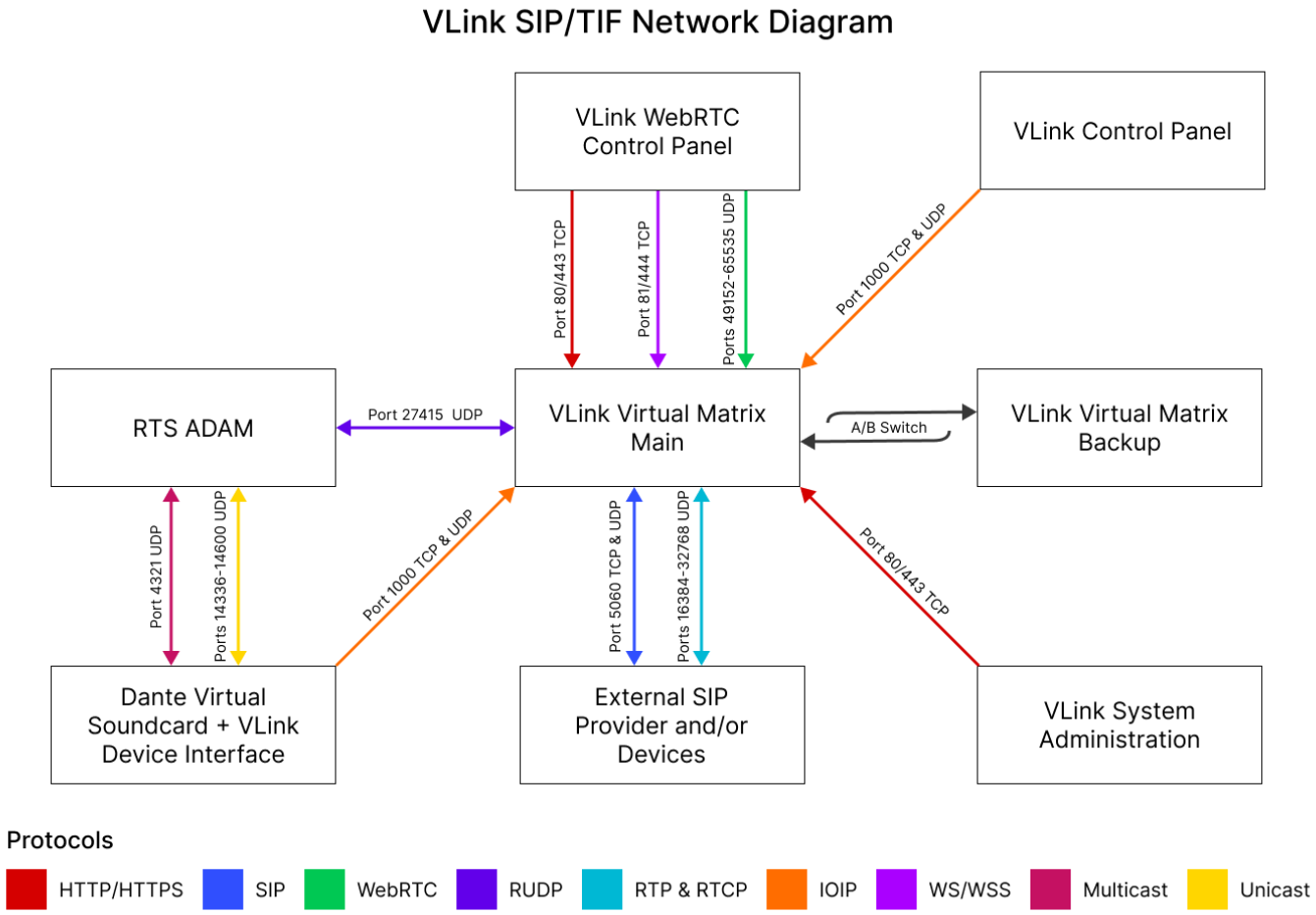
1.2 Network Requirements

Network Diagrams



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

Copyright Bosch Security Systems



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.

Copyright Bosch Security Systems

VLink Control Panel and VLink 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

VLink 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.

Copyright Bosch Security Systems

Firewall Requirements

VLink uses the below ports. It is only necessary to open the ports for the VLink features you use in the "Required for" column below. In VLink 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
27415	UDP (RUDP)	RTS Trunkmaster	Intelligent Trunking

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

Copyright Bosch Security Systems

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 a 3rd party partner. 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 VLink Virtual Matrix from our downloads page and unzip the installer.

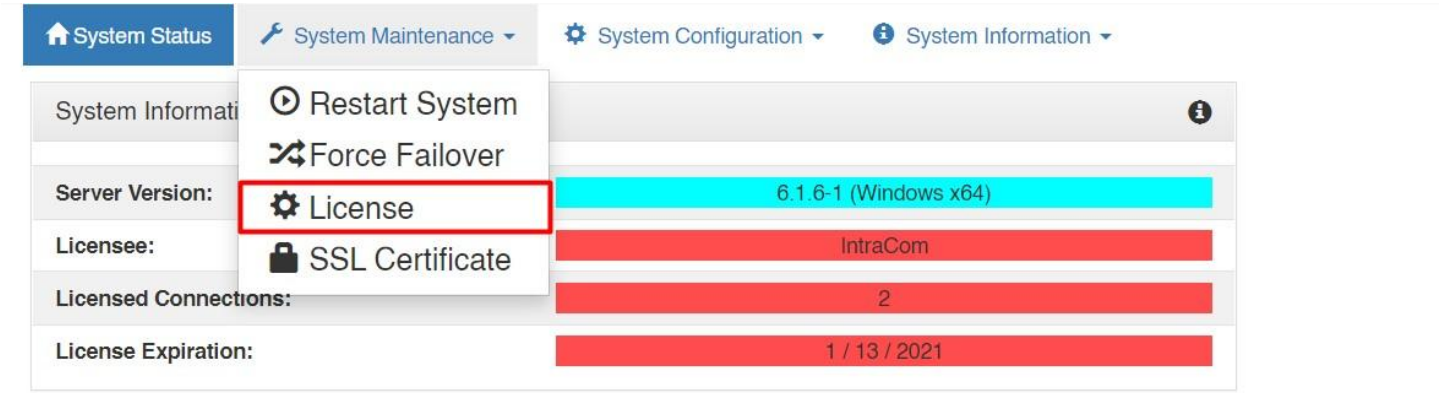
Run the installer and follow the prompts. You will need to accept RTS Systems’ License Agreement to install the software. During the installation process you will be asked if you want to install the VLink Virtual Matrix to run as a service or application. Servers should run VLink as a service.

To open the VLink Virtual Matrix once installed click on your VLink Virtual Matrix shortcut icon on your desktop or click on your start menu and select All Programs. Find RTS and select VLink Virtual Matrix.

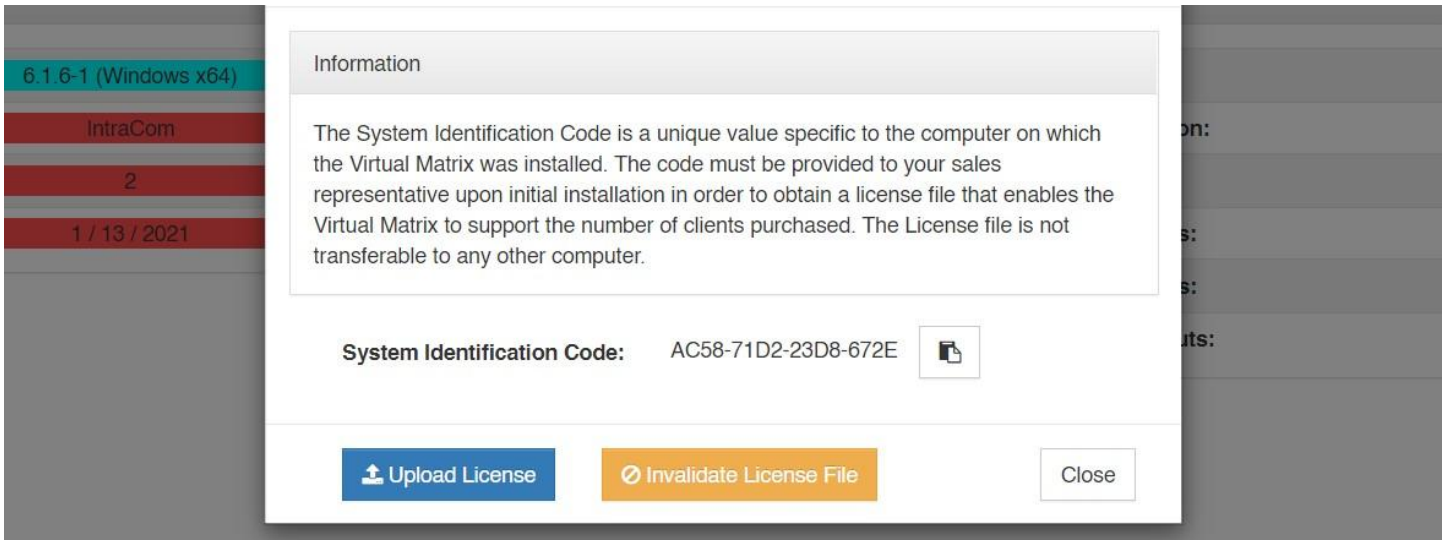
1.5 Licensing

To license your VLink System you need to acquire a valid license file from RTS. To do so you must provide RTS with your unique ‘System Identification Code’ generated automatically when you install the VLink 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 VLink 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.

Copyright Bosch Security Systems



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



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

Once the license file is installed, the VLink 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”.

Copyright Bosch Security Systems

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 VLink Virtual Matrix server and the VLink WebRTC Control Panel as well as the VLink System Administration. The VLink Virtual Matrix server will automatically generate a self-signed SSL certificate upon first launch.

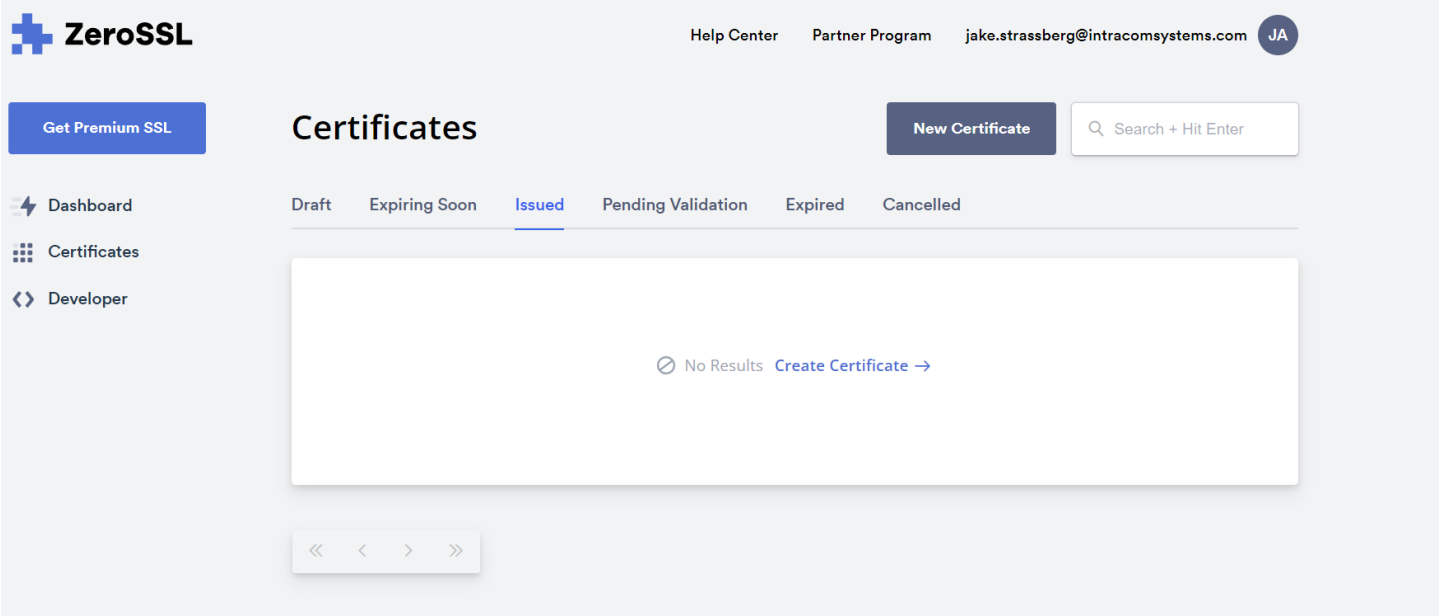
By default, browsers do not trust self-signed certificates. As such when you try to access the System Administration or WebRTC Control Panel through a browser you will likely see a warning message or be blocked entirely. Despite the warning message, your connection to VLink is still secure and encrypted. 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 VLink server. Organizations that generate their own certificates can do so and install the certification on VLink as they would with any other server. For organizations that do not have this capability, or for VLink servers that are cloud hosted, the guide below can be followed to generate and install a certificate authority signed certificate.

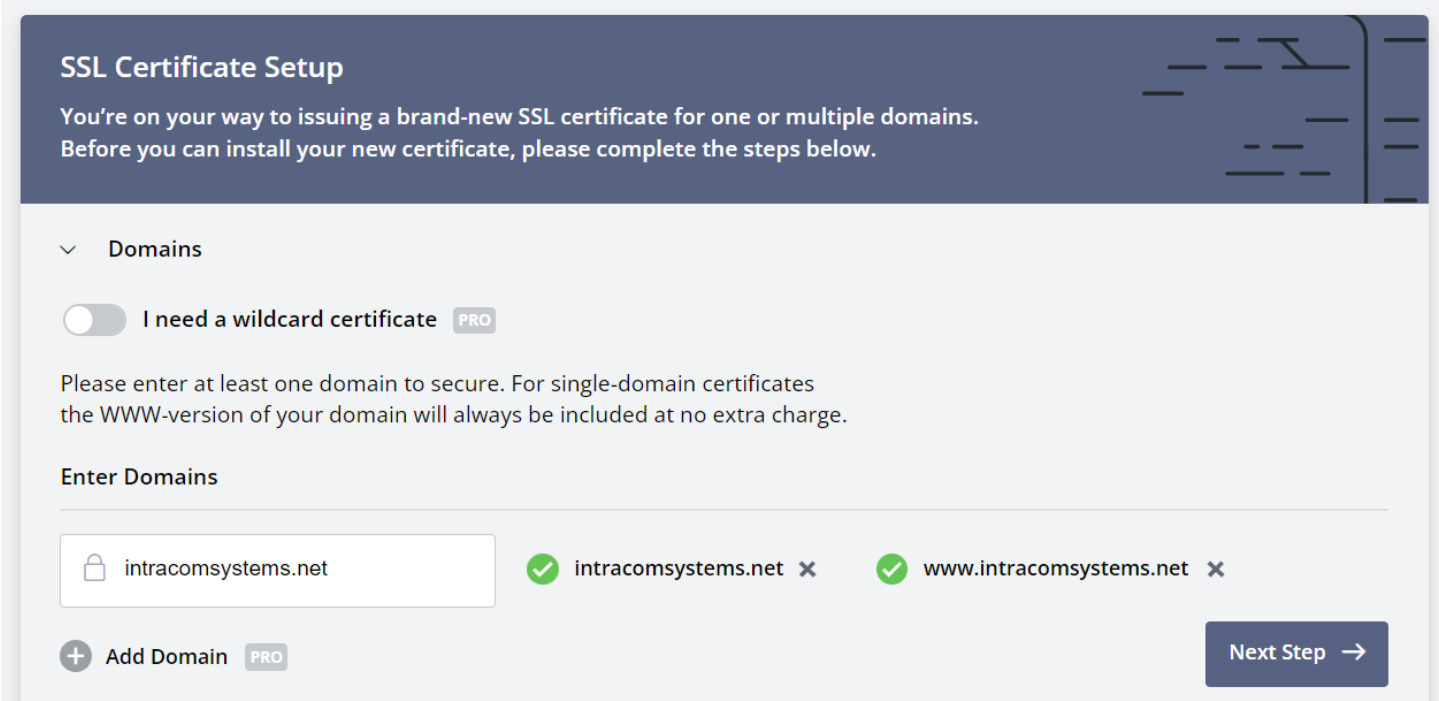
Copyright Bosch Security Systems

1.7 SSL (CA Certificate)

To generate a CA (Certificate Authority) SSL certificate a domain name must be registered for the server. Additionally, the VLink 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.

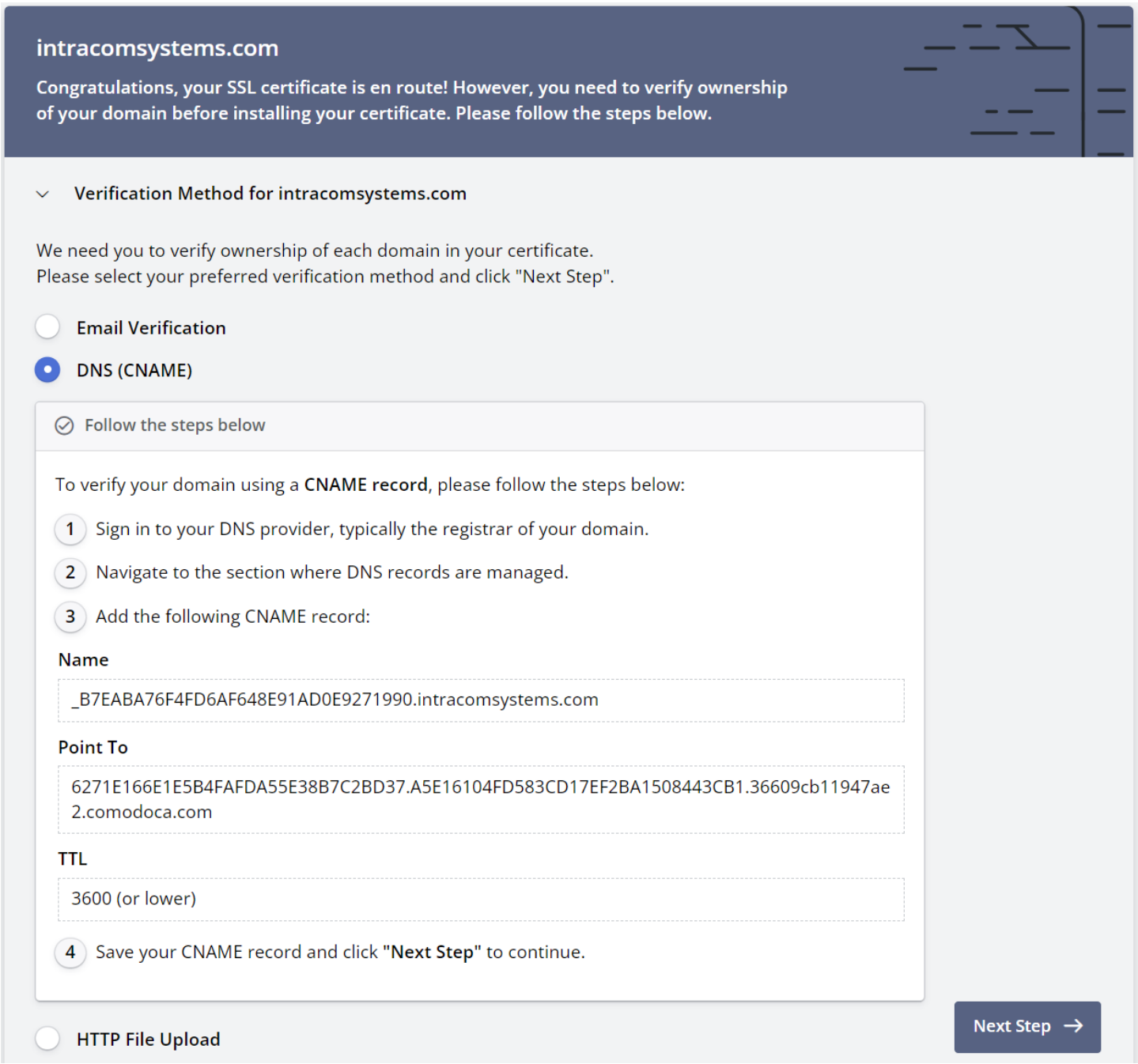


Make an account at zerossl.com then click Create Certificate.



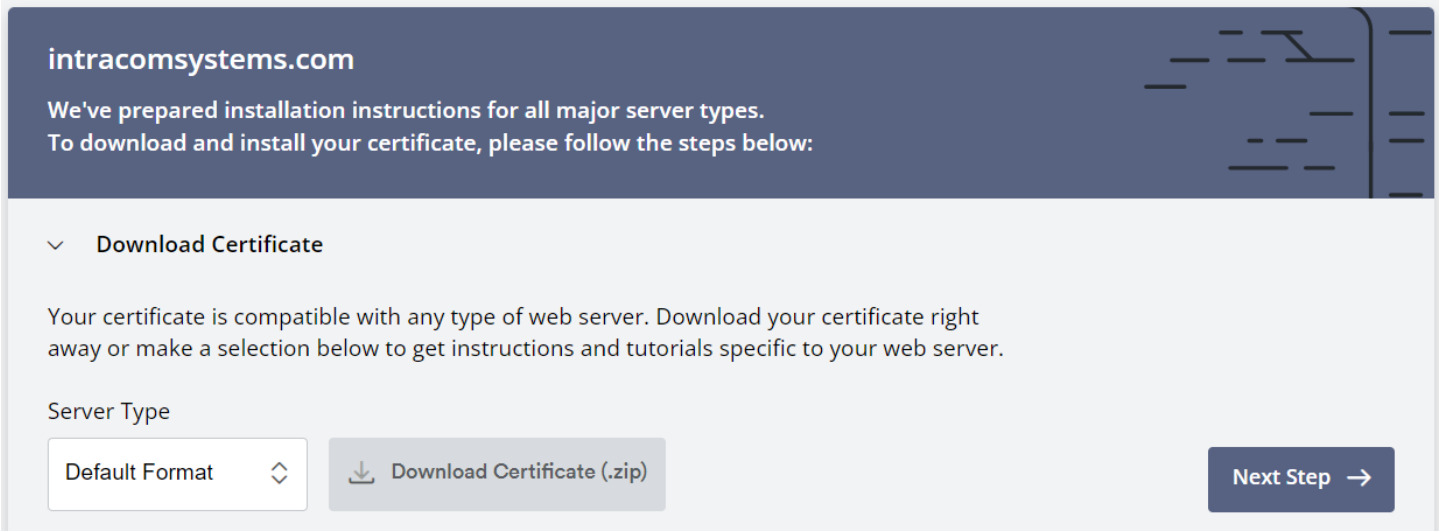
Copyright Bosch Security Systems

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

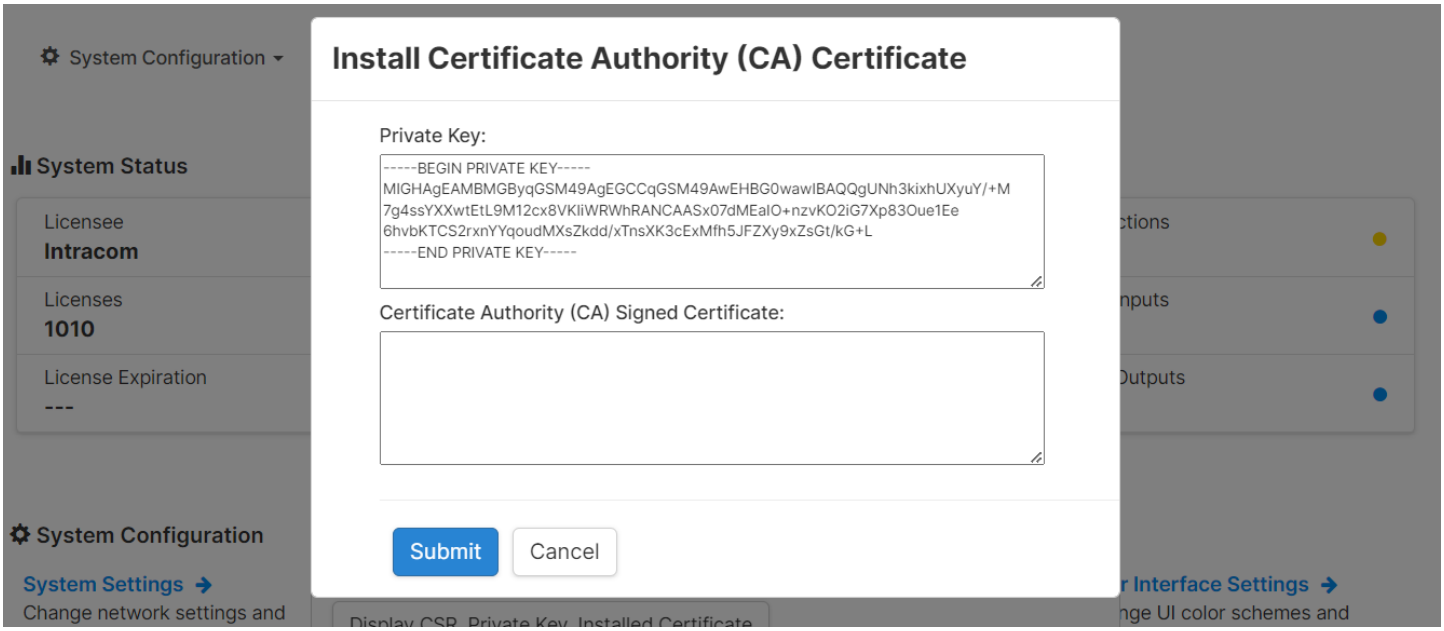


There are a variety of methods that can be used to verify ownership of your domain. For this guide we have chosen the DNS (CNAME) option however any of the methods will work. Follow the instructions to create the necessary DNS records then click the Verify button.

Copyright Bosch Security Systems



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 VLink. Log into the System Administration and from the System Maintenance dropdown select Certificate. Click Install 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.

Copyright Bosch Security Systems

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 VLink server.

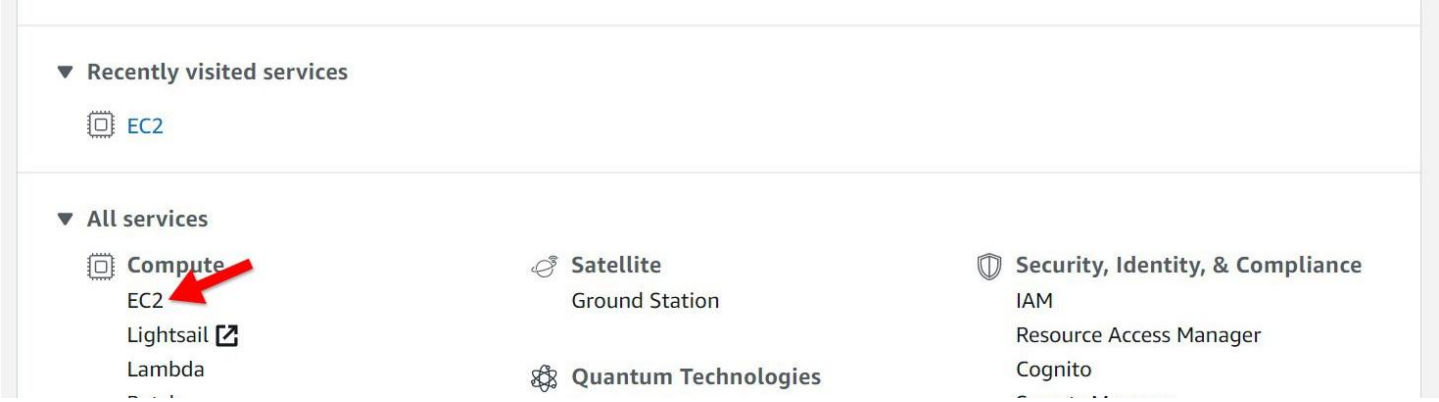
Installing the Self-Signed Certificate on iOS
1. From the WebRTC Control Panel login screen press the button to download the SSL certificate
2. A popup will display with instructions on how to install the certificate on your device

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 RTS Certificate that you downloaded previously

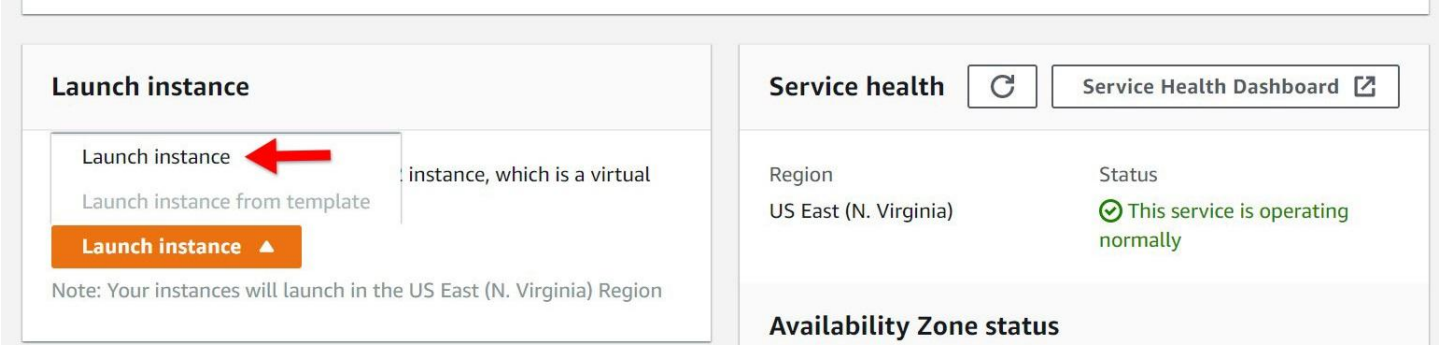
Copyright Bosch Security Systems

2. AWS Installation

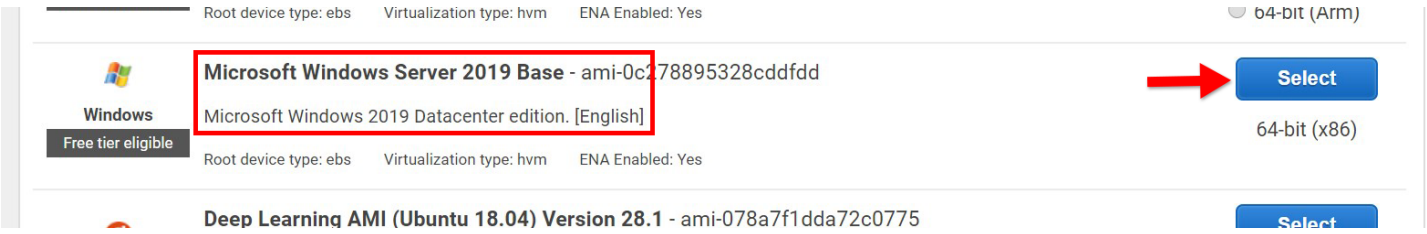
This portion of the guide will show you how to create a virtual machine in the AWS EC2 Cloud.



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



Click the orange Launch instance button then click Launch instance.

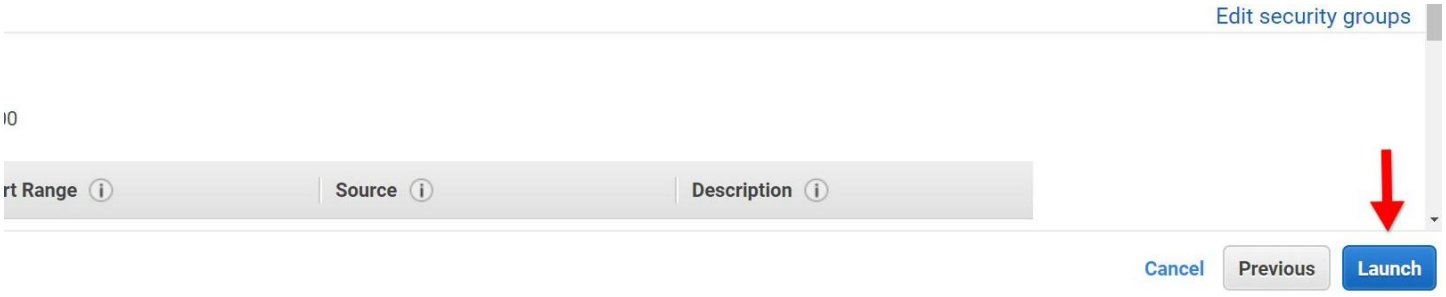


Scroll through the server OS options and select the Microsoft Windows Server 2019 Base image.

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

Copyright Bosch Security Systems

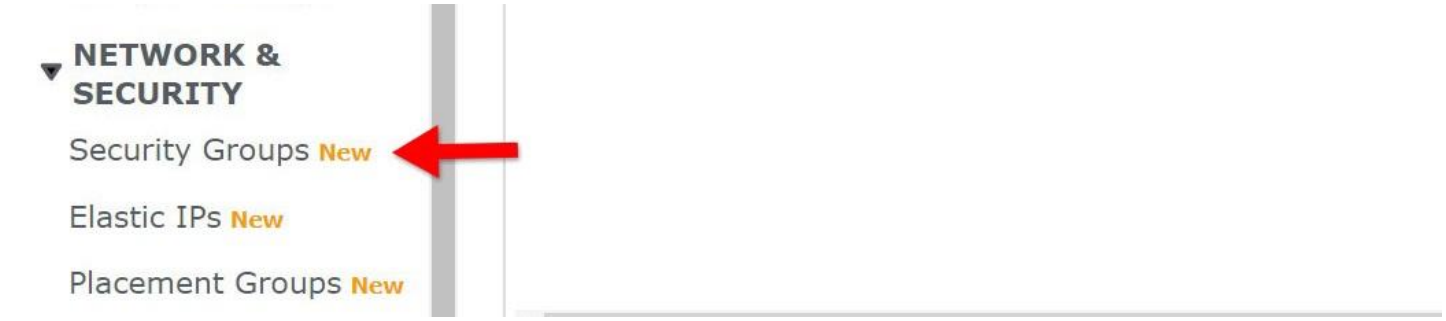
You will now select the hardware specifications for your EC2 instance. System hardware requirements are dependent on the number of concurrent users that will be accessing the system. Please refer to the VLink Virtual Matrix Intercom System Requirements document for more information. For the purpose of 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.

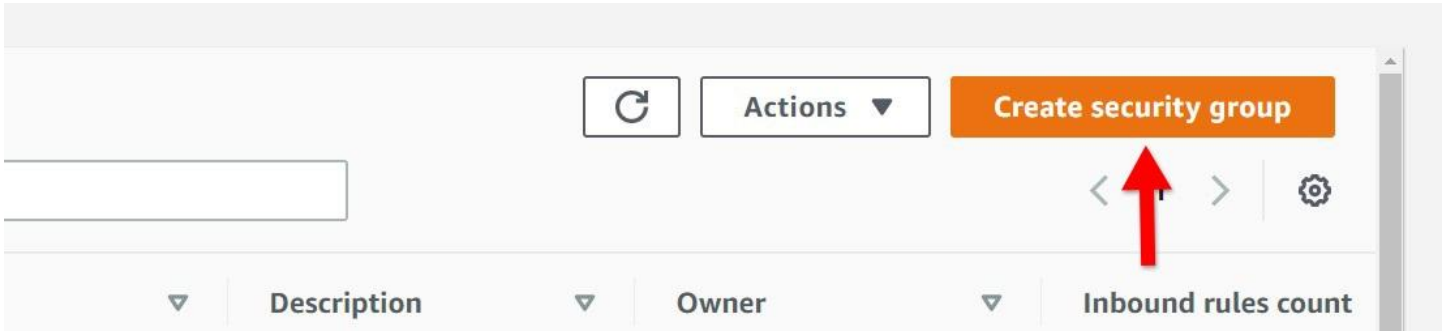
2.1 AWS Security Group (firewall) Configuration

VLink 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 VLink Virtual Matrix.

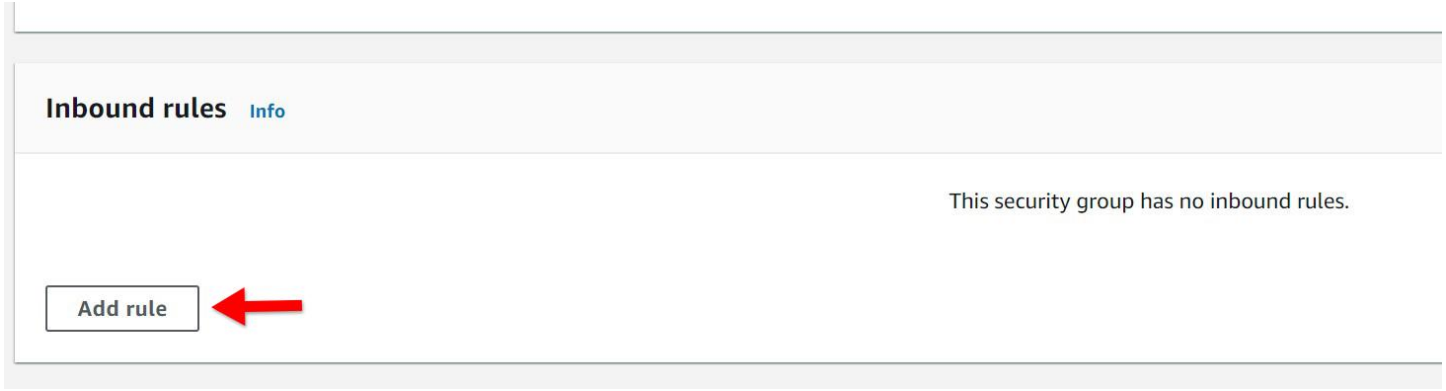


From the left-hand site of the AWS EC2 Management Console click the Security Groups option under the Network & Security section.

Copyright Bosch Security Systems

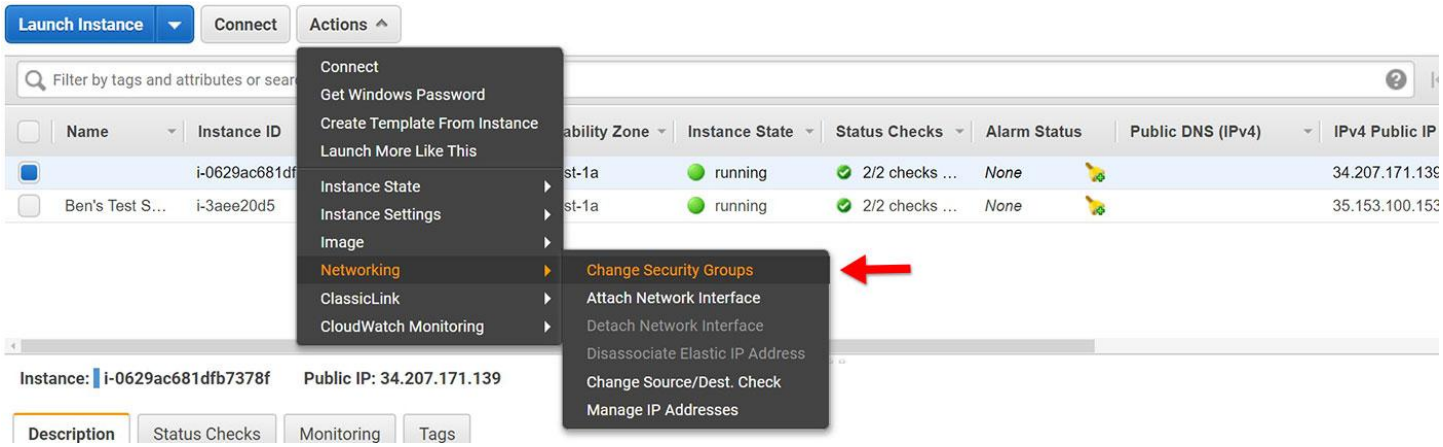


On the top right click Create security group.



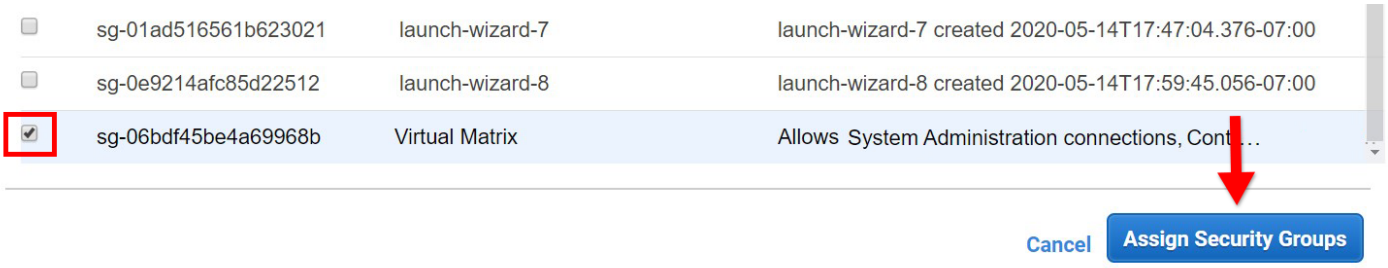
Enter a Security group name and Description (other options can be left default). Scroll down and under the Inbound rules section click Add rule. A list of ports used by VLink Virtual Matrix is available in the Network Requirements section of our documentation. Add a rule for every required port.

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.



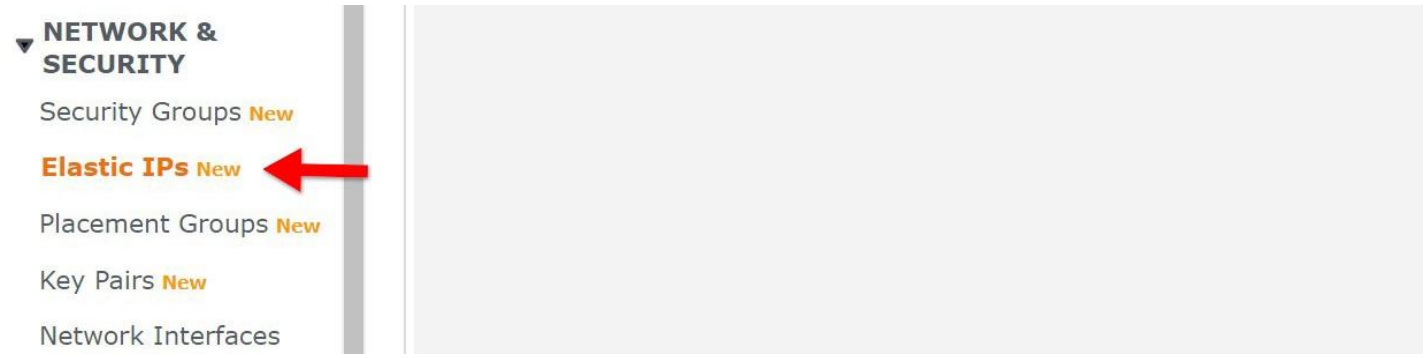
Copyright Bosch Security Systems

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.

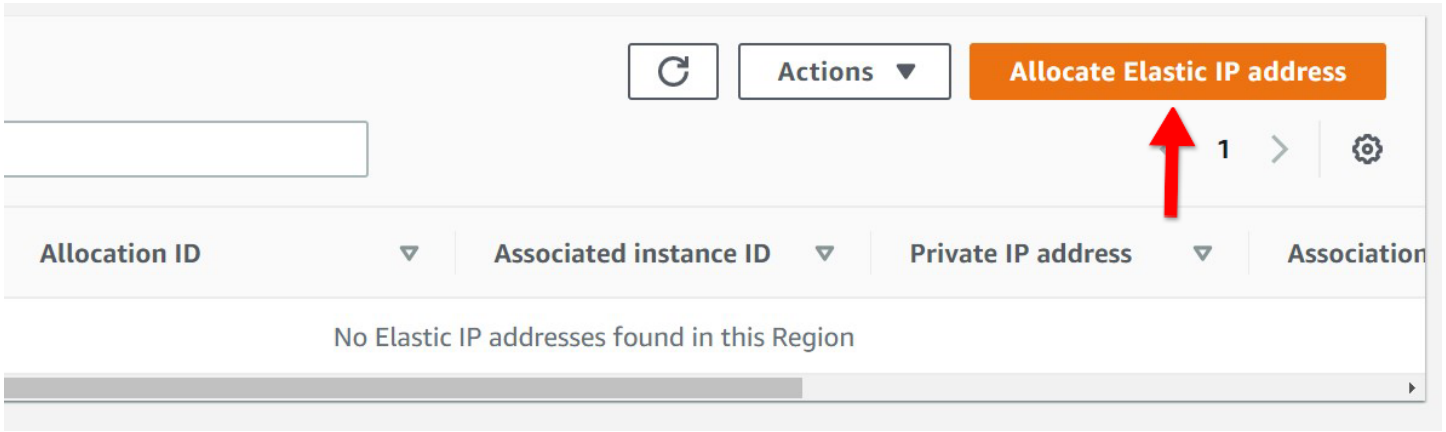


Deselect the default Security Group assigned to the instance and select the Security Group you just created. Finally, click Assign Security Groups to complete the process.

2.2 Static IP Address Configuration (recommended)

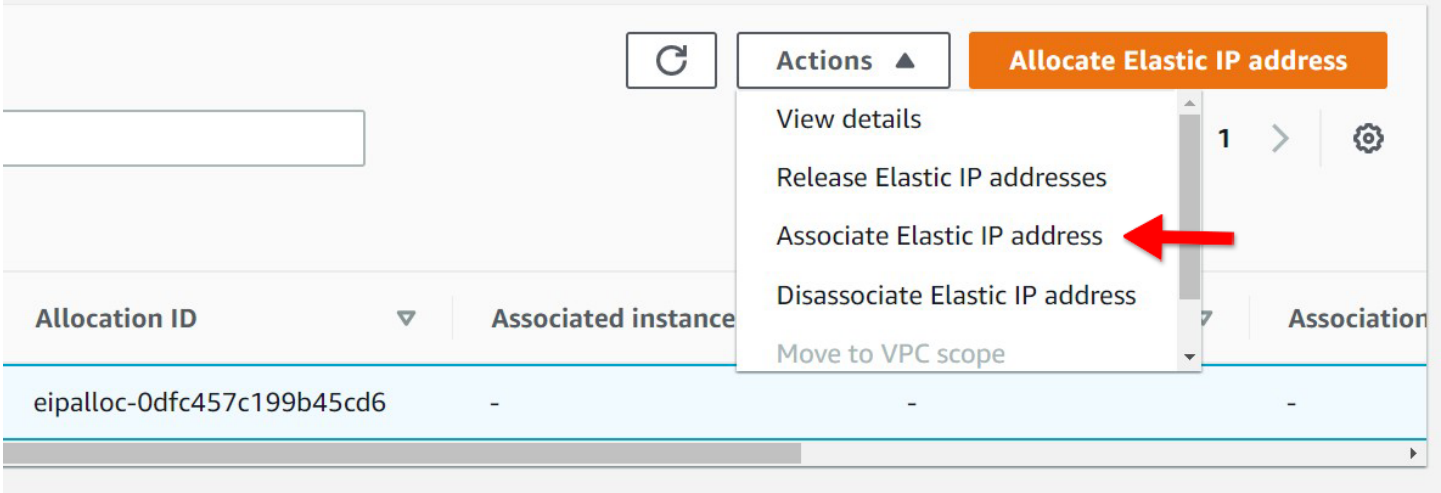


From the left side menu select Elastic IPs

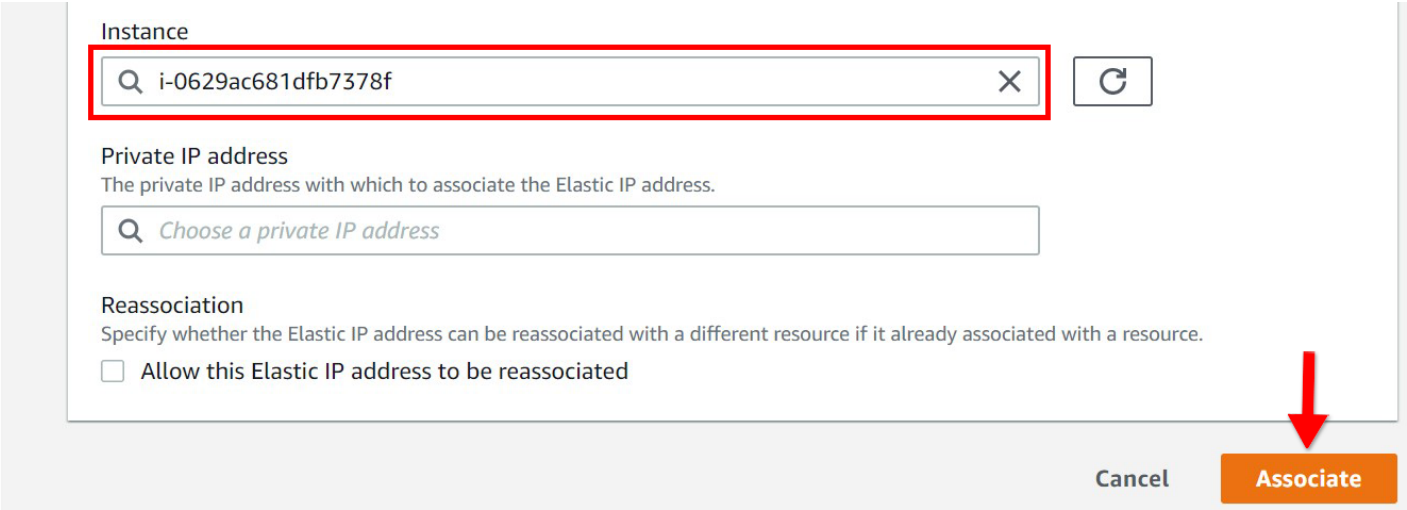


Copyright Bosch Security Systems

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



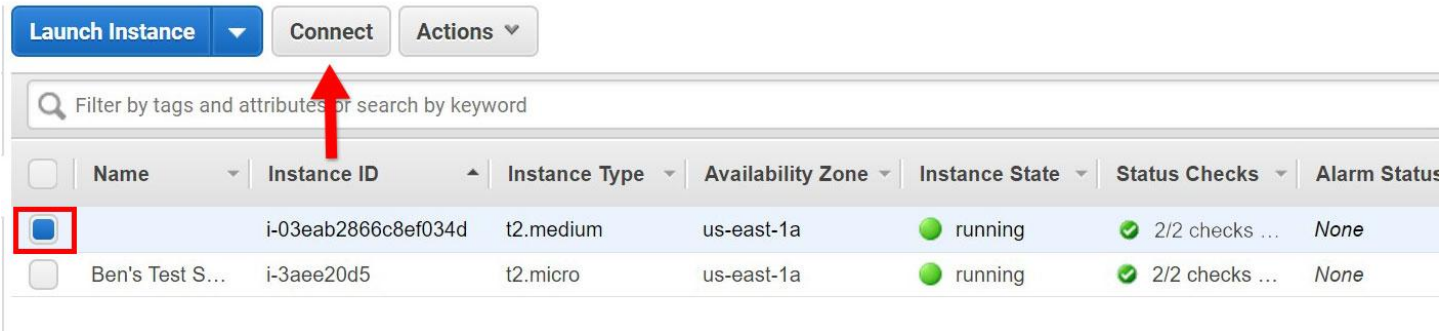
Ensure that the IP address you were just given is selected on the list and then from the Actions menu select Associate Elastic IP address.



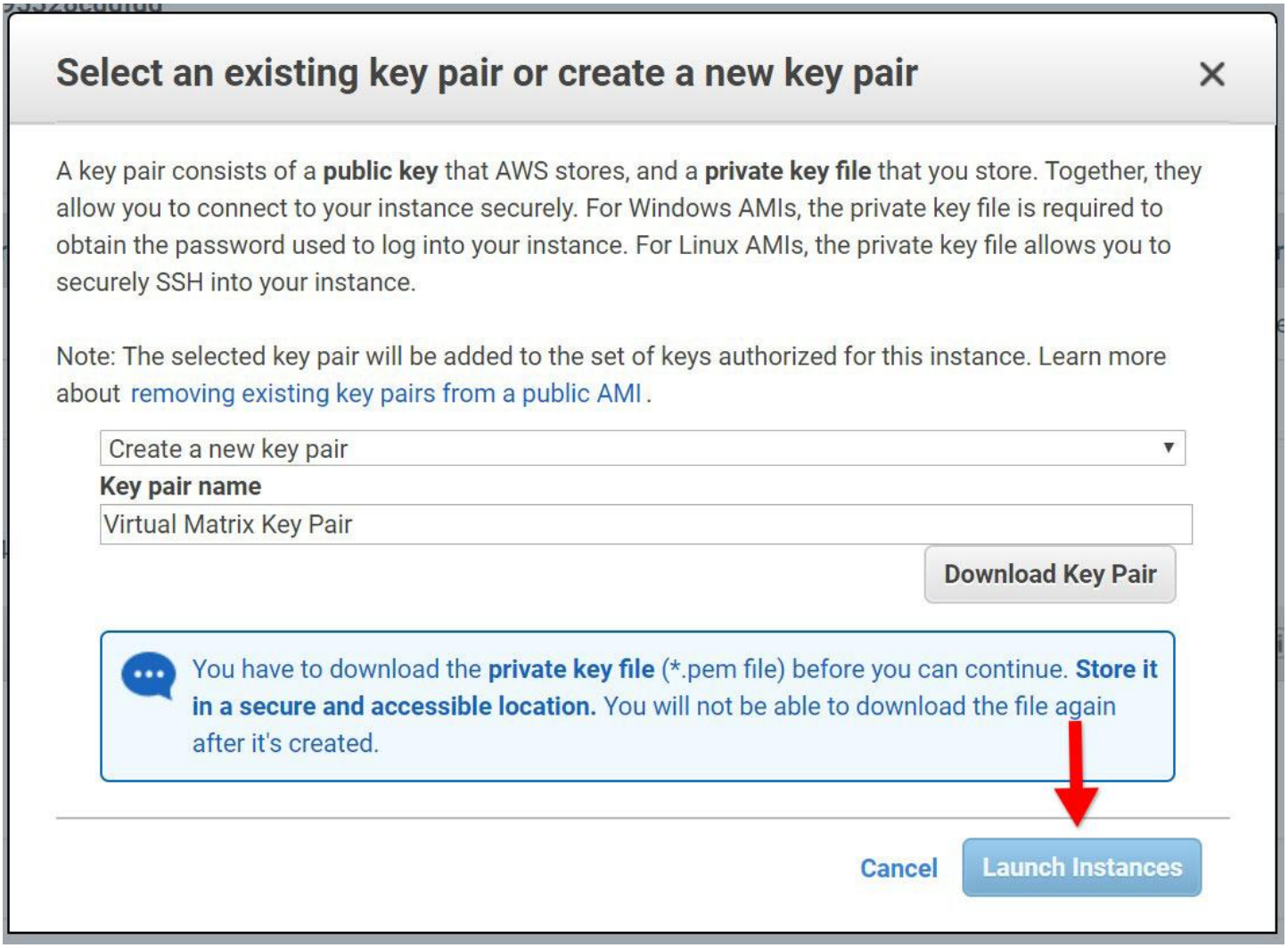
Select your EC2 instance from the list and then click Associate. All other options can be left default.

Copyright Bosch Security Systems

2.3 Connecting to the EC2 Instance

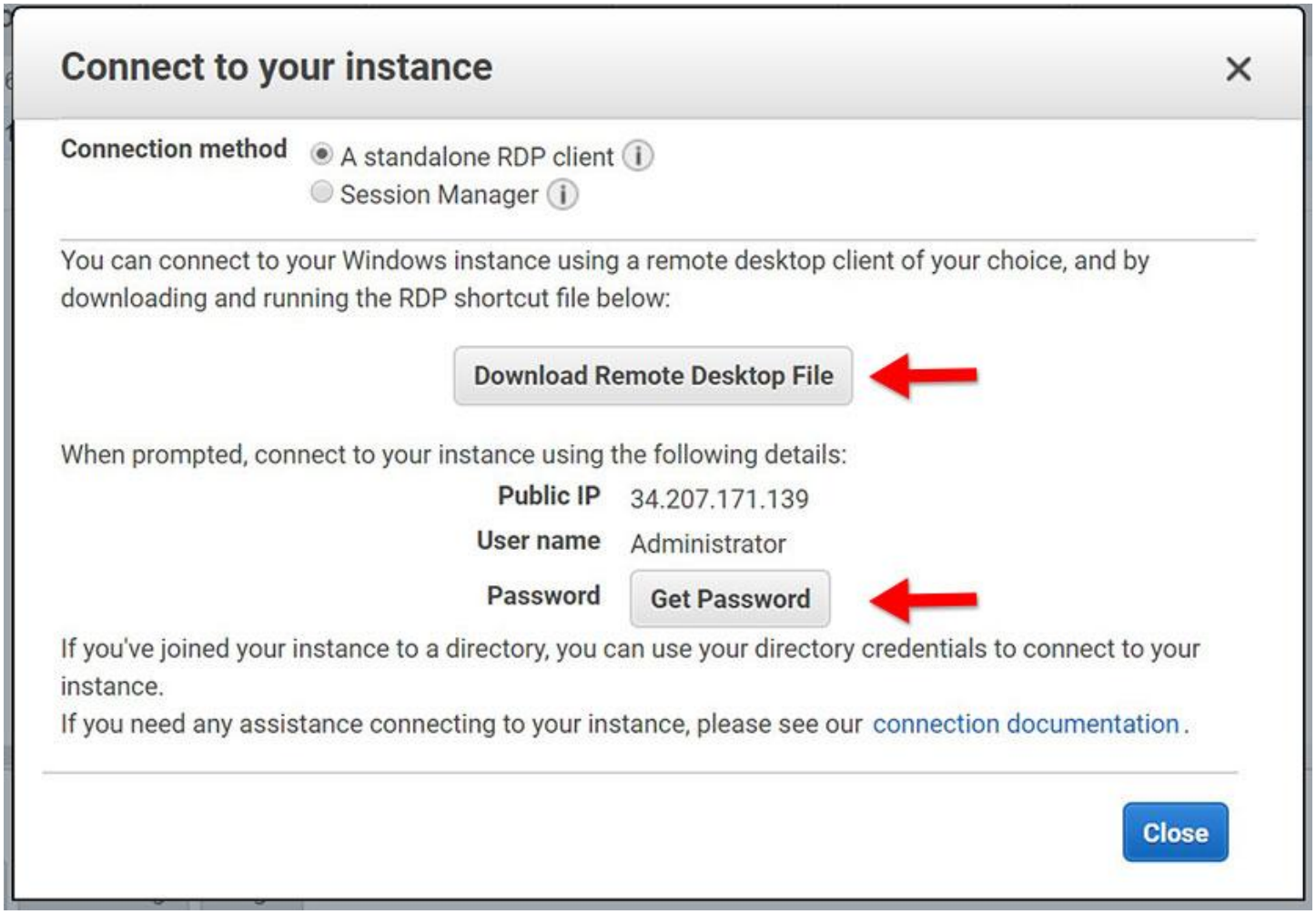


Select your server from the list and click the Connect button at the top.



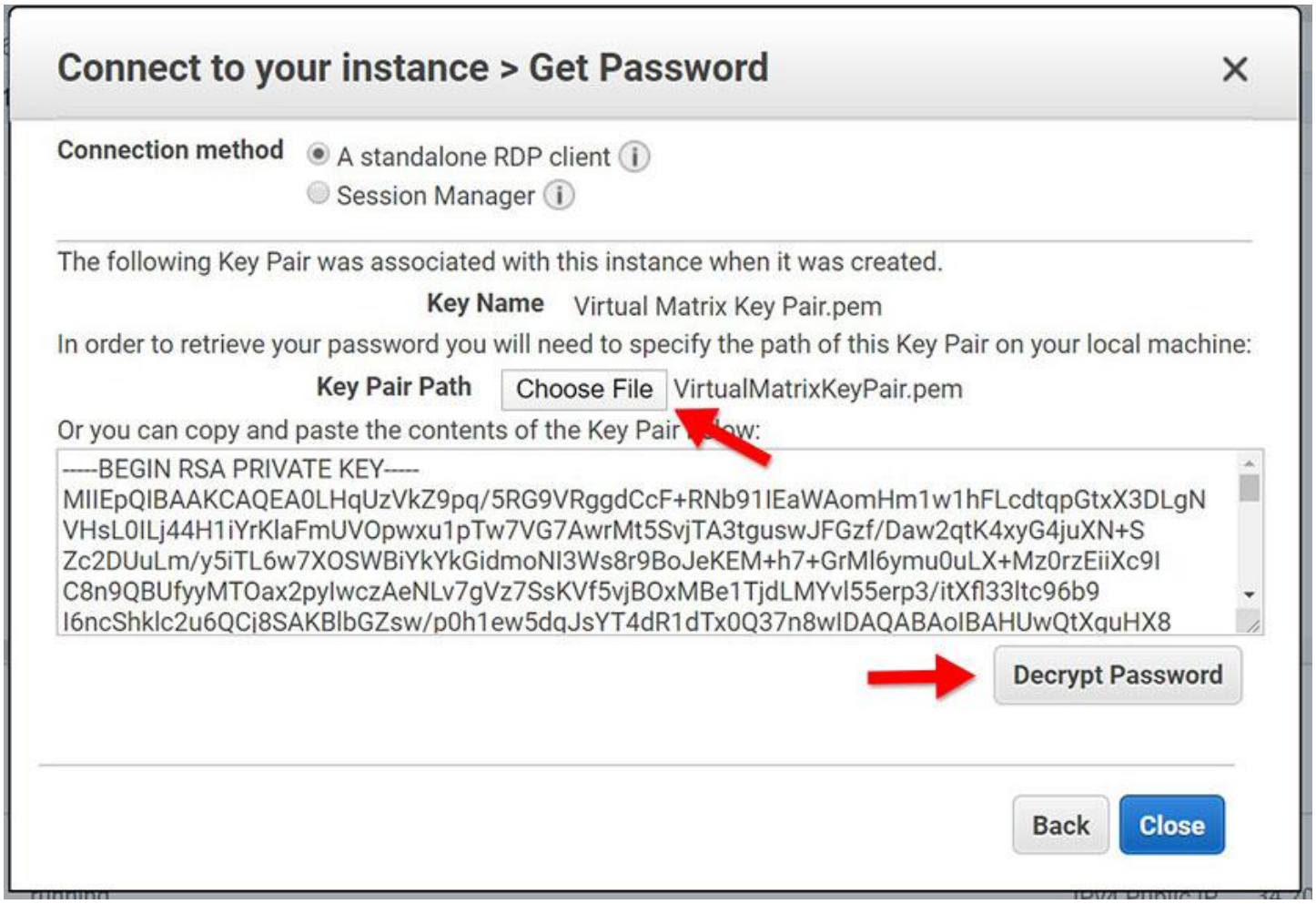
Copyright Bosch Security Systems

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



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.

Copyright Bosch Security Systems



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.

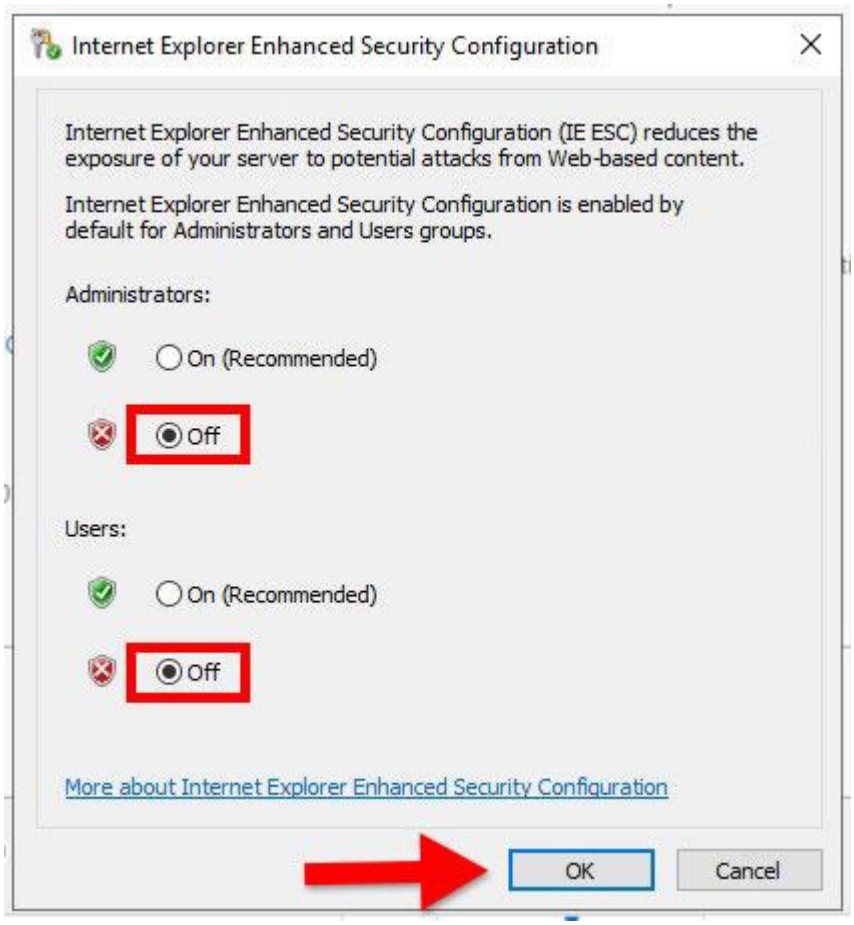
2.4 Configuring the EC2 Instance

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 VLink Virtual Matrix from the internet. You can skip this portion of the guide if you plan to transfer the VLink Virtual Matrix installer to the server using RDP.

Copyright Bosch Security Systems

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 VLink 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.

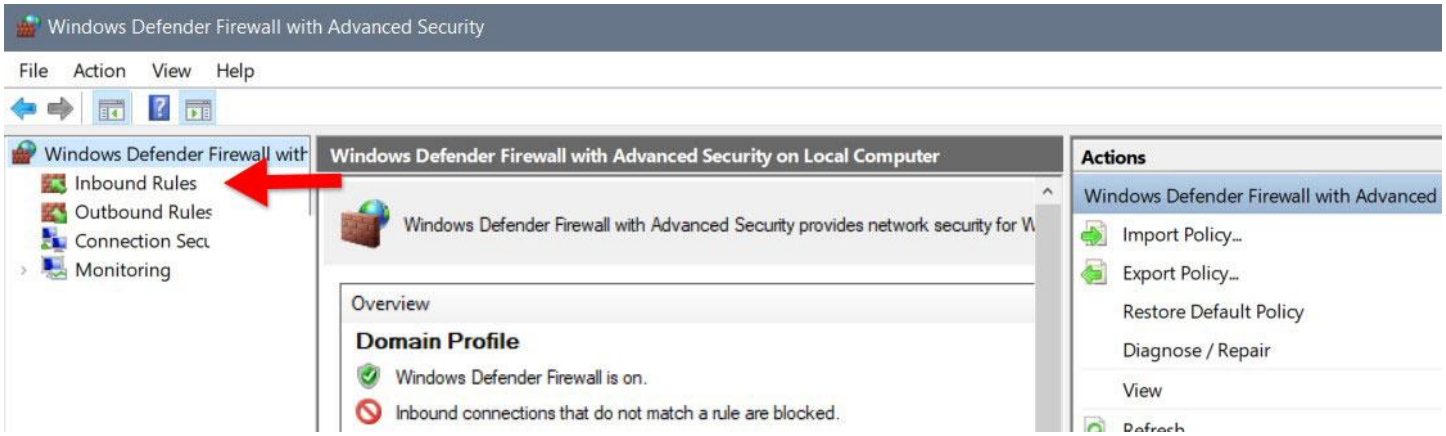


Disable the IE Enhanced Security Configuration as show above then click Ok. You will now be able to download the VLink Virtual Matrix Software from our website.

Copyright Bosch Security Systems

Windows Firewall Configuration

You will need to either disable the Windows firewall entirely or configure Inbound Rules for all of the ports required by VLink 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 VLink Virtual Matrix is available in the Network Requirements section of our documentation. Add a rule for every required port.



Software Installation and Licensing

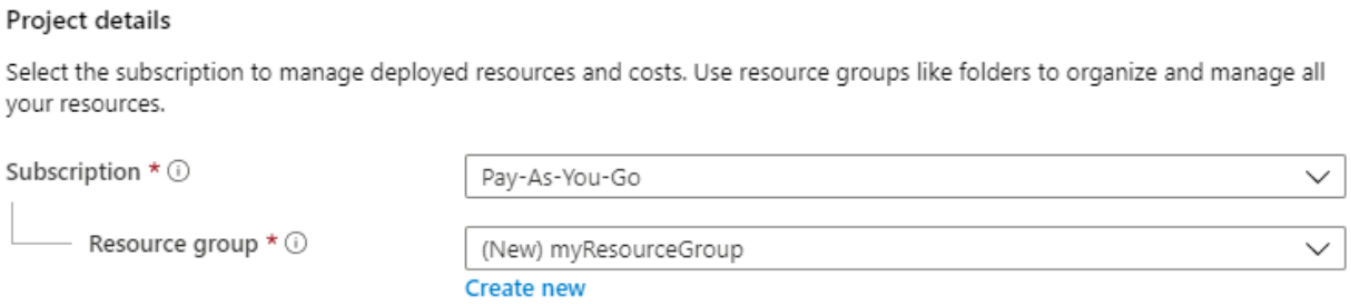
Please follow the VLink Virtual Matrix Software Installation and Licensing documentation to complete the setup.

Copyright Bosch Security Systems

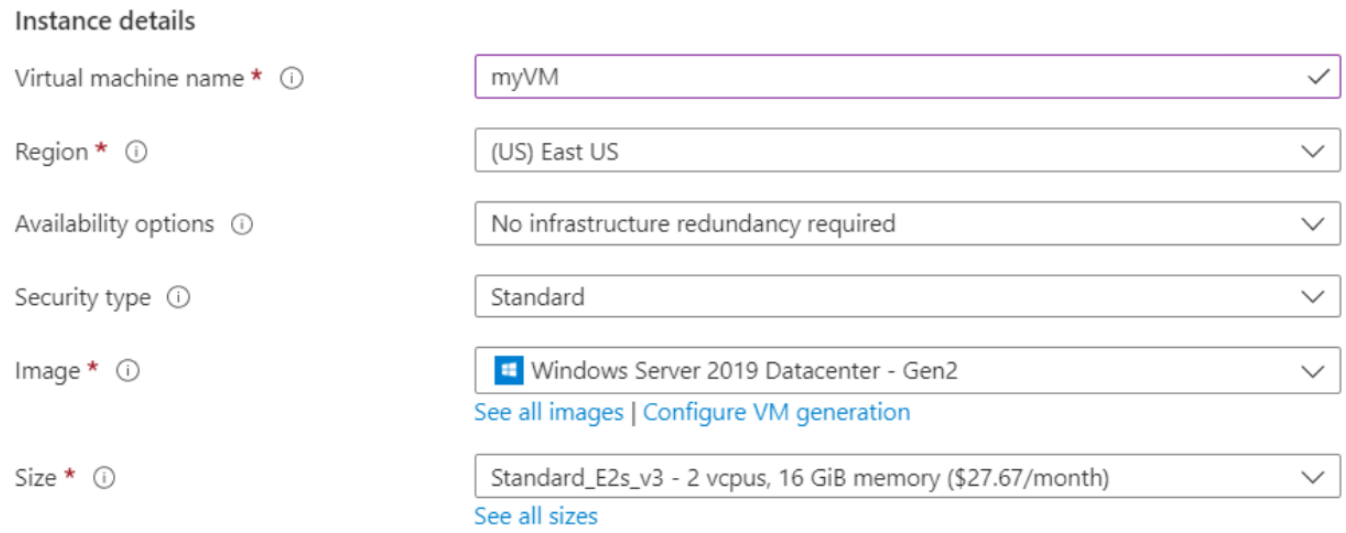
3. Azure Installation

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.



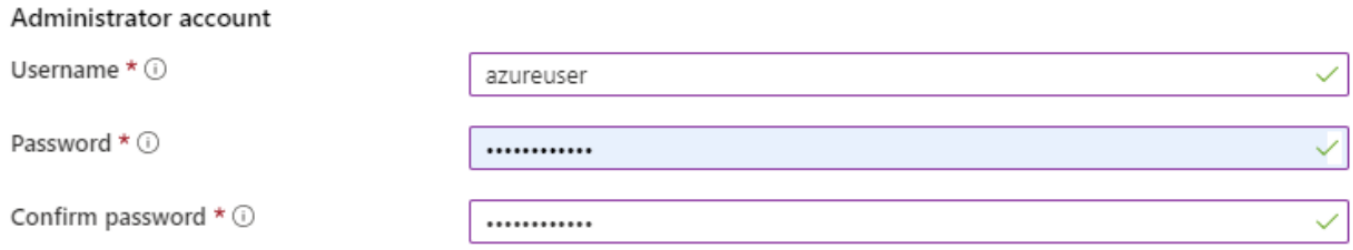
Select the Basics tab and select an existing Resource group or create a new one.



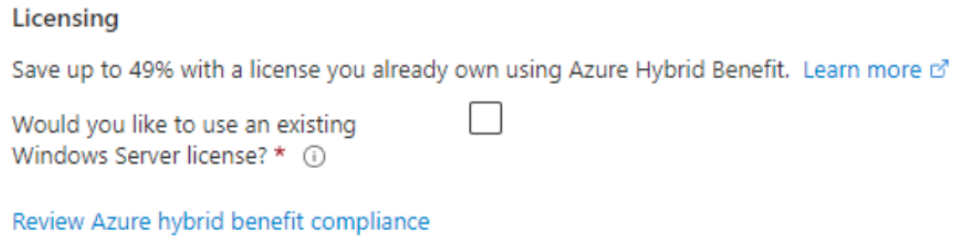
Specify your instance details. System hardware requirements are dependent on the number of concurrent users that will be accessing the system. Please refer to the VLink Virtual Matrix Intercom System Requirements for more information.

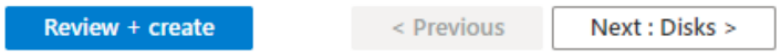
Note: VLink can be run on all modern Windows Operating Systems. You may use a different version than what is show above.

Copyright Bosch Security Systems



Under Administrator account provide a username and password.

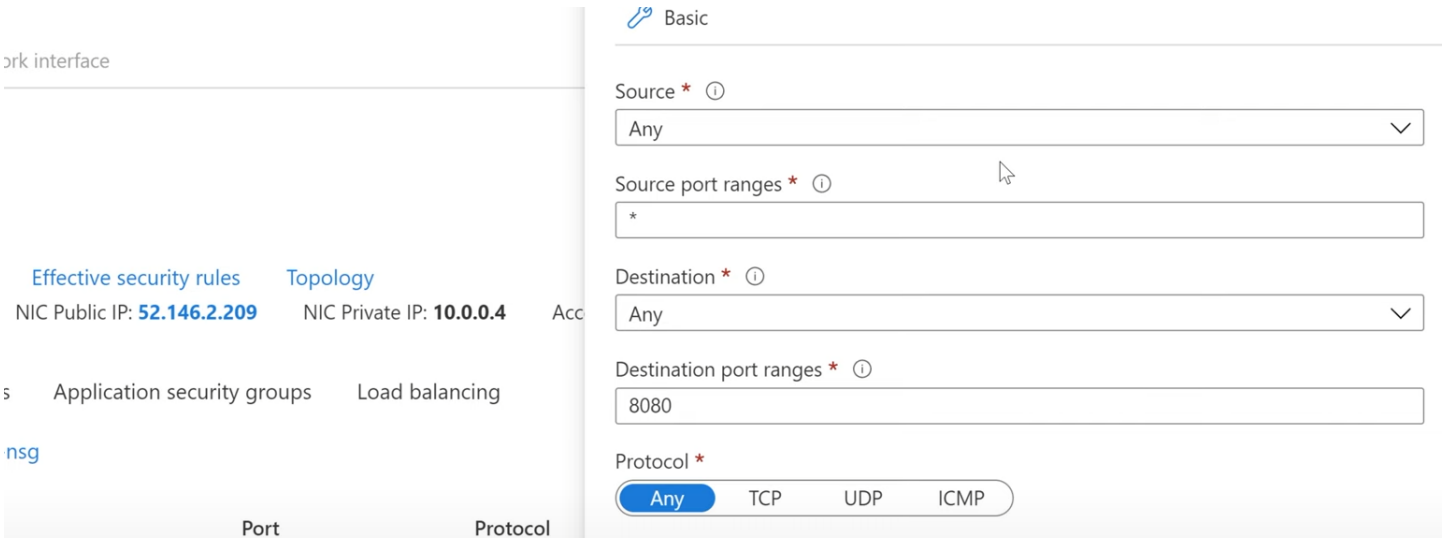




Click the Review + Create button at the bottom of the page.

3.1 Firewall Configuration

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

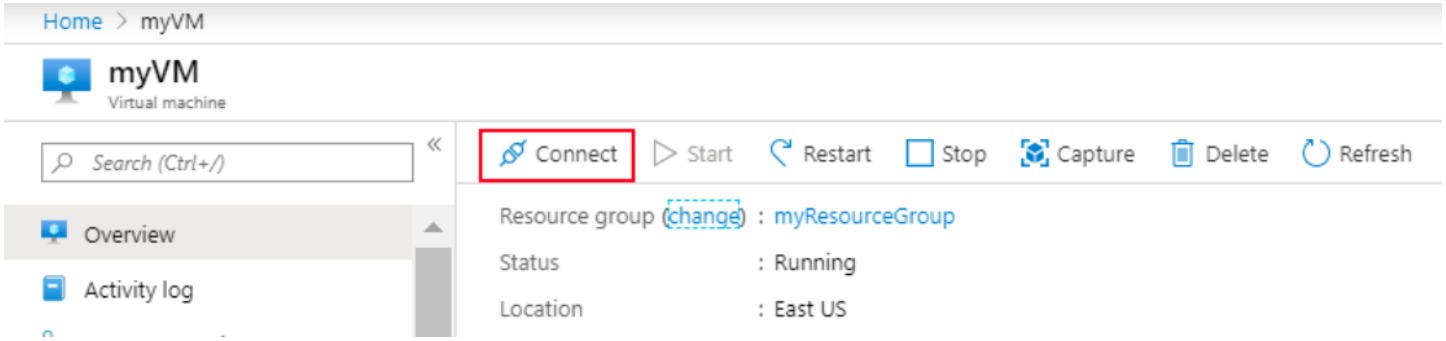


Copyright Bosch Security Systems

A list of ports used by VLink 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



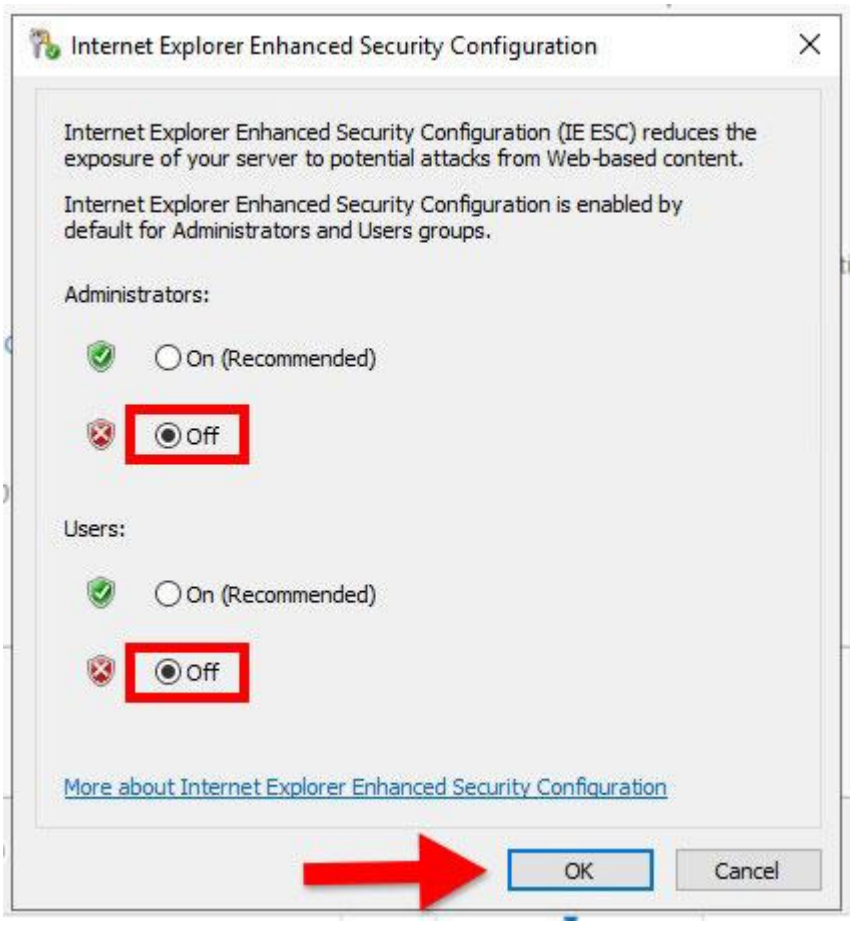
From the Overview page select Connect and then RDP. Then click Download RDP file. Double click the RDP file and click connect then enter in the username and password for the server.

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 VLink Virtual Matrix from the internet. You can skip this portion of the guide if you plan to transfer the VLink Virtual Matrix installer to the server using RDP.

Copyright Bosch Security Systems

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 VLink 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.



Disable the IE Enhanced Security Configuration as show above then click Ok. You will now be able to download the VLink 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 VLink 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 VLink Virtual Matrix is available in the Network Requirements section of our documentation. Add a rule for every required port.

Copyright Bosch Security Systems

Software Installation and Licensing

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

Copyright Bosch Security Systems

4. VLink TIF

4.1 Introduction

This guide provides the basic outline of configurations required to use VLink to connect ADAM to SIP phone systems and provide intelligent control and status of phone lines.

Please refer to your phone system administrator or SIP phone service provider for configuration information needed to properly connect SIP lines from your VLink, and which may be required on the phone system side for proper interconnect.

4.2 Phone Switch SIP Line Planning

The first step in a successful setup is to establish the number of phone lines to be configured and determine the details of the phone switch or SIP service provider being used. VLink will generally interface with any typical phone switch or service provider.

In each case there will be an IP address for the SIP line services, and most likely user name and password access information for each line being configured.

Before moving forward, please ensure this preliminary information is on hand for entry into the configuration screens described in this document.

4.3 Phone Switch / PBX Connect Method

There are two possibilities for the VLink TIF server to connect to a Phone Switch or PBX. The first is via a Registered connection where we use a username and password to register a SIP Client to the PBX and then receive and initiate calls via SIP Invites from/to the PBX in the same manner as a SIP client. The second is via a Direct IP or non-registered connection in which we only use the user name to receive and initiate calls via the PBX. In this case there is no registration or authentication but rather simply SIP Invites from/to the PBX. At some customer installations, this second method is used to install a SIP Trunk between the VLink TIF server and an offsite 3rd party provider for the phone line access.

Copyright Bosch Security Systems

4.4 IP Network Considerations

A critical element in successful planning is the IP network connectivity required for the system components to link to each other. Whether the SIP lines are provided by an external SIP service provider, or internal phone switch, the VLink server must have direct IP connectivity with at minimum TCP/UDP Port 5060 open between the VLink and the SIP signaling server. Also, all UDP ports must be open between VLink and the RTP media servers.

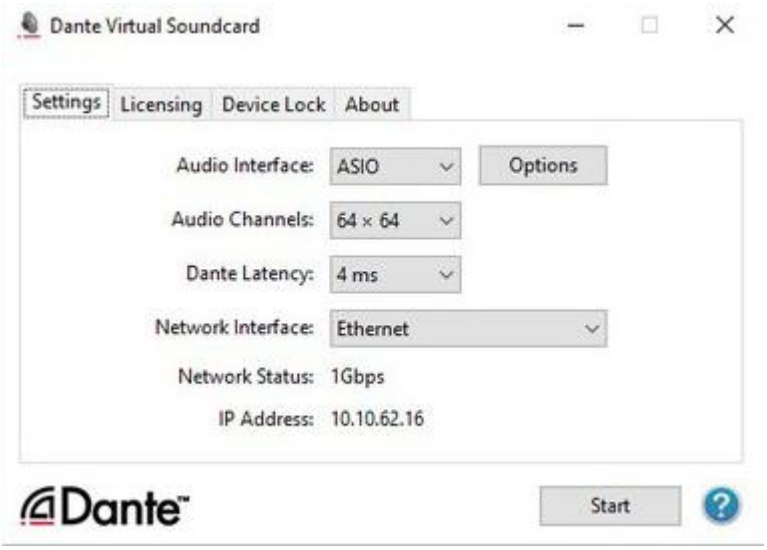
Additionally, the RTS ADAM Omneo card(s) and master controller cards, AZEDIT configuration PC, and optional Pacific Interactive TIF Tally display must have IP connectivity between each other and the server.

An important note about Dante audio is that it requires direct IP connectivity on the same local subnet. For this reason, the VLink server and the RTS Omneo cards should be plugged directly into the same network switch for best results. Other components can be plugged in anywhere on a network, so long as IP connectivity between them is available. If network connections between components other than the VLink server and Omneo card(s) are routed and/or protected by firewalls, certain TCP and UDP ports must be configured as passable between components.

4.5 Dante Virtual Soundcard (DVS)

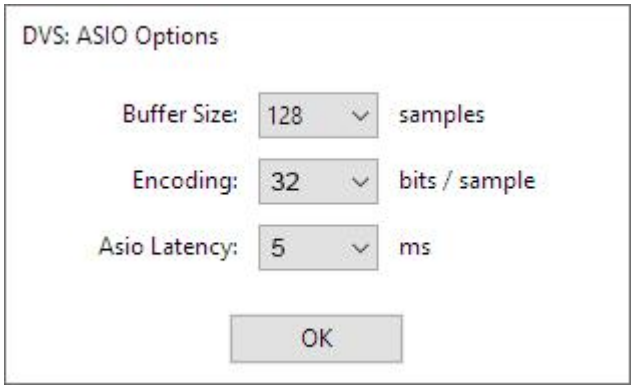
This guide details audio connectivity between the VLink and RTS intercom utilizing Audinate’s Dante audio protocol. Instructions on how to install and activate DVS can be found on Audinate's website.

Copyright Bosch Security Systems



Once activated, select configure Dante's settings as shown above.

Audio Interface = ASIO Audio Channel = 64 x 64 Dante Latency = 4ms Network Interface = (choose the appropriate Ethernet connection the server uses)



Next, click the options button and configure the fields as shown.

Buffer size = 128 samples Encoding = 32 bits / sample Asio Latency = 5 ms

4.6 RTS Intercom Port Planning

Based on the number of lines being interfaced, and the number of channels on the RTS OMNEO card, it is important at an early stage to clearly identify which phone line will connect to which intercom port. For example, if a 16 channel Omneo card is used, and it is installed as intercom ports 97-112, and the phone numbers being interfaced are

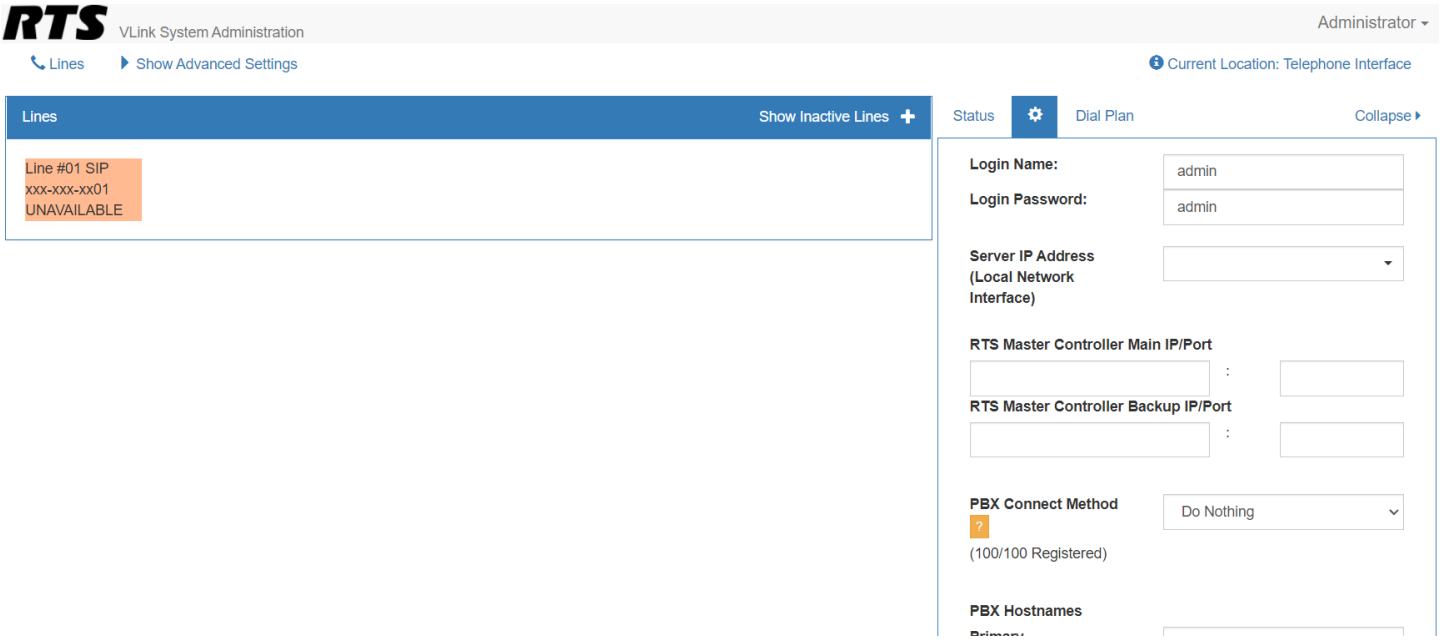
Copyright Bosch Security Systems

999-999-1001 thru 999-999-1016, you should determine and note which line will be on which RTS ADAM port. For this example, 999-999- 1001 might connect to intercom port 97, 999-999-1002 to port 98 thru 999-999-1016 connecting to intercom port 112.

Also note that VLink TIF server features require ADAM Master Controller software version 3.1.0 or later (3.4.1 or later preferred), and AZEDIT version 4.7.0 or later (5.1.0 or later preferred). Contact your RTS support representative should you require this software or assistance with upgrades.

4.7 VLink Configuration

To follow this portion of the guide your VLink server must be license. Follow the Licensing documentation to complete this step.



Next, set up the main system settings for SIP and the connection to the RTS ADAM intercom. Click on the System Settings button from the main System Administration window.

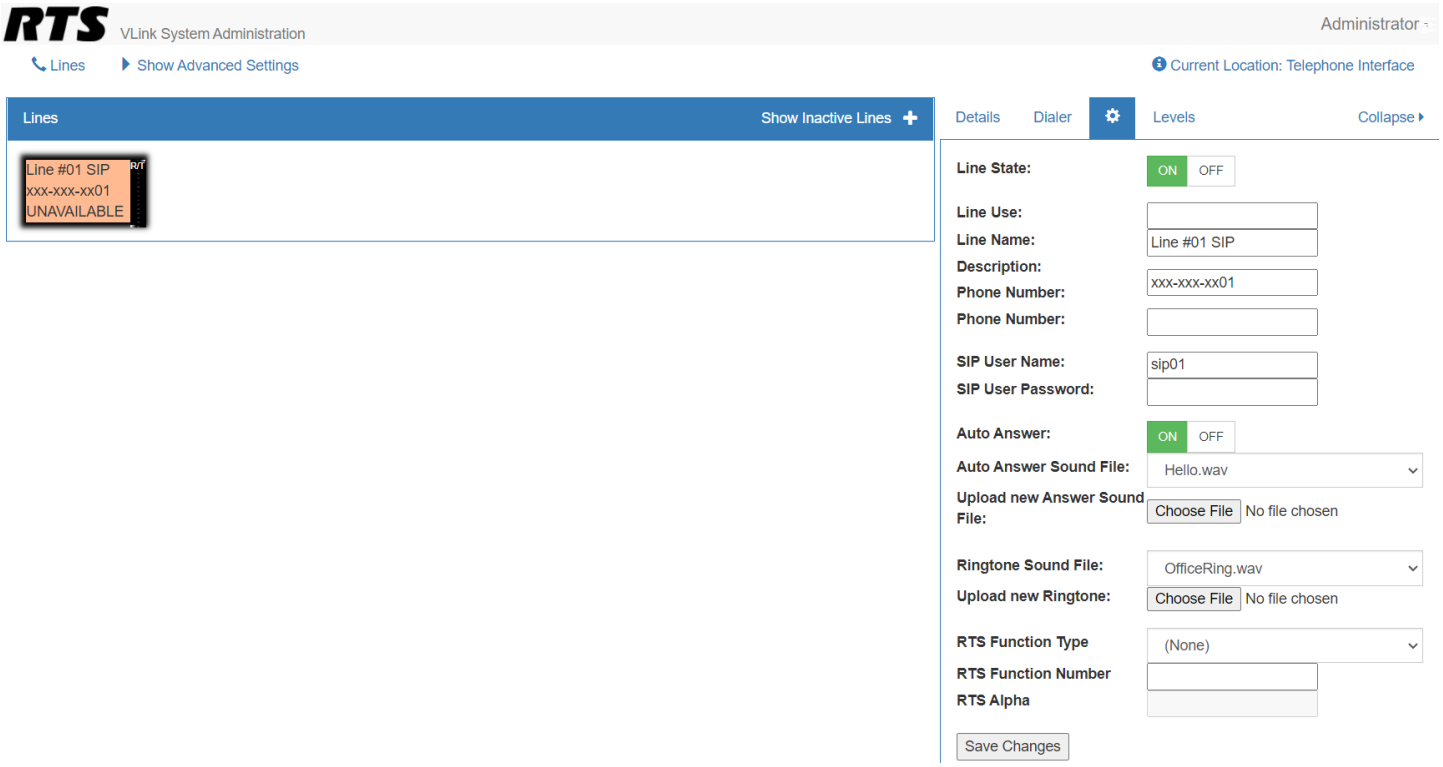
Server IP address (Local Network Interface) should be the IP address of this VLink under most circumstances.

RTS Master Controller Main / Backup IP should be the IP address of the ADAM main master controller followed by the IP address of the ADAM backup master controller.

Copyright Bosch Security Systems

RTS Master Controller Main / Backup IP Port should be 27415 / 27415 under most circumstances.

Adding a SIP Phone Line to VLink



To add a SIP Phone line connection from your phone switch or service provider to the server click Show Inactive Lines from the main System Administration Window. From the lines list, select a line and click the settings gear button.

In the Line Name section enter the phone number. The Phone Number Section will be the name that will appear on the VLink Control Panel selector. Enter the Sip User Name and SIP User Password.

Important Notes

The SIP User Name and Password should be that provided by your SIP phone line provider for that particular line. Click OK.

The Line Name field will be the one that is used and displayed within AZEDIT to link the VLink SIP line and the ADAM intercom ports, so it is highly recommended that the actual phone number is used for the Client Description. The Phone Number will be the default

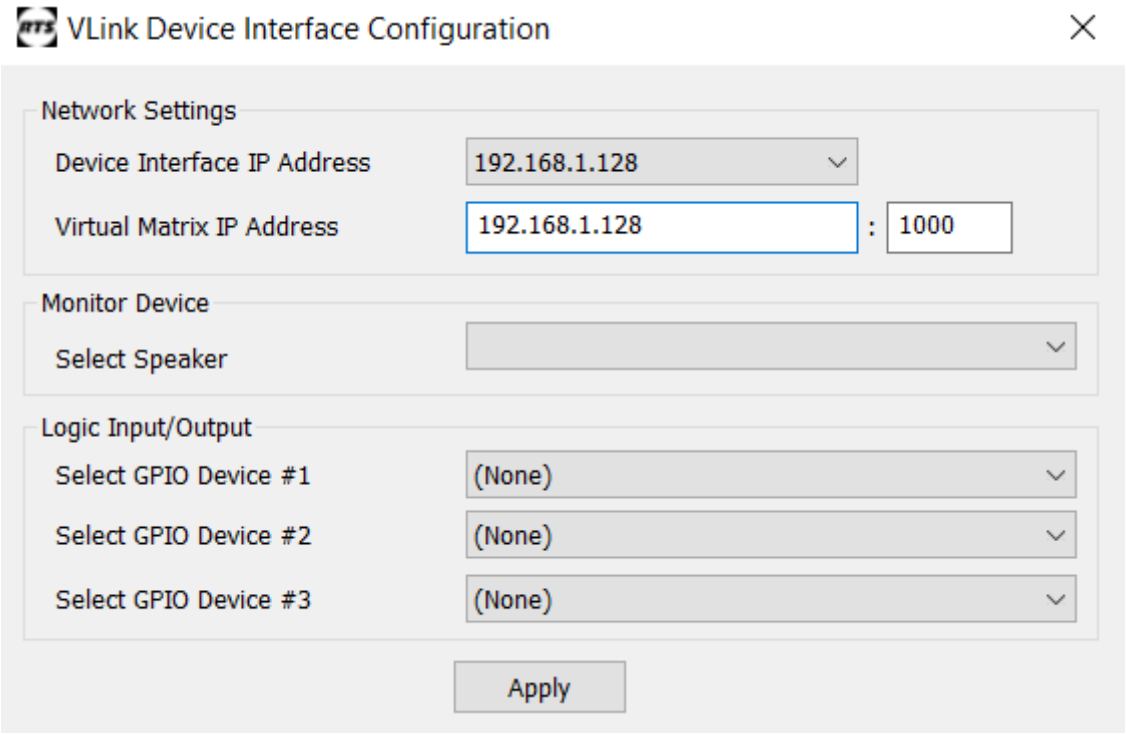
Copyright Bosch Security Systems

that is displayed on the optional Pacific Interactive Status Display System, however you will also be able to explicitly assign the specific ADAM type and function number (ie. IFB, # 1) as the alpha that will be displayed on a line-by-line basis.

4.8 Internal server Dante Virtual Soundcard Channel Connections

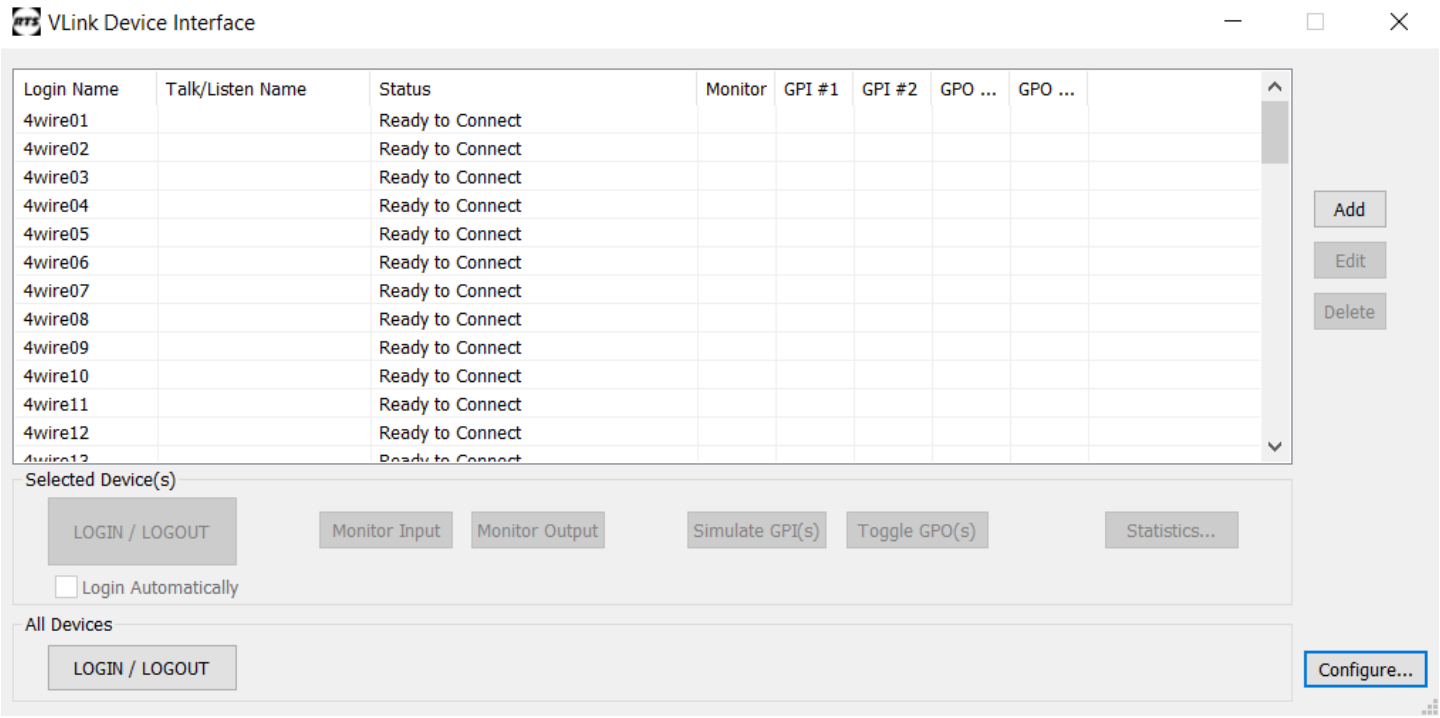
The connection between VLink and Dante Virtual Soundcard is done using the VLink Device Interface application. VLink Device Interface can be downloaded from our downloads page. After installing VLink Device Interface, a registry edit file is used to quickly configure it for use with VLink TIF.

The registry file can be downloaded here. Double-click the registry file. When prompted, click Run and then click Yes.



Launch VLink Device Interface. Enter in your VLink IP address in the Virtual Matrix IP Address field and click Apply.

Copyright Bosch Security Systems

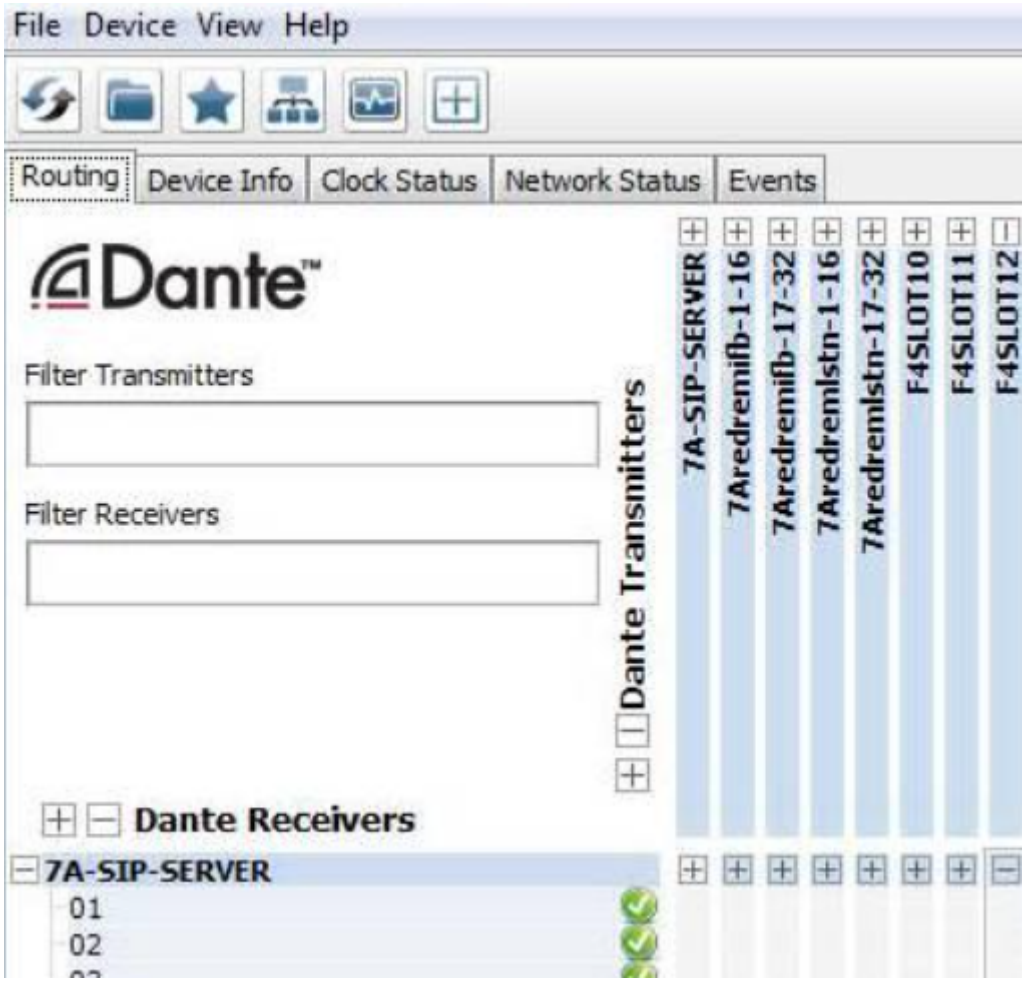


Each row in the VLink Device Interface represents a Dante connection to VLink. Click on a row and press the LOGIN button to connect to the VLink Virtual Matrix.

4.9 Setup of Audio Channels Between VLink and Omneo Cards

Once the SIP phone line has been configured to connect to VLink, and internally the server has been configured to send audio from an installed Dante Virtual Soundcard, the next step in configuration is to map audio channels from the Dante Virtual Soundcard to the associated ADAM Omneo channels. Note it is important to pre-design which phone lines will connect to which intercom port, as this mapping relationship will also need to be done later for phone line control.

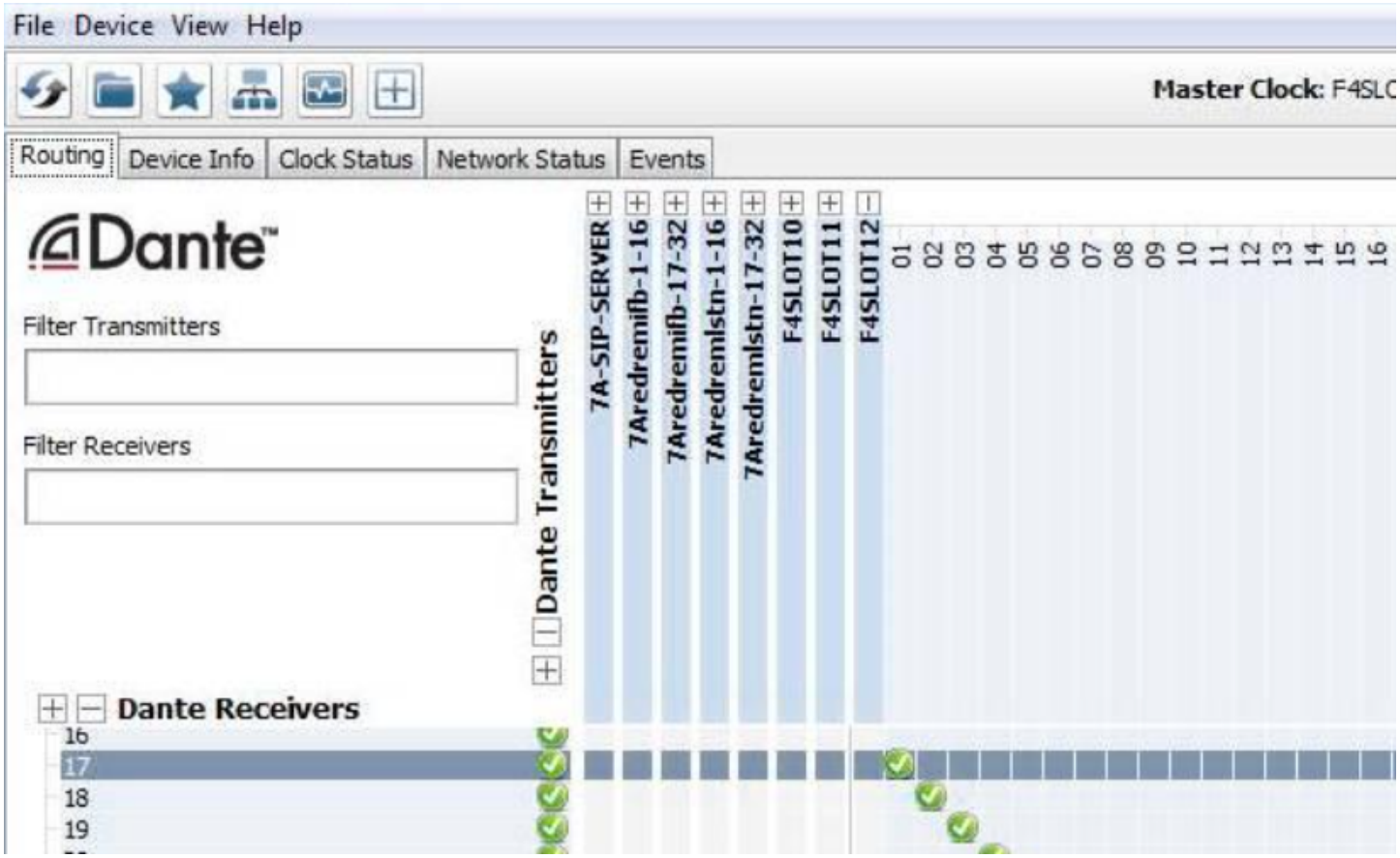
Copyright Bosch Security Systems



The screenshots above show a one-for-one mapping of phone lines in the server to intercom ports via Omneo in the intercom using the Dante Controller software

Click the + next to the VLink name on the left. Click the + next to the RTS Omneo Card name on the top. Click at the crosshairs to create an audio connection (indicated by a green circle) in a diagonal so each VLink channel is mapped in one direction to the associated Omneo card channel. Click the – next to the VLink Sever PC name on the left. Click the – next to the RTS Omeno Card name at the top.

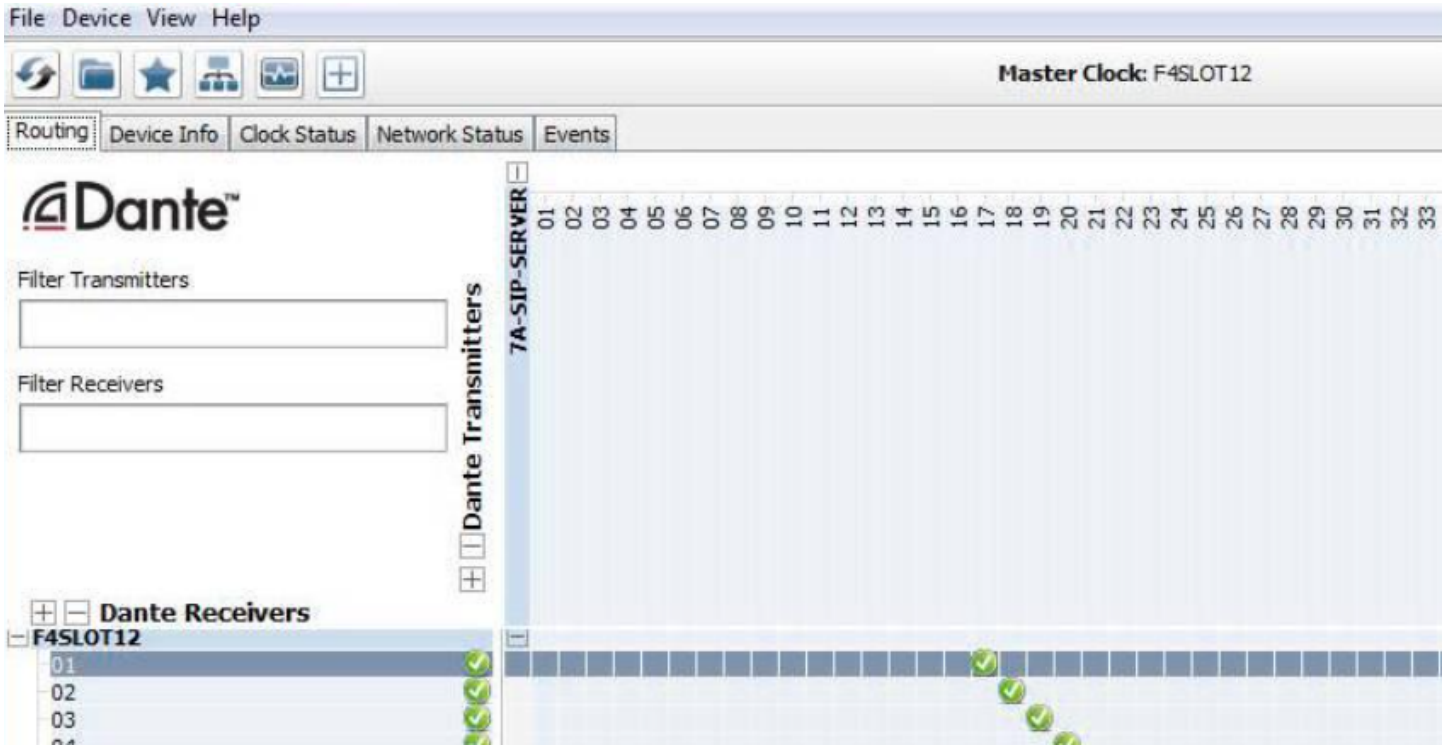
Copyright Bosch Security Systems



Next, click the + next to the RTS Omneo Card name on the left. Click the + next to the VLink name on the top. Click at the crosshairs to create an audio connection (indicated by a green circle) in a diagonal so each Omneo card channel channel is mapped in the other direction to the associated VLink channel.

Click the – next to the VLink Sever PC name on the left. Click the – next to the RTS Omeno Card name at the top.

Copyright Bosch Security Systems



To connect a VLink to be used for SIP phone line connection to an ADAM intercom, follow the steps below:

The RTS ADAM intercoms support up to eight redundant and separate SIP servers. In AZEDIT, name the server you are currently configuring. Click Alphas / SIP server. Double Click on the SIP server being configured.

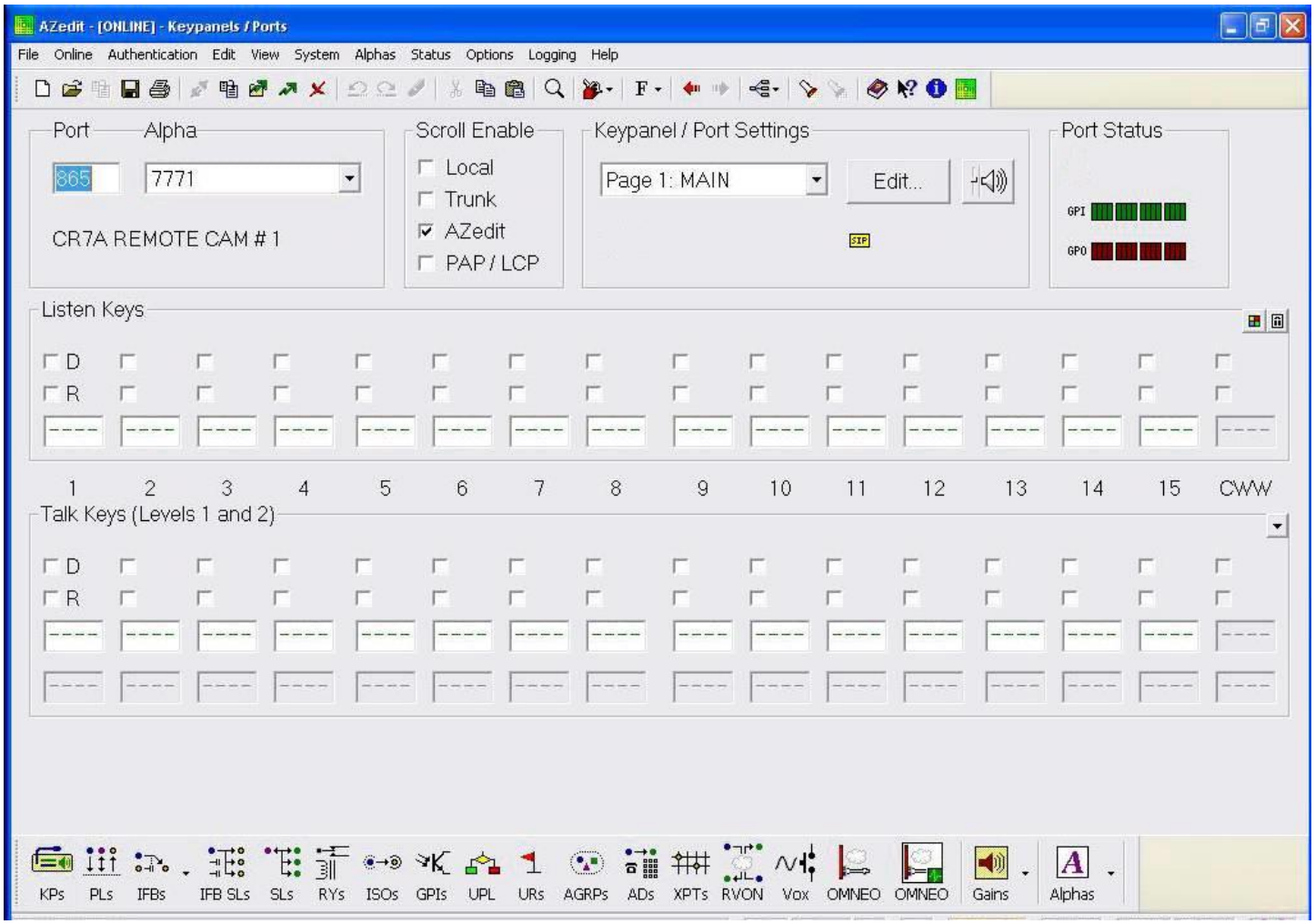
Enter the SIP server Description in the EDIT box and click DONE.

Under Options/SIP server communications, enter the IP address of the SIP server (and redundant server if applicable) as shown below.

4.10 Intercom Port to SIP Line Association

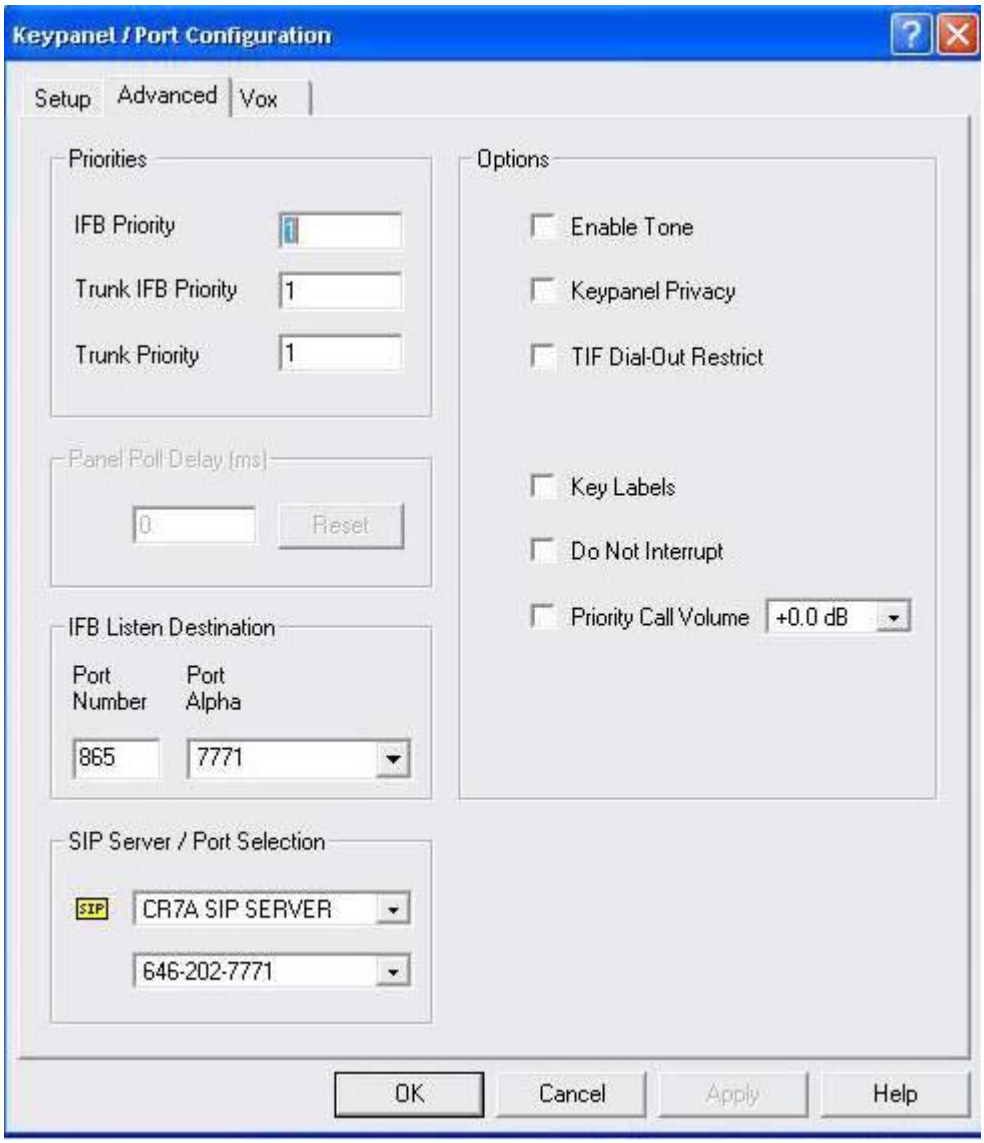
Next you must tell the intercom which intercom port is connected via audio to which VLink device interface channel / SIP Phone Line. This must be consistent with how you have designed the phone line connection to the server 4-wire, and the internal Dante Virtual Soundcard channel to the Omneo intercom port channel.

Copyright Bosch Security Systems

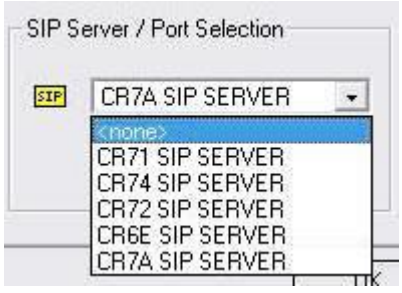


When completed, the intercom port keypanel setup page for each phone line’s intercom port will have a yellow SIP indicator box under the Edit button. From the keypanel setup screen for the first SIP phone line port, Click the EDIT button.

Copyright Bosch Security Systems

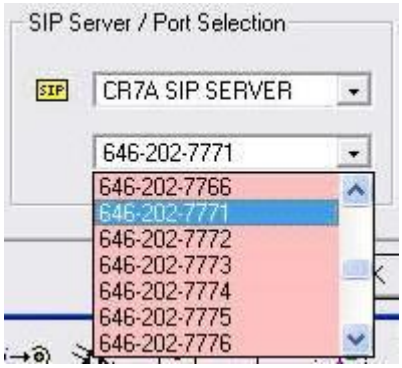


Click the Advanced Tab



Under the SIP / server / Port Selection, Click the first pulldown and select the VLink for the phone lines being configured

Copyright Bosch Security Systems



Click the second pulldown and select the VLink phone line to be associated with this RTS intercom port.

Click OK. Do this for each intercom port that has been connected to each of the VLink SIP phone lines

4.11 Testing

To test the completed system, first make sure all systems are turned on and connected to the IP network. Make sure the VLink Device Interface application is running. Additionally, make sure Dante Virtual Soundcard application is running (the Dante Controller Program does not need to be running).

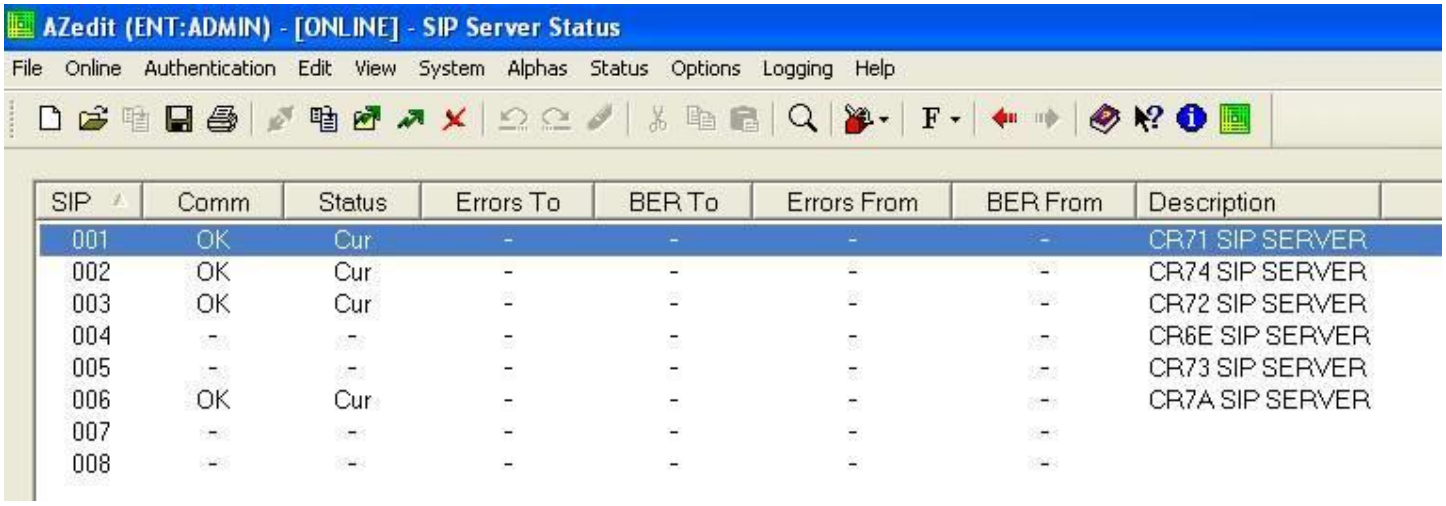
Begin testing by opening a command prompt on the VLink server. One-by-one ping the IP addresses for the following and make sure a reply is received: IP address of phone switch or SIP service provider network, optional TIF Tally Display PC, RTS ADAM Primary master controller card, RTS ADAM back-up master controller card, RTS Dante Omneo card. If any of the devices are not pingable, check the IP network configurations and connections.

On the VLink server, using the System Administration program, click client statistics. Make sure the SIP line clients are shown as online. If not, check the configured SIP Provider / Phone switch settings and SIP login information for each line.

Also on the VLink server, maximize the Device Interface program which is running. Make sure all of the device interfaces are shown as Connected. If not, click configure and check the IP address in both fields is the IP address of the VLink server.

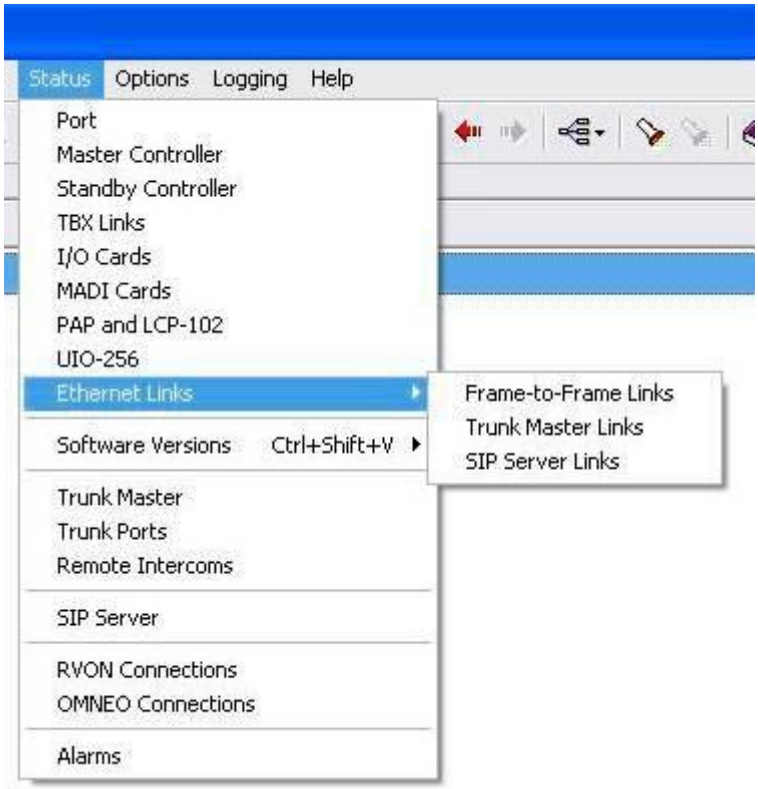
Copyright Bosch Security Systems

If necessary, click EDIT for each of the device interfaces and check the Dante Virtual Soundcard channel mapping. WARNING: NEVER EXIT OR CLOSE THE VLink DEVICE INTERFACE PROGRAM. Always just minimize it when you are done looking at status.



Check the SIP server status in AZEDIT.

When the VLink TIF server is correctly connected for SIP Line Control, you can see the status under Status/SIP server.



You can see more detailed status by going to Status/Ethernet Links/SIP server Links.

Copyright Bosch Security Systems

If status is not shown correctly, check the IP address listed for the VLink TIF server and check the network connection between the VLink and the ADAM Master Controller again.

Place key assignments on any RTS panel for the ports used for the SIP phone lines. Dial into each line from an external phone and check the functionality of auto-answer, manual answer by keypanel, and audio in both directions

Further operational information concerning RTS ADAM control of telephone line interfaces, including those which come from a VLink server is detailed below.

The VLink SIP phone lines are operated from the intercom keypanels, and from the dial pad on the telephone at the remote end of the line. Any keypanel with a keypad may use the VLink SIP phone lines. All that is necessary is to program a key to talk to the VLink SIP phone line, as if it were a keypanel. The alpha numeric display or tally LED for that key then provides information about the phone line. A solid display or non-illuminated LED indicates a line which is not in use. A slow flash indicates a line which is in use (off-hook). A rapidly flashing display or LED indicates a line which is ringing. In addition, the alpha numeric display shows digits as they are dialed, and the LED flashes for each digit.

NOTE: Displayed tallies are different if the Don’t Generate Tallies for TIF or Trunk Use option has been selected in Options|Intercom Configurations|Options.

To use a VLink SIP phone line, either to answer a call, or to call out, you first need to program a key to talk to the VLink SIP phone line. This is accomplished in the same manner as programming a key to talk to a keypanel. To program a key by port number, enter NUM-nnn_PGM-t, where NUM is the number 1 key, nnn is the port number of the TIF-4000 you want to use, and t is any talk key. You also need to use the listen key, so it should be assigned as either AF (auto-follow) or AL (auto-listen).

NOTE: The VLink SIP phone lines only respond to commands which are sent via a point-to-point key assignment. If you wish to use the VLink SIP phone line primarily on a PL, you must add a point-to-point assignment as the L2 talk assignment on the talk keys which are going to either answer the line, or dial out on the line.

Dialing a Call To dial a call on a VLink SIP phone line using a or KP-32, do the following: 1. Turn on the listen key for the line you wish to dial on. This allows you to hear dial tone, and your DTMF dialing tones. 2. Enter dial mode by entering PHONE-PGM-T. 21 PHONE is the 4 button on the keypad. PGM is on the keypad, and T is the talk key which is

Copyright Bosch Security Systems

programmed to talk to the TIF-4000 you are dialing on. Leave the talk key in the latched position as you dial the number. 3. Dial the number. As you enter each digit, it appears in the alpha display above the key you are dialing on. If the listen key is latched, you hear each DTMF tone as it is generated. 4. When you have completed dialing, momentarily turn off the talk key to exit dial mode. The alpha numeric display reverts to normal, and you may use the key and keypad in the normal manner. NOTE: Digits 0-9 generate the DTMF digits 0-9. PGM generates the #, and CLR generate * (# and * are displayed for these keys). It is necessary to press CLR twice if you wish to generate an *, as a single CLR is used to trigger the speed dial and redial features.

To dial a call on a VLink SIP phone line using a KP-12 or KP-32, do the following: 1. Tap the phone key to begin your call. This places the keypanel in dial mode: the CALL indicator turns on, and the MAN DIAL (manual dial) displays in the call waiting window. You should also hear the dial tone. NOTE: You can hang up the phone line at this time by simply tapping the phone key again. 2. Tap SEL (select) to select MAN DIAL. The twelve intercom keys can now be used to dial a telephone number. Each key corresponds to the number printed next to it on the front of the panel. If the keypanel has alphanumeric displays, the key numbers are displayed above each key. 3. Begin dialing the number by tapping the appropriate keys. After you dial the first digit, END DIAL appears in the call waiting window. 4. When you have completed the dialing, tap SEL to select END DIAL. This returns the keypanel to normal operating mode. If the called party answers, proceed with your conversation.

Hanging Up

The VLink SIP line control detects the call at the far end has hung up under most circumstances. It detects the hang up by either loop interrupt, battery reversal, or the presence of a dial tone or busy signal. Some telephone systems do not provide any of the above, so it is necessary to force a hang up. In addition, if the call was placed to an auto-answer device, it is necessary to force a hang up when the call is complete.

Enter PHONE-CLR-t, where PHONE is the 4 on the keypad, CLR is the CLR button, and t is the talk key which is programmed to talk to the VLink SIP phone line which you want to hang up. This disconnects the line for which you struck the talk key. NOTE: If talk is in the on position, you must turn off the key, then momentarily turn it on again to indicate which line you wish to disconnect. If the line is in dialing mode, then you must first exit dialing mode by turning off the key, then use PHONE-CLR-t to hang up.

Copyright Bosch Security Systems

5. 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.

5.1 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

5.2 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 ‘rts’ and Password of ‘vlink’. If a different port #, Username or Password is desired, these items can be changed in this configuration file.

Copyright Bosch Security Systems

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 VLink Server
8. To have the VLink 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.

Copyright Bosch Security Systems

6. Video Media Server

The VLink 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.

6.1 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
```


Copyright Bosch Security Systems

6.2 STUN Server

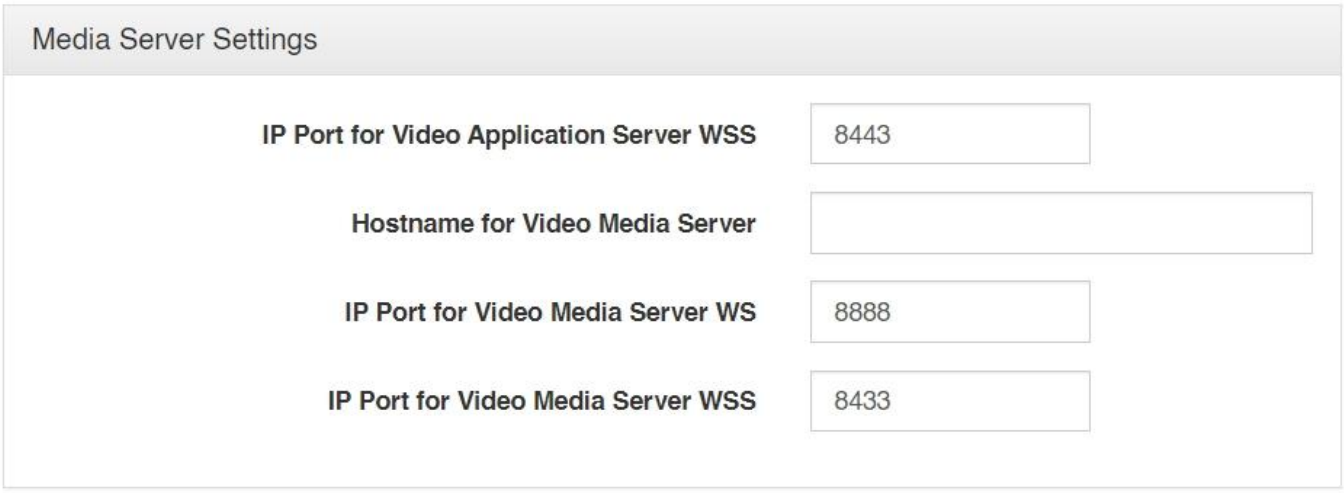
If the Media Server is deployed behind a NAT it is necessary to configure the Media Server to use a STUN server. Follow the steps below to configure the Media Server to use Google's public STUN server.

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`

6.3 Configuration



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.

Copyright Bosch Security Systems

7. System Administration

7.1 Logging In

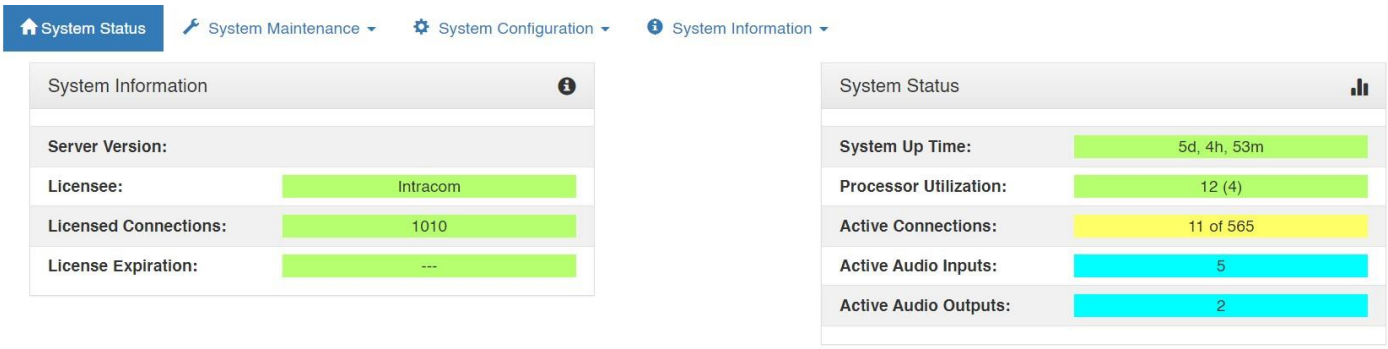
If you are using the VLink System Administration from the same machine VLink is installed on:
After VLink Virtual Matrix is installed on the machine, a shortcut will be placed on the desktop called ‘VLink System Administration.’ Click on the shortcut. A browser window will appear. The VLink System Administration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

If you are using the VLink System Administration from a different machine:
Open a browser window and type the local IP address of the machine running VLink 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’.

Copyright Bosch Security Systems

7.2 System Status



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 VLink Virtual Matrix has been running in days, hours, and minutes.

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

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

Copyright Bosch Security Systems

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 VLink Control Panels, VLink 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.

Copyright Bosch Security Systems

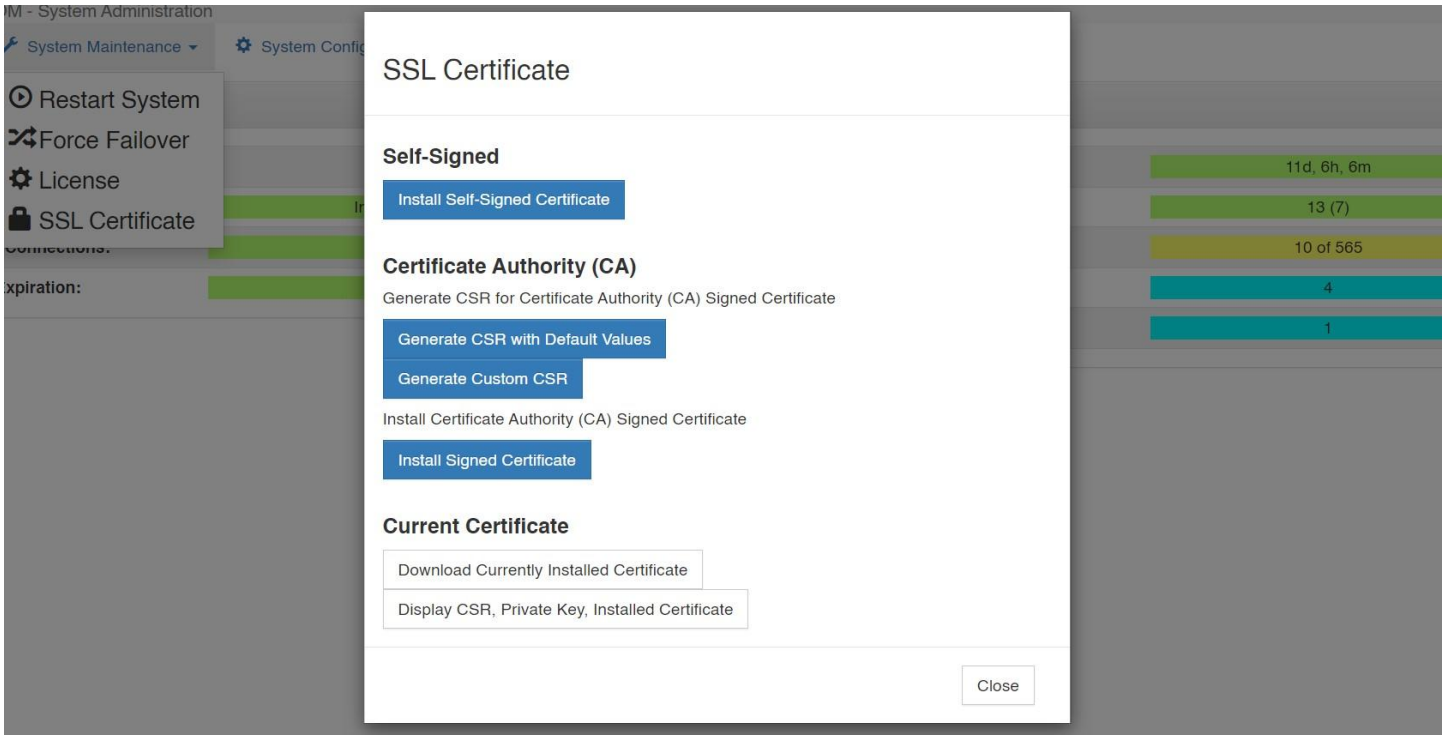
7.3 System Maintenance

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.

7.3.1 SSL Certificate



VLink Virtual Matrix generates its own self-signed certificate upon initial launch. All data transmitted between the VLink Virtual Matrix and the System Administration as well as the VLink 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 VLink server.

Copyright Bosch Security Systems

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.

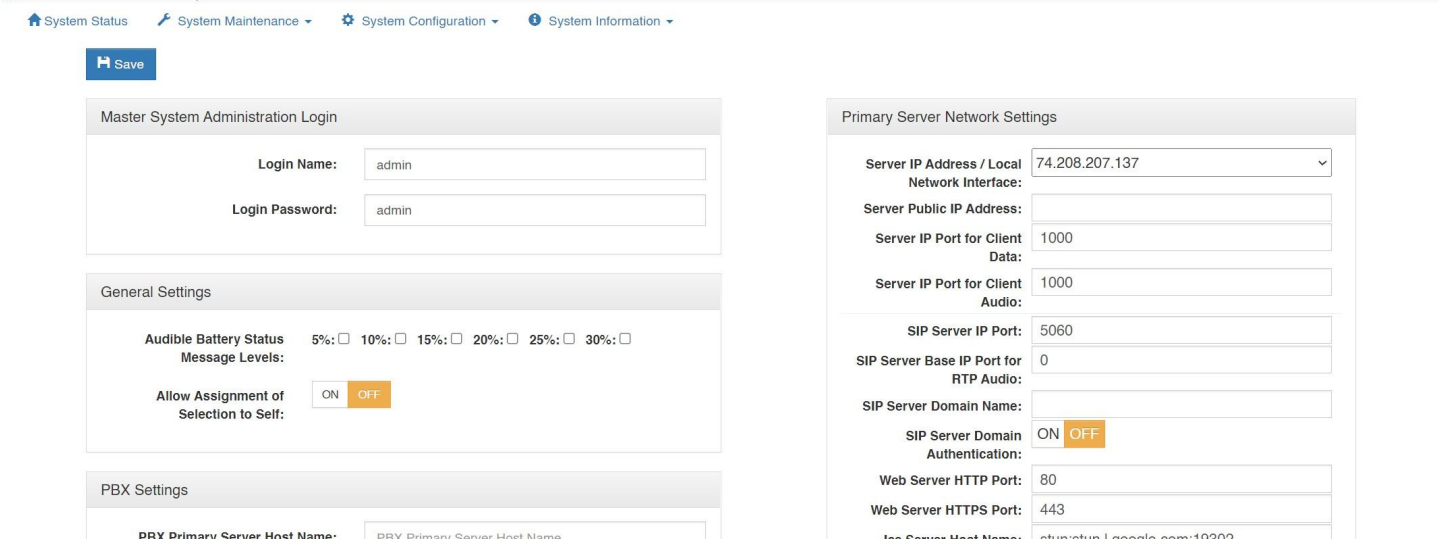
Generate Custom CSR: Prompts the user for Domain name(s), Organization Name, County Name, and State/Province. These values are used to generate a CSR to send to a Certificate Authority.

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

Copyright Bosch Security Systems

7.4 System Configuration

7.4.1 System Settings



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

Copyright Bosch Security Systems

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 VLink 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 VLink 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 VLink 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.

Copyright Bosch Security Systems

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 VLink 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 VLink Client Data / Audio: The Server IP Port for Client Audio under ‘Server IP Port for VLink 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 VLink will use to establish a secure websocket with the Video Application Server.

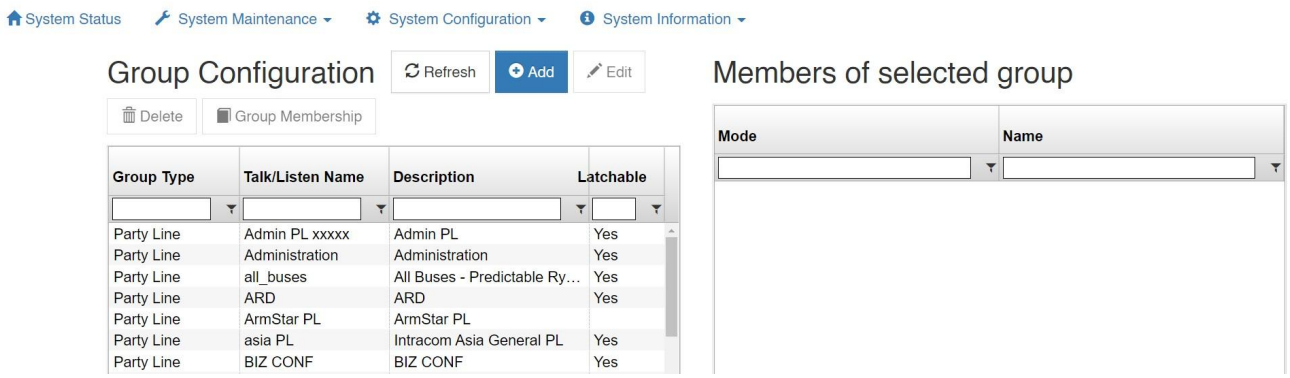
Copyright Bosch Security Systems

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 VLink will use to establish an unsecure websocket with the Media Server.

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

7.4.2 Group Configuration



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.

Copyright Bosch Security Systems

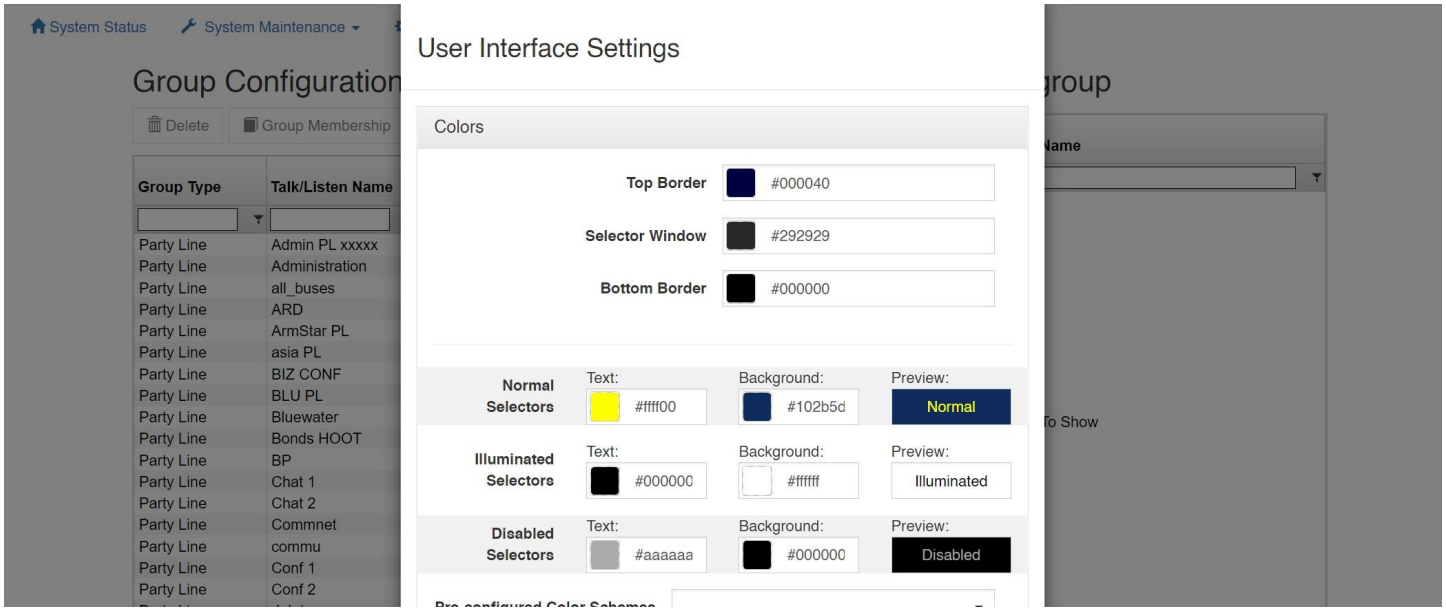
Type: Choose from the drop down box ‘Party Line’ or ‘Fixed Group’

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.

7.4.3 User Interface Settings



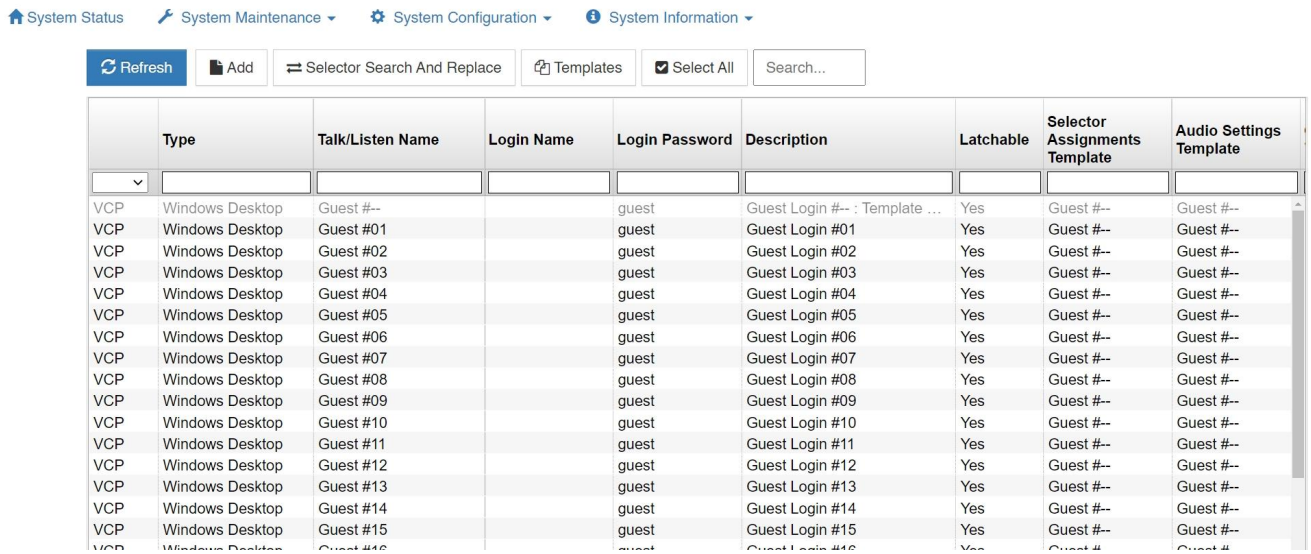
This allows customizations of the VCP GUI such as the Colors (Background and Text), Selector Spacing, and 24-bit PNG graphic files that can be uploaded such as a logo.

7.4.4 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.

Copyright Bosch Security Systems

7.5 Client Configuration



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.

Copyright Bosch Security Systems

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 VLink Control Panels, Device Interfaces, Two-Way radios, and SIP devices.

Category	Client Type	Purpose
VLink Control Panel	VCP: Windows Desktop	For logging into the VLink (WebRTC) Control Panel on Windows
VLink Control Panel	VCP: Apple iOS	For logging into the VLink (WebRTC) Control Panel on iOS
VLink Control Panel	VCP: Google Android	For logging into the VLink (WebRTC) Control Panel on Android
VLink Control Panel	VCP: Apple MAC	For logging into the VLink (WebRTC) Control Panel on Mac
VLink Control Panel	VCP: Linux	For logging into the VLink (WebRTC) Control Panel on Linux
VLink Device Interface	VDI: Four-Wire Interface	For logging into the VLink Device Interface
VLink Device Interface	VDI: 2-Way Radio Interface	For logging into a VLink 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 VLink
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 VLink
SIP	SIP: Direct IP Trunk	Enables a connection between PBX/SIP Servers and VLink using IP settings
SIP	SIP: Registered Trunk	Enables a connection between PBX/SIP Servers and VLink using Registration of clients
SIP	SIP: Four-Wire Interface	Enables connection of a SIP based Four Wire Interface to transport audio into VLink
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
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.

Copyright Bosch Security Systems

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 VLink 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 VLink Login Password becomes obsolete because the VLink 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. VLink 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 VLink Control Panel that is configured to hide the off-line selectors. It is generally used for VLink Device Interface clients that should, under normal operation, never go off-line thus allowing VLink 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.

Copyright Bosch Security Systems

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.

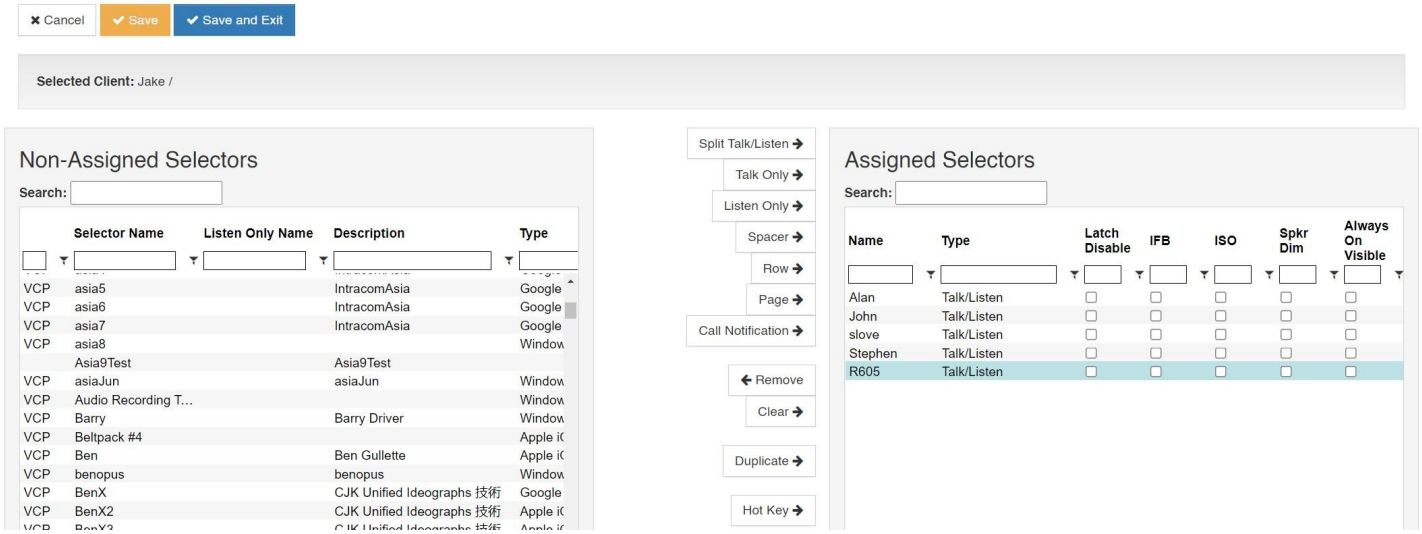
Master System Administration Privileges: Gives Master System administrator privileges to the client.

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

Copyright Bosch Security Systems

7.5.1 Selector Assignments



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.

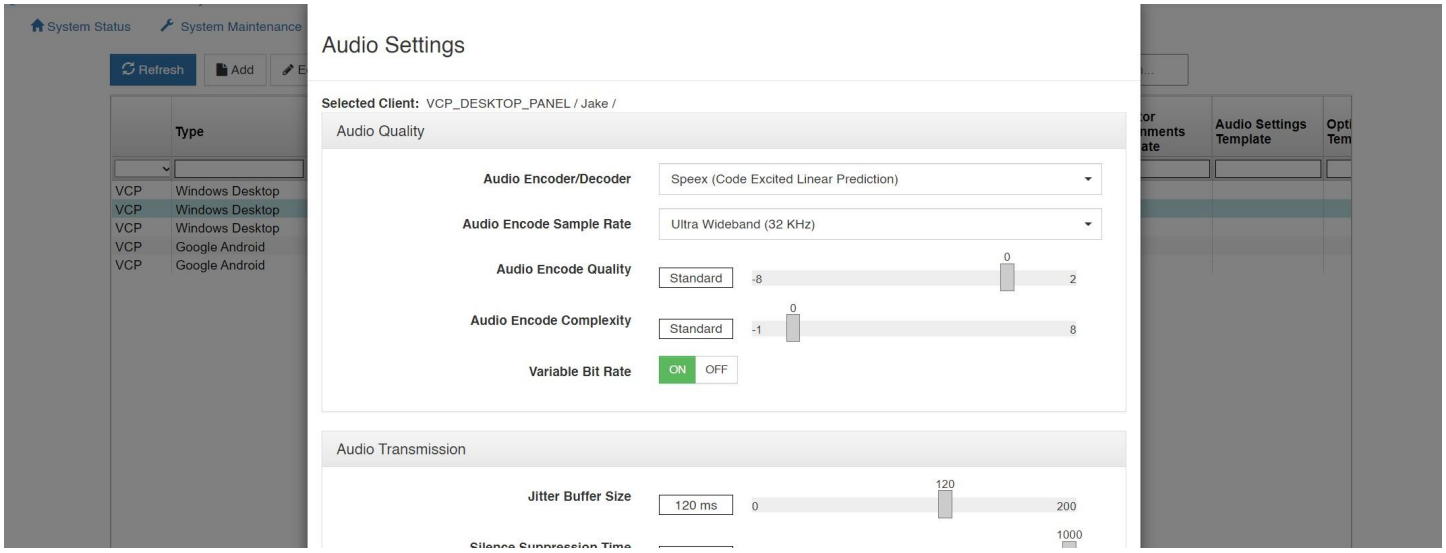
Remove: Highlight a selector in the right-hand portion of the screen and select 'Remove' to delete an assigned selector.

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 VLink Control Panel. This option is only supported on the VLink Control Panel for Windows.

Copyright Bosch Security Systems

7.5.2 Audio Settings



Audio Quality Audio Encoder/Decoder: This setting allows selection of a different encoder/decoder. For VLink Control Panels and VLink 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 VLink 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 VLink 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.

Copyright Bosch Security Systems

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

Copyright Bosch Security Systems

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.

Copyright Bosch Security Systems

7.5.3 VLink Client Configuration Options

screenshot of vlink system administration client configuration options menu

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)

Copyright Bosch Security Systems

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.

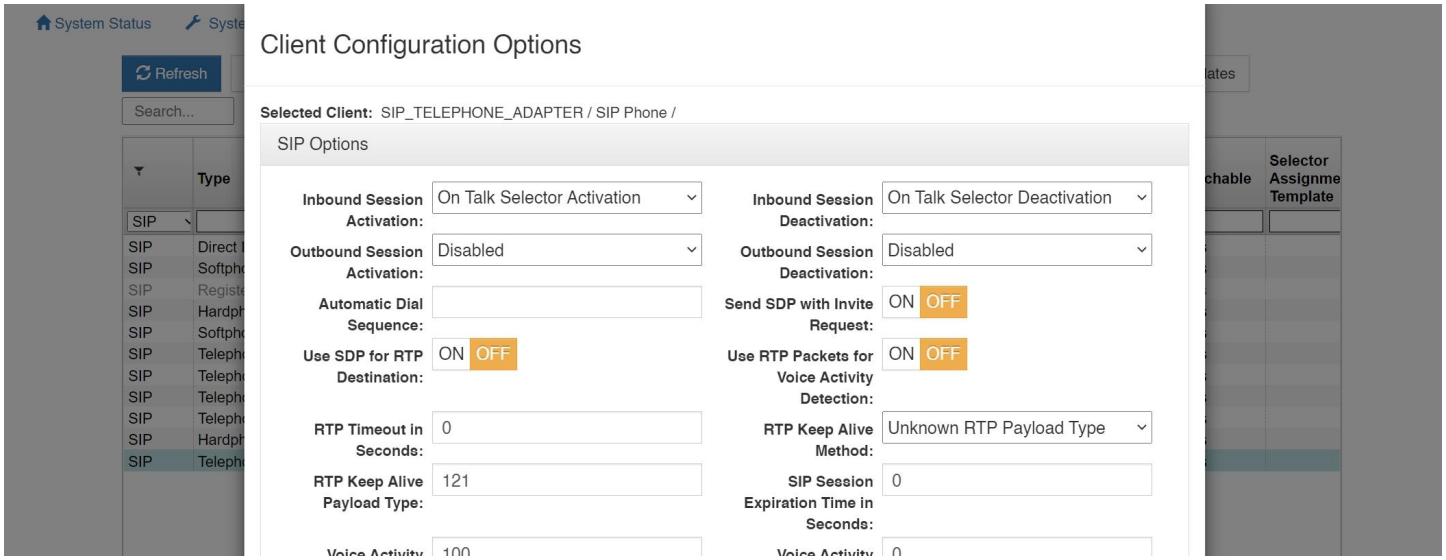
Copyright Bosch Security Systems

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.

7.5.4 SIP Client Configuration Options



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 VLink 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 VLink 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 VLink 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 VLink Control Panels deactivate the talk selectors associated with the SIP Client.

Copyright Bosch Security Systems

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 VLink 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 VLink 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 VLink 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.

Copyright Bosch Security Systems

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 VLink 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.

Copyright Bosch Security Systems

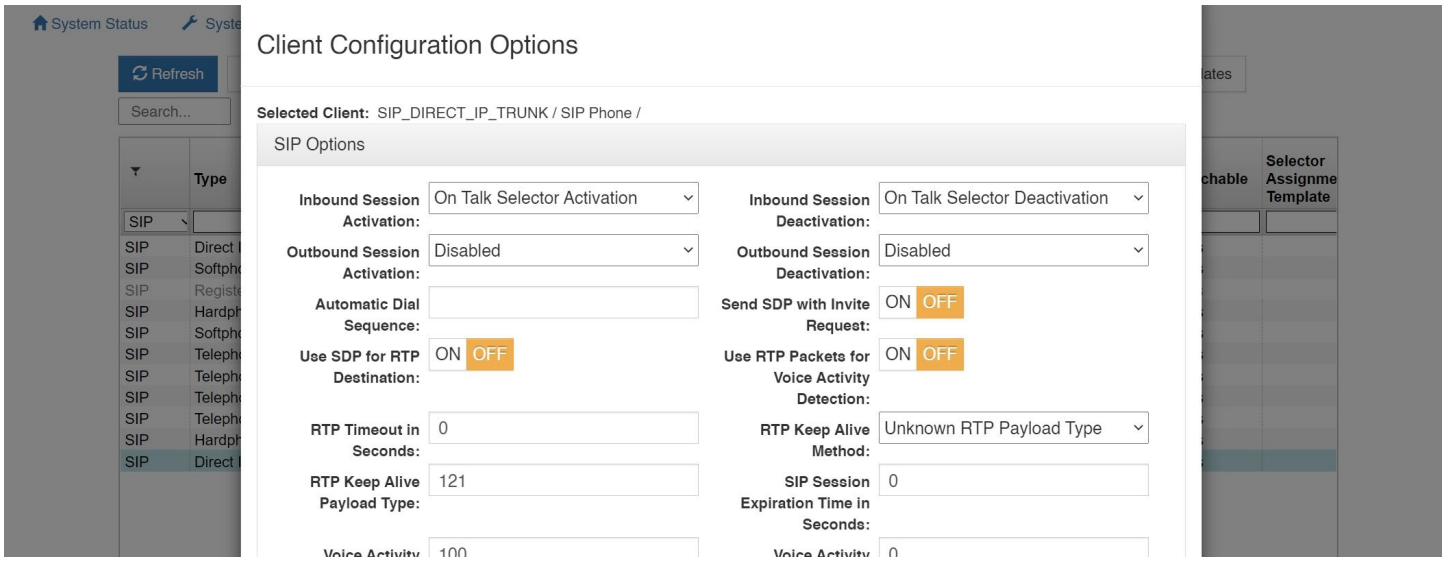
Auto-Answer Delay Time In Ms: This option sets the delay time in milliseconds after which the VLink Virtual Matrix will automatically answer a received SIP call. Typically this value will be set to zero such that the call is answered immediately. In some situations it is desirable to delay answering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

7.5.5 SIP Direct IP Trunk and Registered Trunk Options



In most situations, the VLink 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 VLink 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:

Copyright Bosch Security Systems

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 VLink 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.

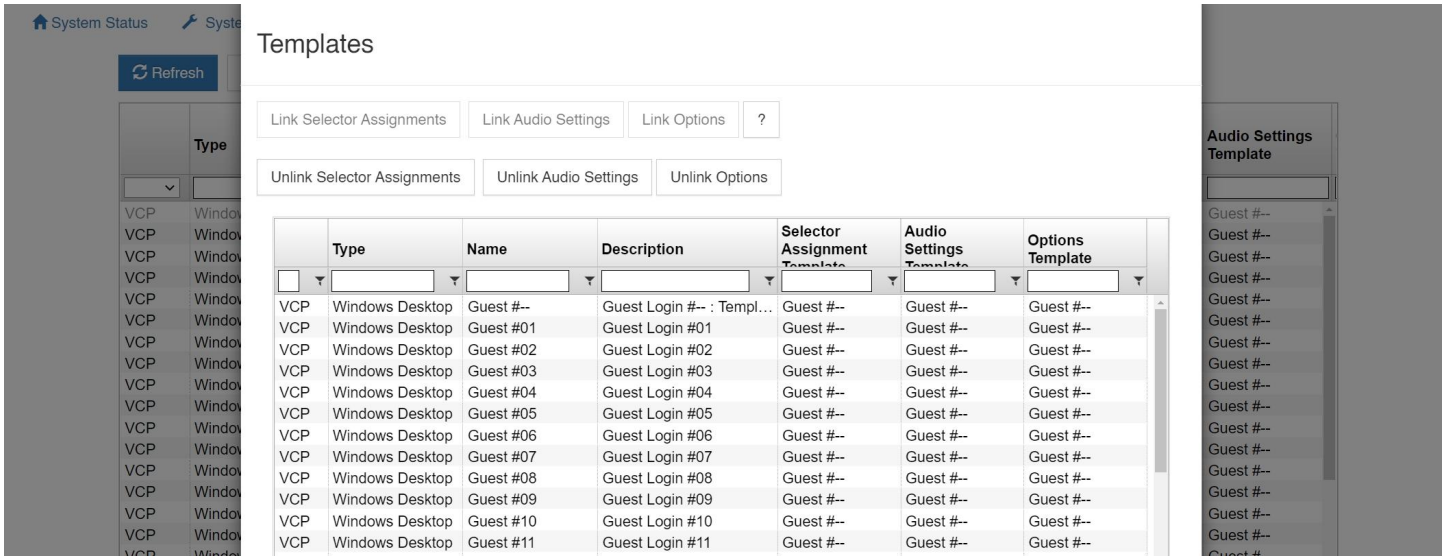
STUN Server or Proxy IP Address: This option enables SIP client transversal through a NAT by specifying the IP address of a STUN Server which will inform the Virtual Matrix of the public IP address of the SIP Client so that it can be included when sending SIP registration and SIP invite requests.

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.

Copyright Bosch Security Systems

7.5.6 Templates



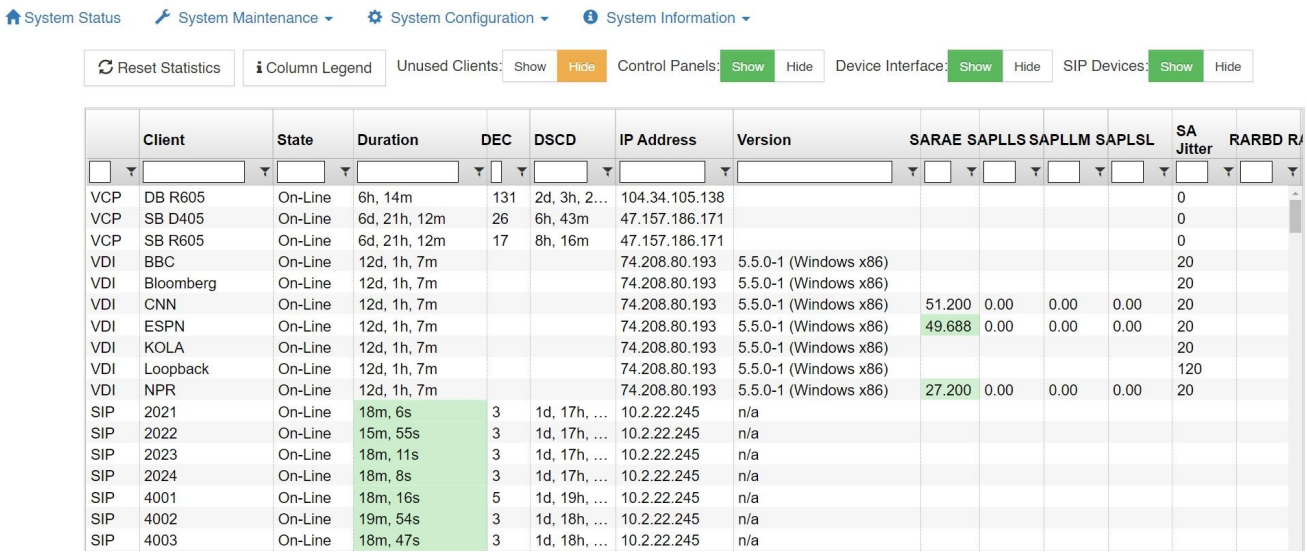
Templates allow you to apply a given client’s selector assignments, audio settings, and/or options to one or more other clients.

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.

Copyright Bosch Security Systems

7.6 System Information

7.6.1 Client Statistics



	Client	State	Duration	DEC	DSCD	IP Address	Version	SARAE	SAPLLS	SAPLLM	SAPLSL	SA Jitter	RARBD
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.

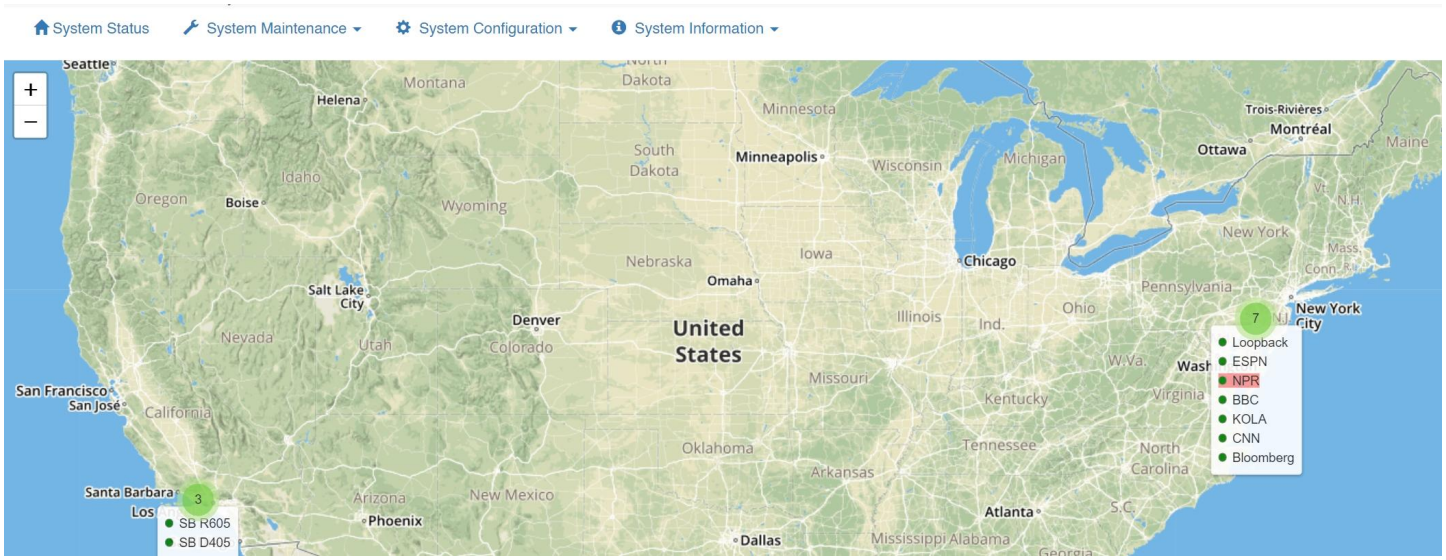
Click the ‘Column Legend’ button in the upper, left-hand side of the ‘Client Statistics’ page to display the legend.

7.6.2 SIP Registrations

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

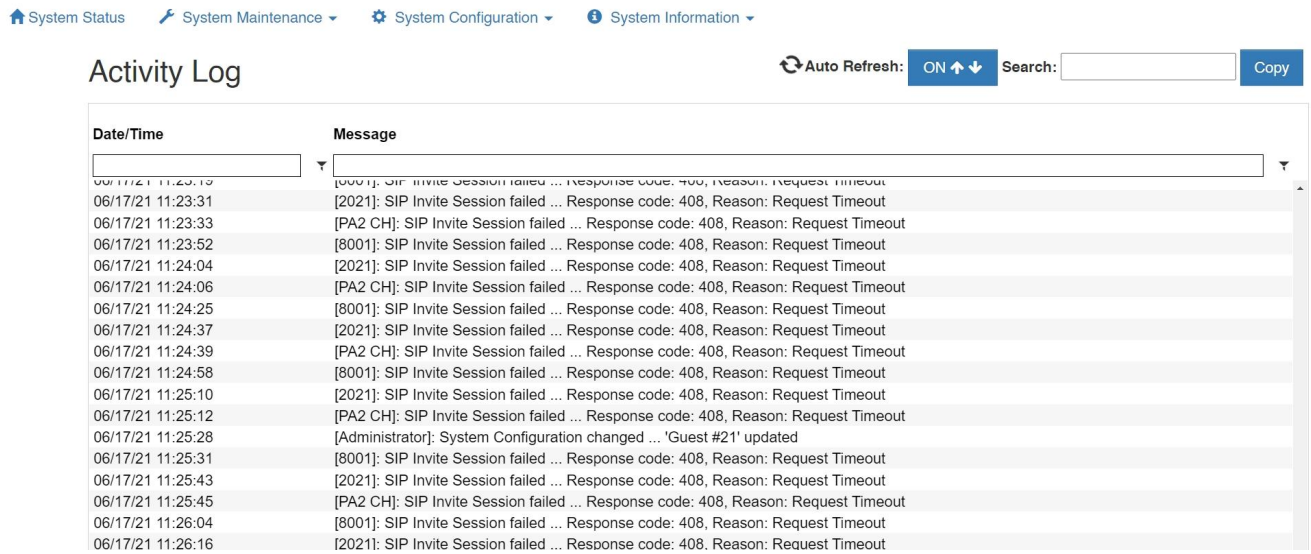
Copyright Bosch Security Systems

7.6.3 Geolocation



Displays the approximate locations of clients on the system. For VLink 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.

7.6.4 Activity Log



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

Copyright Bosch Security Systems

8. Failover Capability

In any mission critical communications system it is imperative to have built in redundancy. VLink 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.

8.1 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 VLink 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 VLink 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 VLink 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.

Copyright Bosch Security Systems

8.2 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 VLink clients the primary server will deactivate itself forcing all remaining clients to connect to the secondary server.

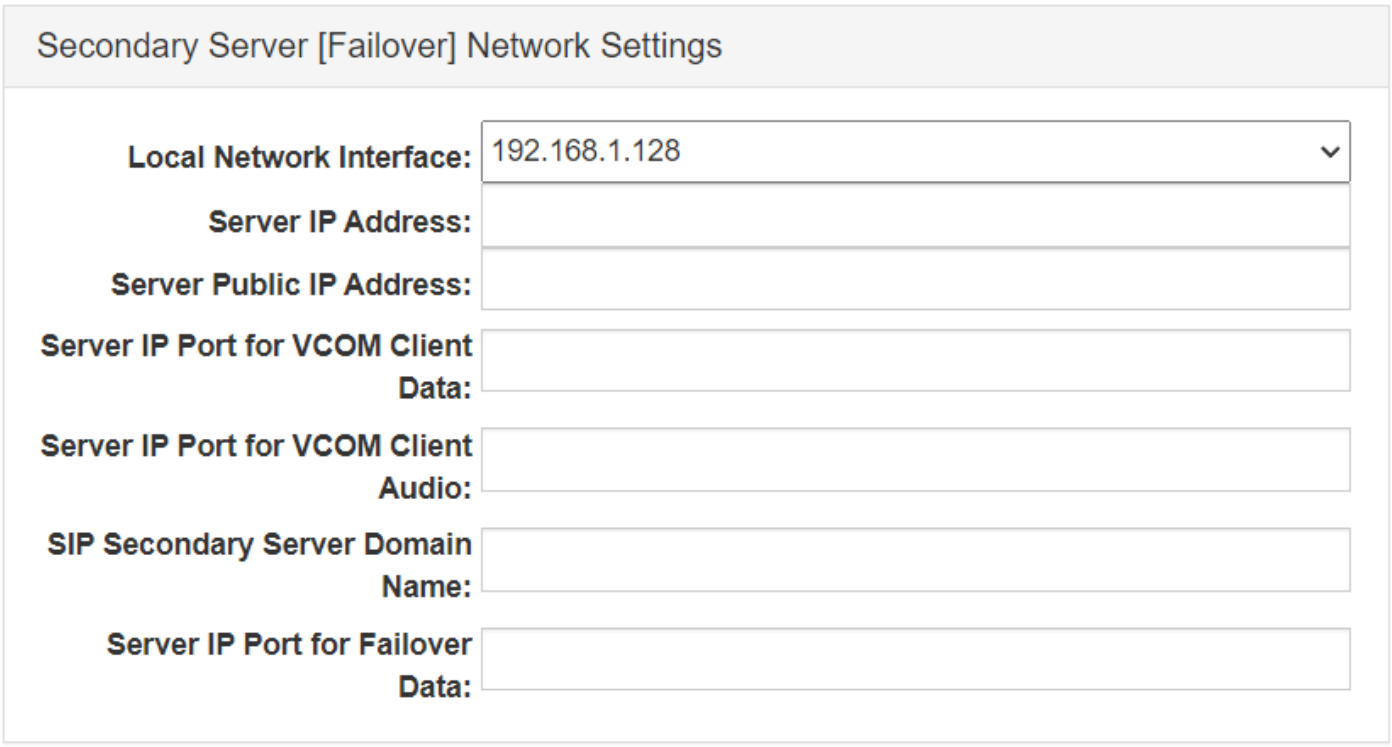
Communication link between primary and secondary servers is not lost but partial failure of network infrastructure:
In this scenario, the partial network failure may result in the loss of a large portion of the VLink clients. In this case the primary server will inform the secondary server to activate 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.

8.3 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.

Copyright Bosch Security Systems

8.4 Setup



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 VLink Client Data and Server IP Port for VLink 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.

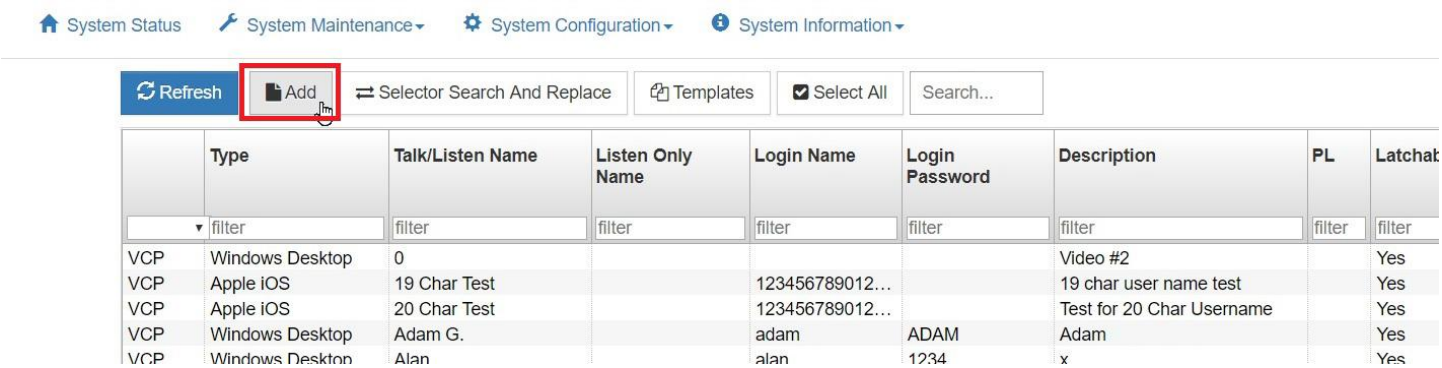
Copyright Bosch Security Systems

9. Connecting SIP Lines

Purchasing SIP Lines

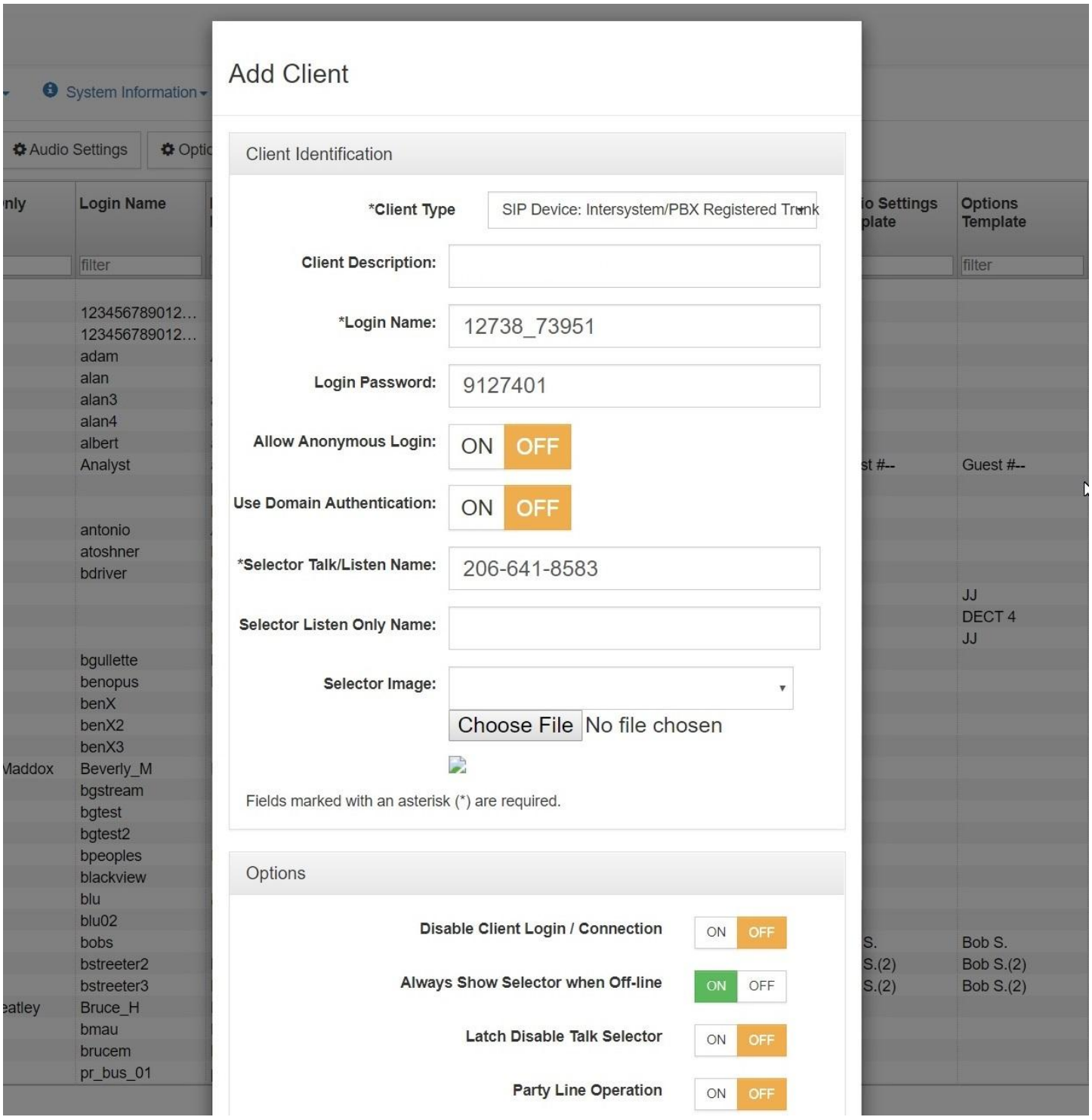
RTS Systems does not provide SIP lines. The lines must be purchased through a 3rd party phone line provider. VLink can connect to SIP lines using a Direct IP Trunk or a Registered Trunk. If you use a Direct IP Trunk SIP Server Domain Authentication must be disabled in the System Settings. A Registered Trunk is the preferred method and will be covered in this guide. VLink 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 VLink System Administration under the System Configuration tab click Client Configuration.



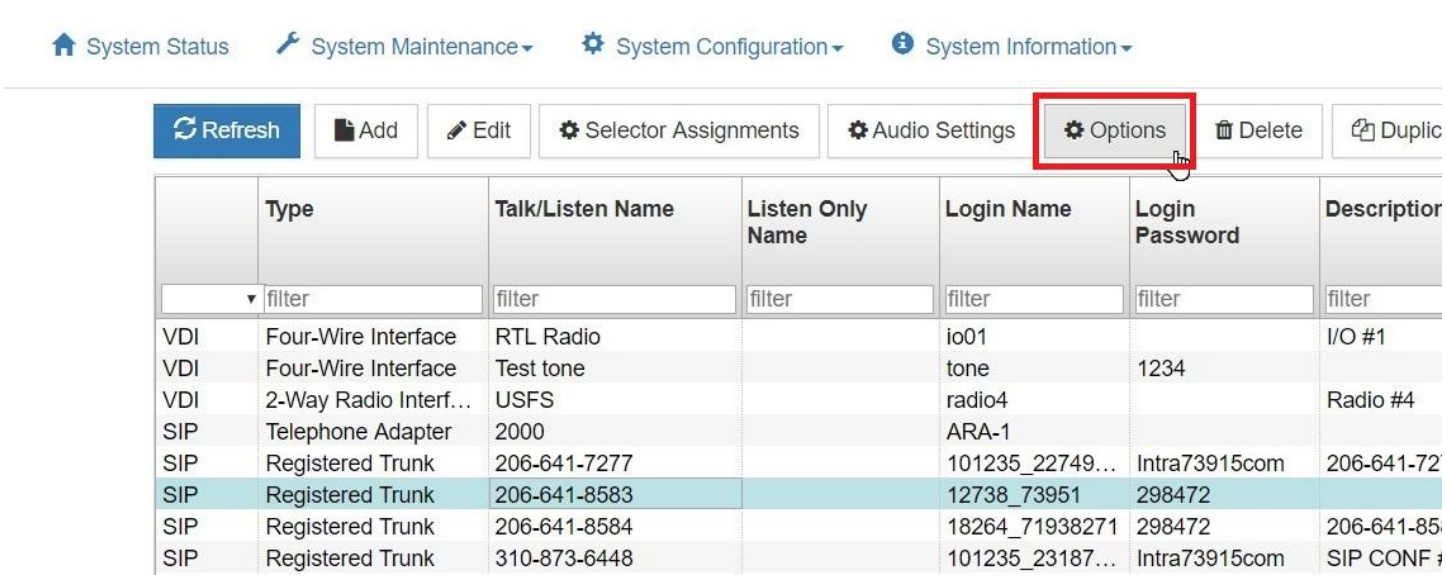
Click Add.

Copyright Bosch Security Systems

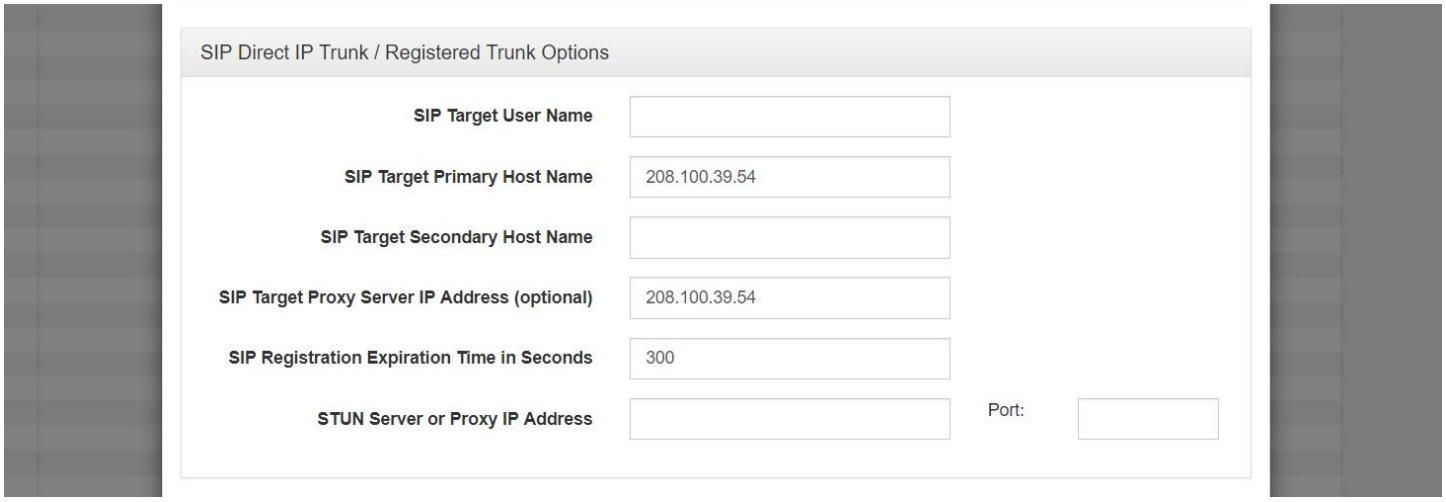


On the Client Type drop-down menu select “SIP Device: Intersystem/PBX Registered Trunk”. For Login Name enter in the username given by your SIP provider. The Login Password will be the password you set up with the SIP provider. In the screenshot above the Selector Talk/Listen Name is set to the phone 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.

Copyright Bosch Security Systems



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



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.

Copyright Bosch Security Systems

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 VLink 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 VLink 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 VLink Control Panels listening to that line will hear a ring signal.

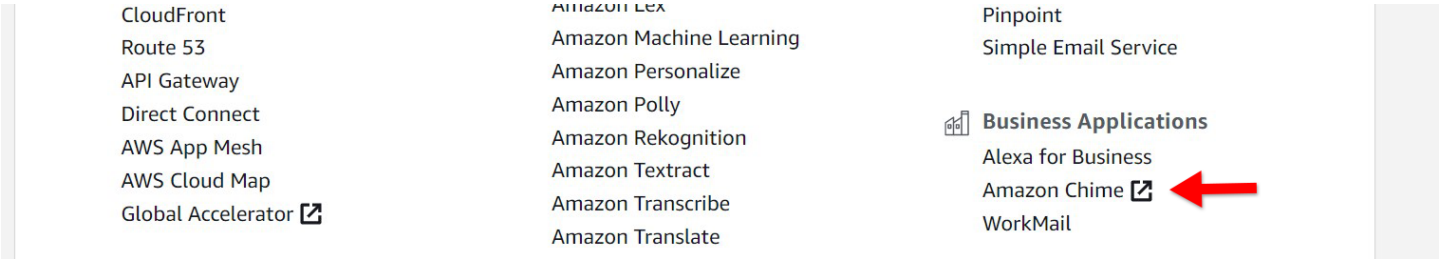
Using the SIP Client You will need to assign the SIP client's selector to a Control Panel in order to talk or listen on the SIP line. Documentation on how to do this is available here. In order to dial out on the SIP line you will also need to set Enable Dial Pad Buttons to On in the client Options.

Copyright Bosch Security Systems

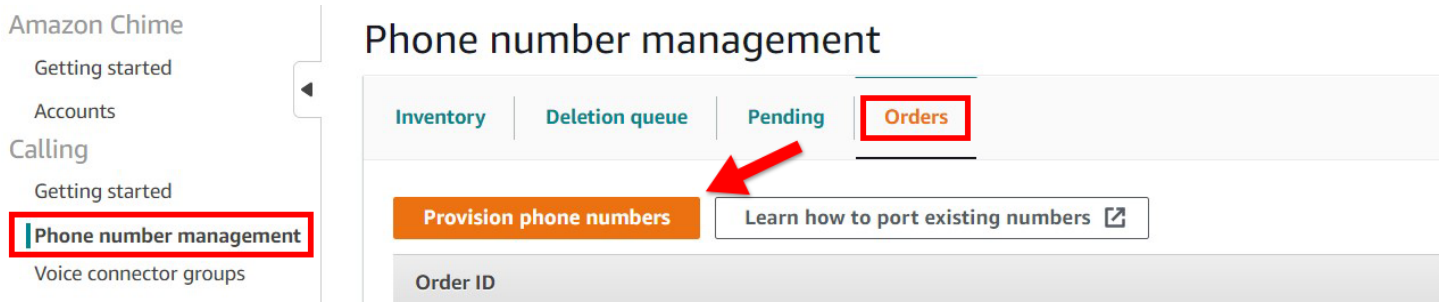
10. Connecting AWS Chime SIP Lines

10.1 AWS Settings

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

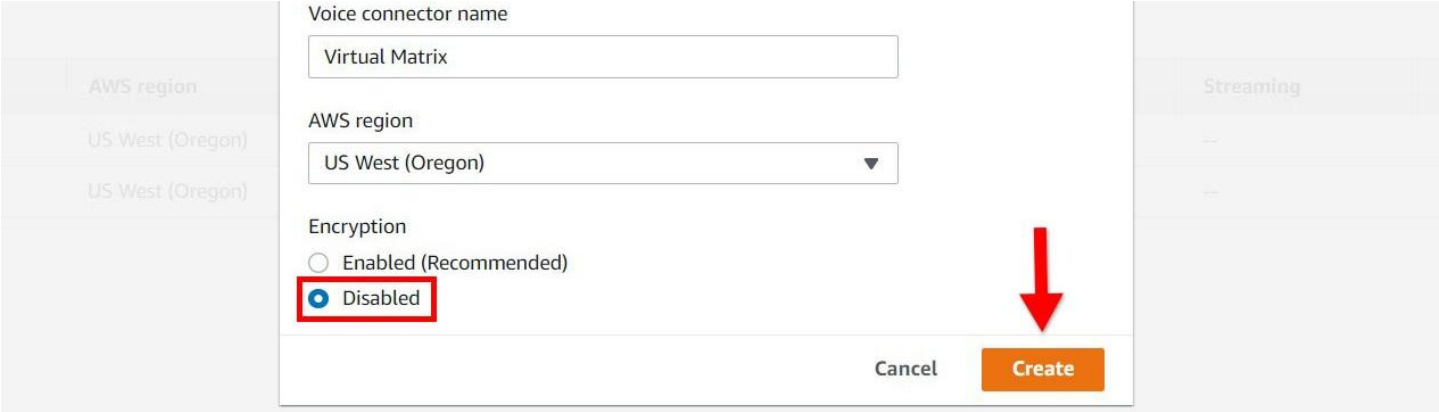


From the AWS Management Console navigate to the Business Applications section and select Amazon Chime.



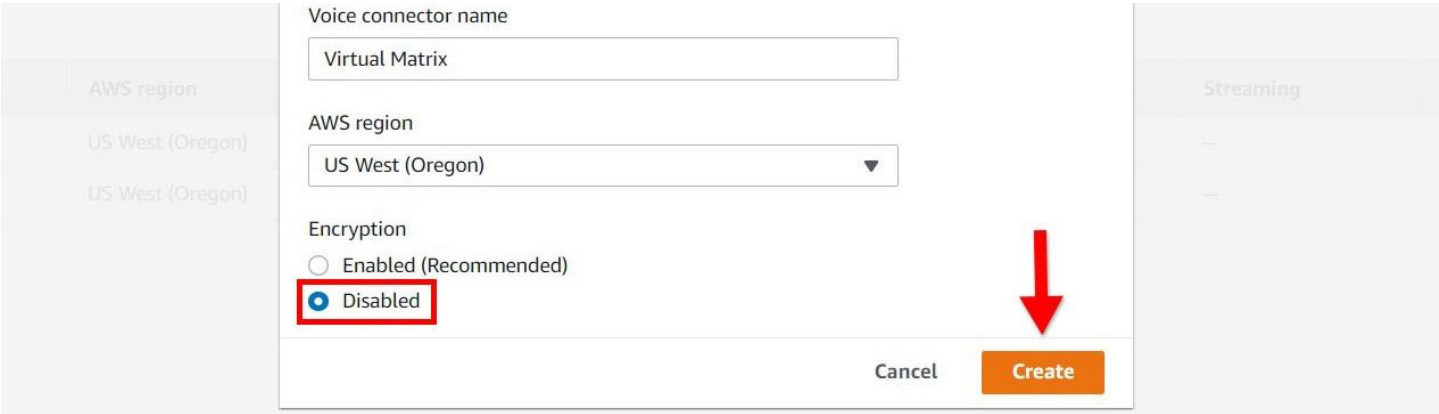
On the left select Phone number management, select the Orders tab and then click Provision phone numbers.

Copyright Bosch Security Systems



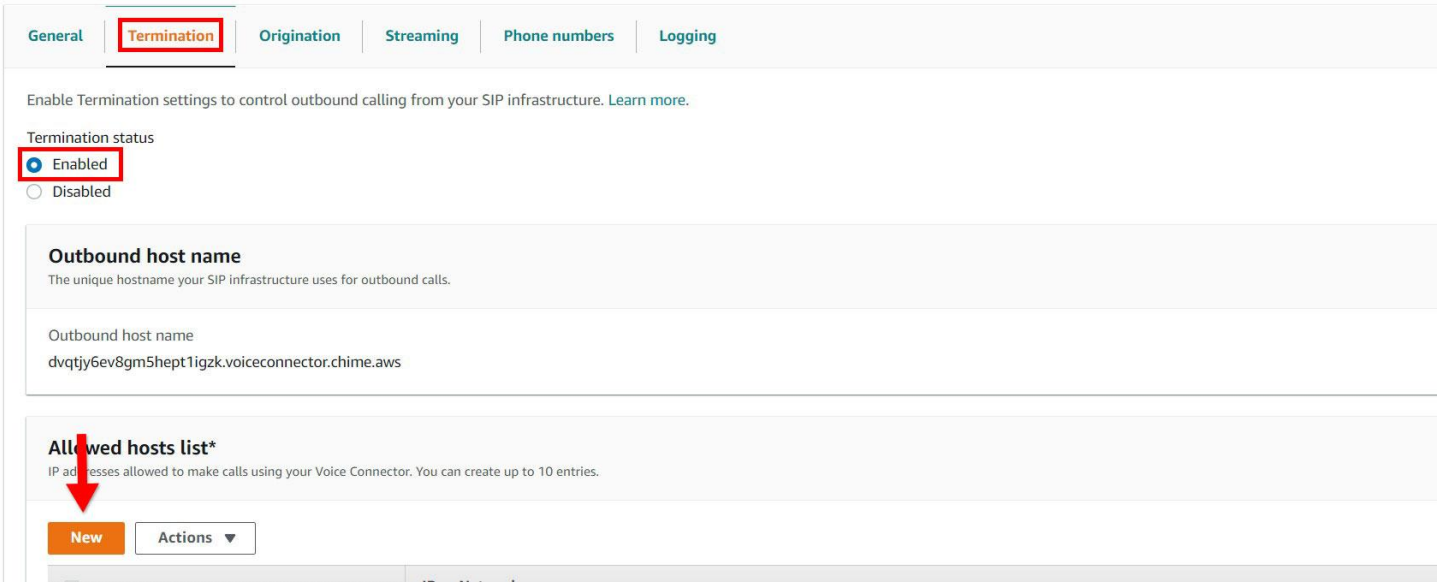
Select Voice Connector and then click Next. Follow the prompts to purchase a phone number.

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

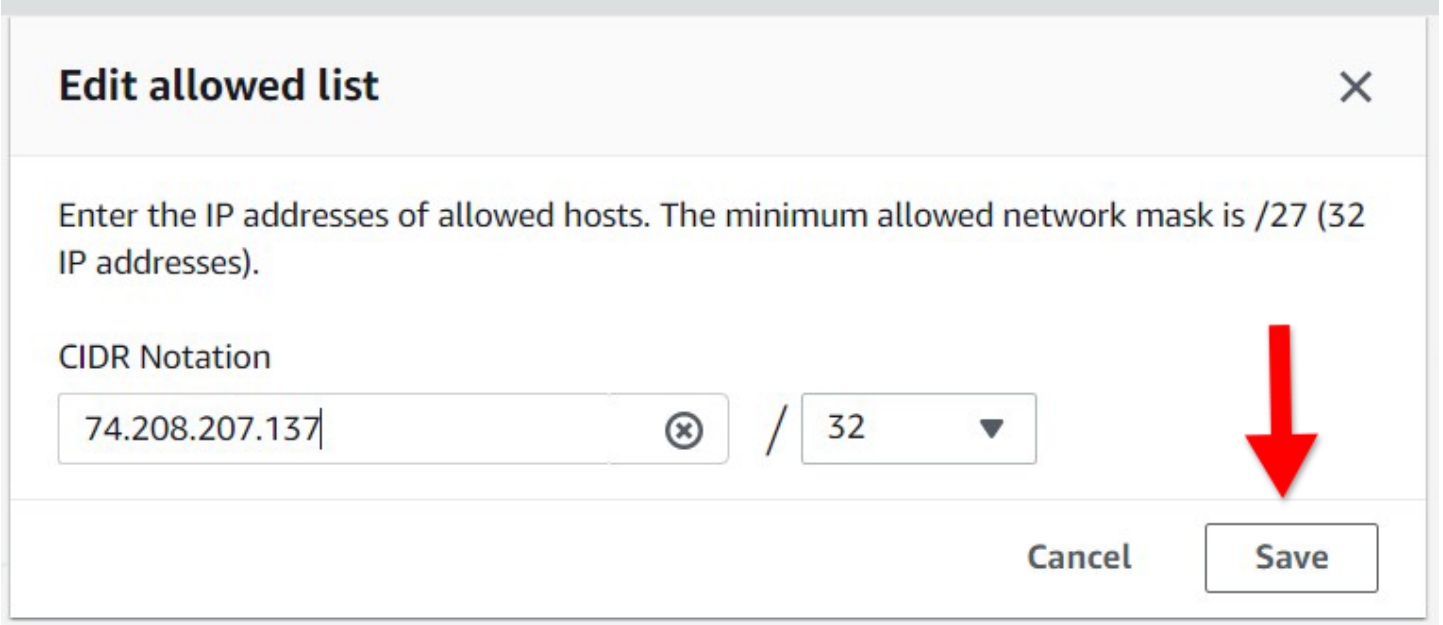


Enter a name for your Voice Connector and Disable Encryption then click Create.

Copyright Bosch Security Systems



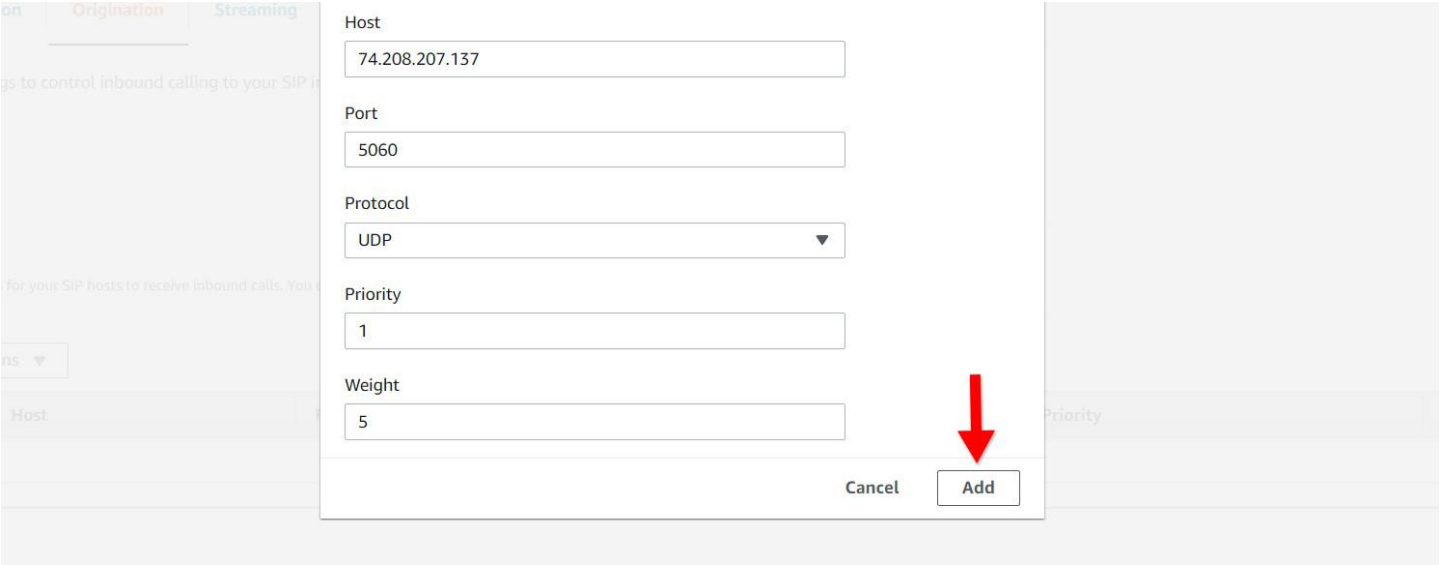
Select your new Voice Connector and navigate to the Termination tab. Set Termination status to enabled and then click New in the Allowed hosts list section.



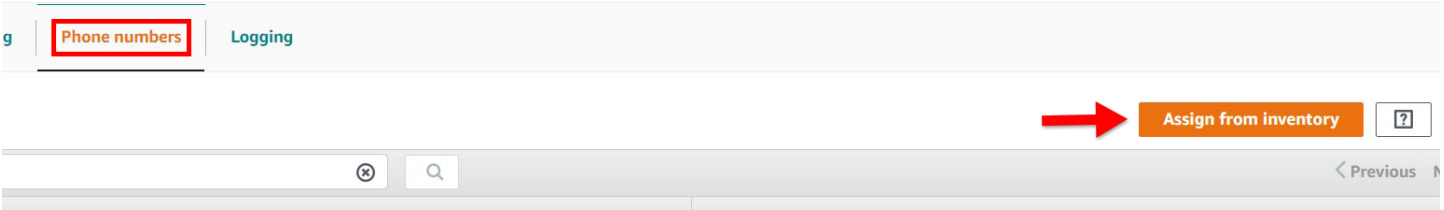
Enter the IP address of your VLink Virtual Matrix server and then click Save. Scroll down to the bottom of the Termination page and click Save.

Copyright Bosch Security Systems

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



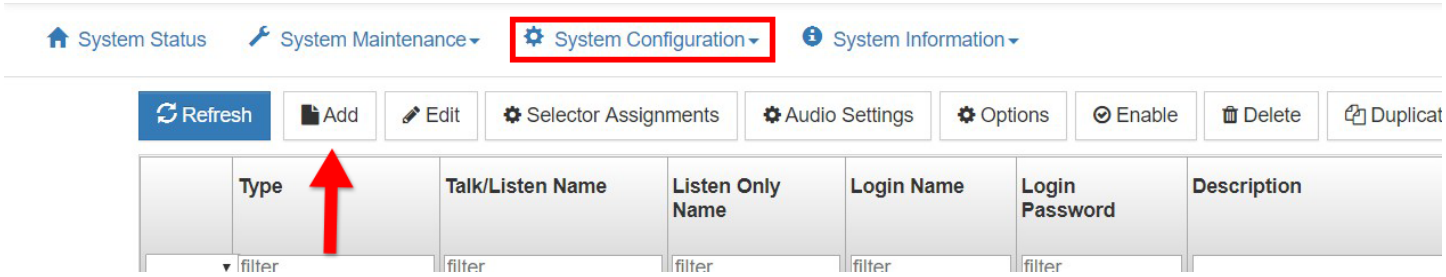
In the Host section enter the IP address of your VLink Virtual Matrix server then fill out the remaining fields as shown then click Add. Scroll down to the bottom of the page and click Save.



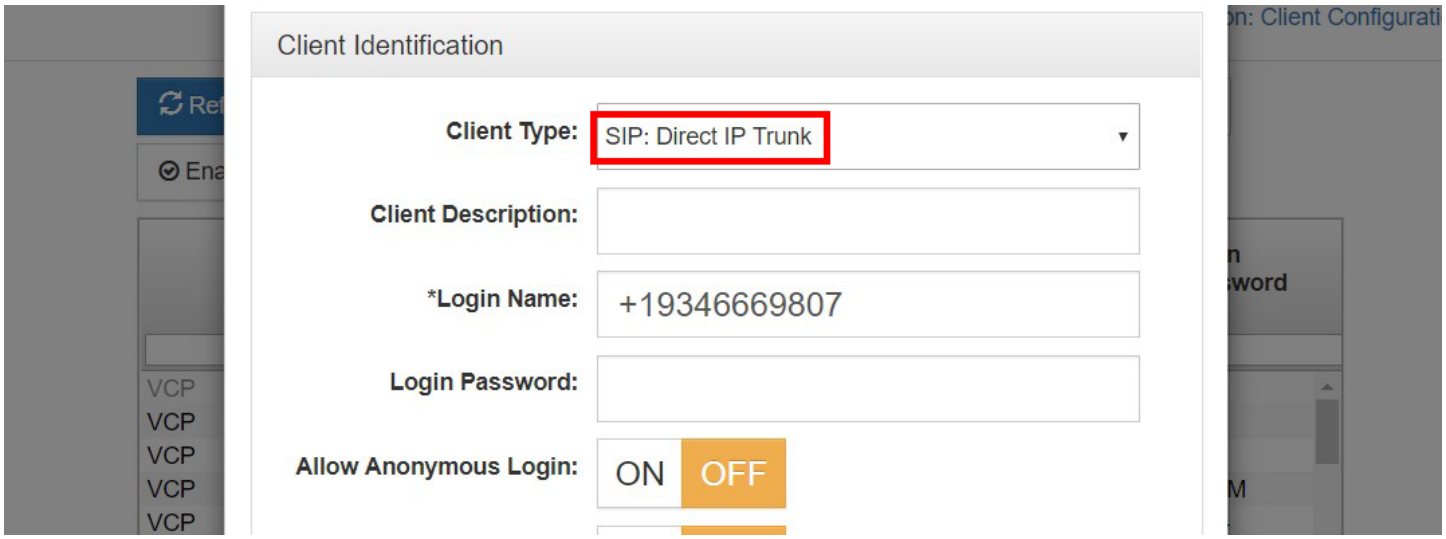
Navigate to the Phone numbers section and then click Assign from inventory. Select your desired phone number and then click Assign from inventory to add the line to the Voice Connector.

Copyright Bosch Security Systems

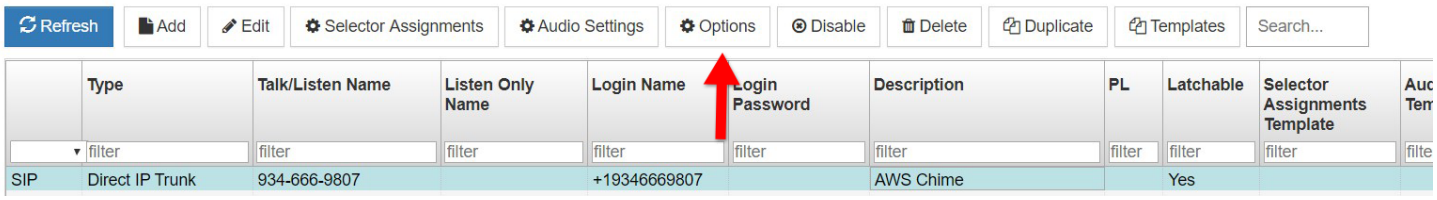
10.2 VLink Settings



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

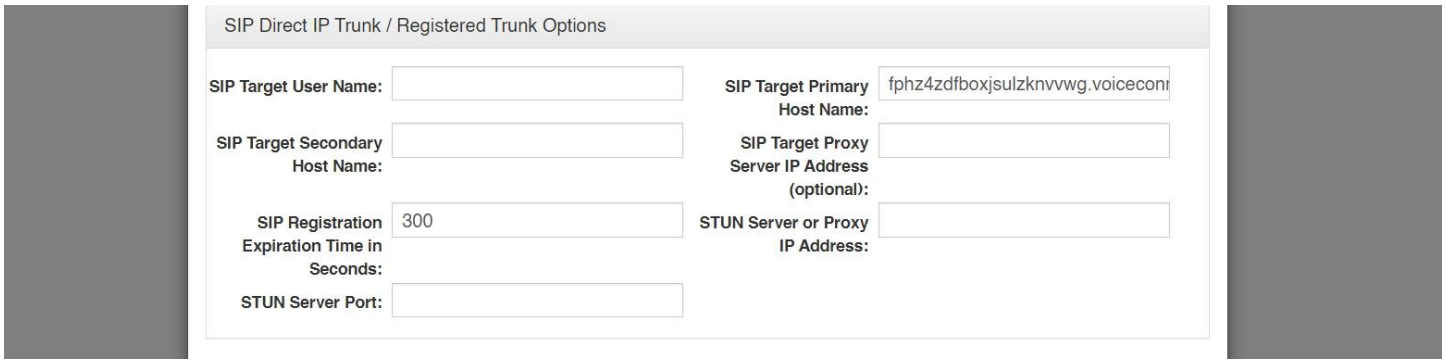


For the Client Type select SIP: Direct IP Trunk and enter the Login Name in the format shown above. Add a Selector Talk/Listen name and then click Save.



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

Copyright Bosch Security Systems



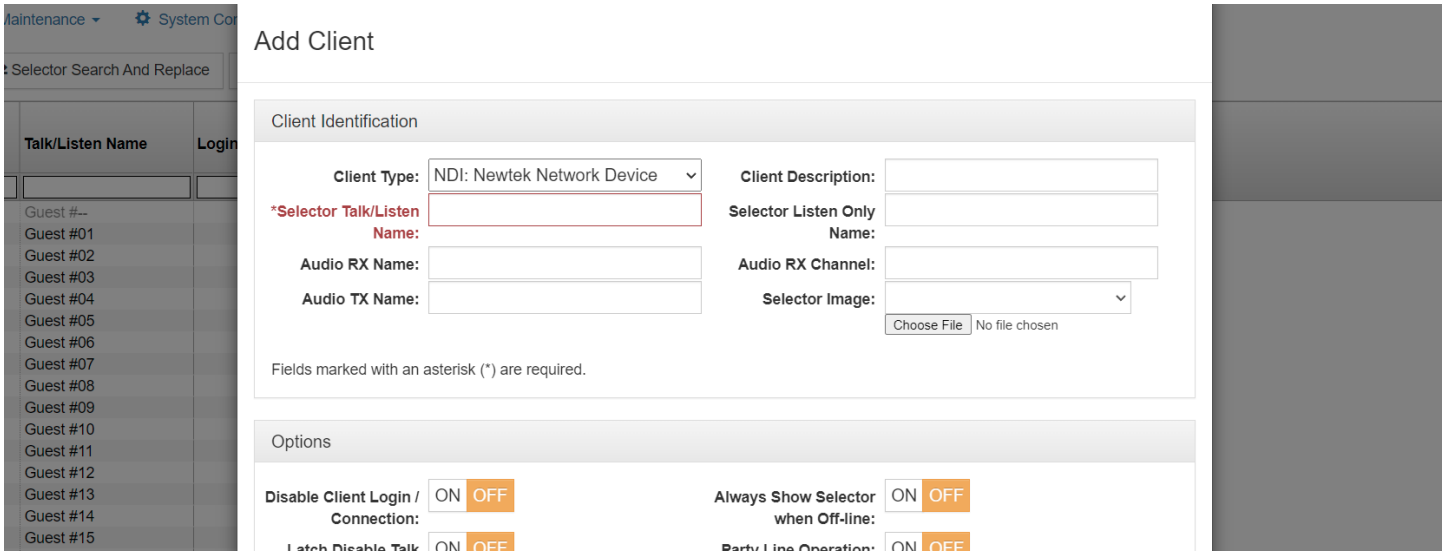
In the SIP Target Primary Host Name field enter your Voice Connector ID in the format your-voice-connector-id.voiceconnector.chime.aws.

Note: When making an outbound call from VLink 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.

Copyright Bosch Security Systems

11. Connecting NDI Audio Streams



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.

Copyright Bosch Security Systems

12. VLink Device Interface

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

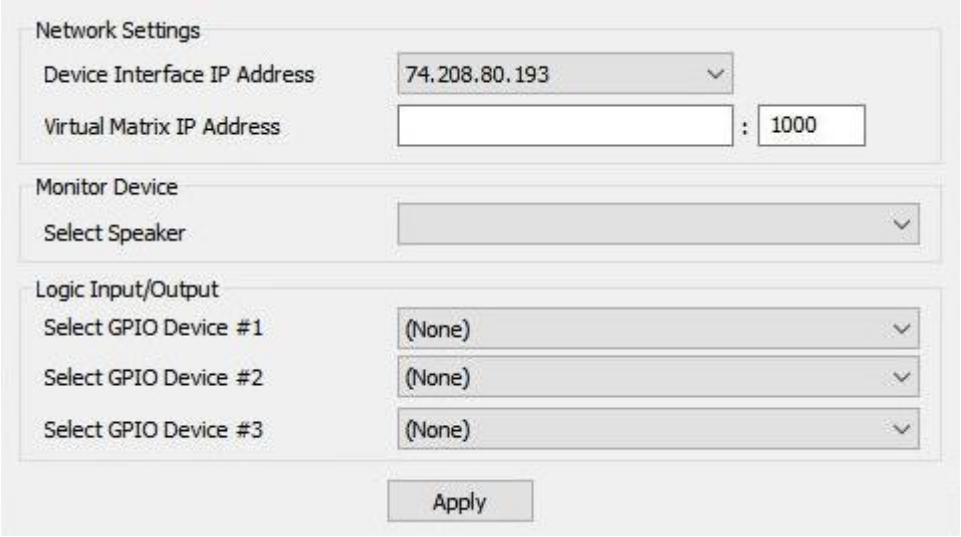
*ATS = Audio Time Slice per packet which controls how many 20ms audio frames are transmitted within a single UDP packet. As each UDP packet requires a fixed amount of overhead, the more frames sent at the same time, the less the UDP overhead which conserves network bandwidth. Conversely, the more audio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

Copyright Bosch Security Systems

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

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

12.2 Configuration



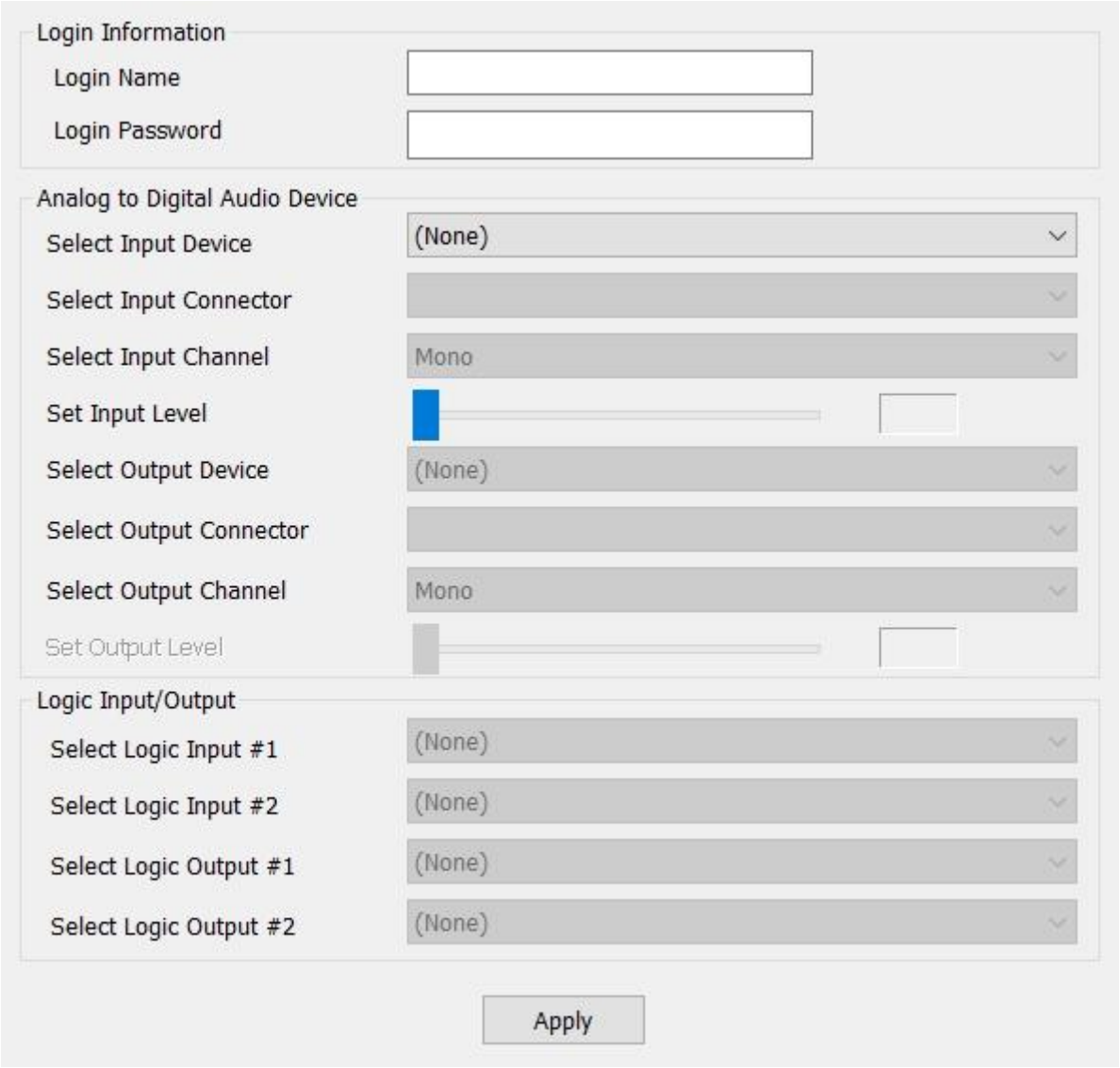
The Configuration menu will be displayed upon first launch.

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.

Copyright Bosch Security Systems



Enter the Login Name and Login Password for the device as pre-configured in the VLink 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.

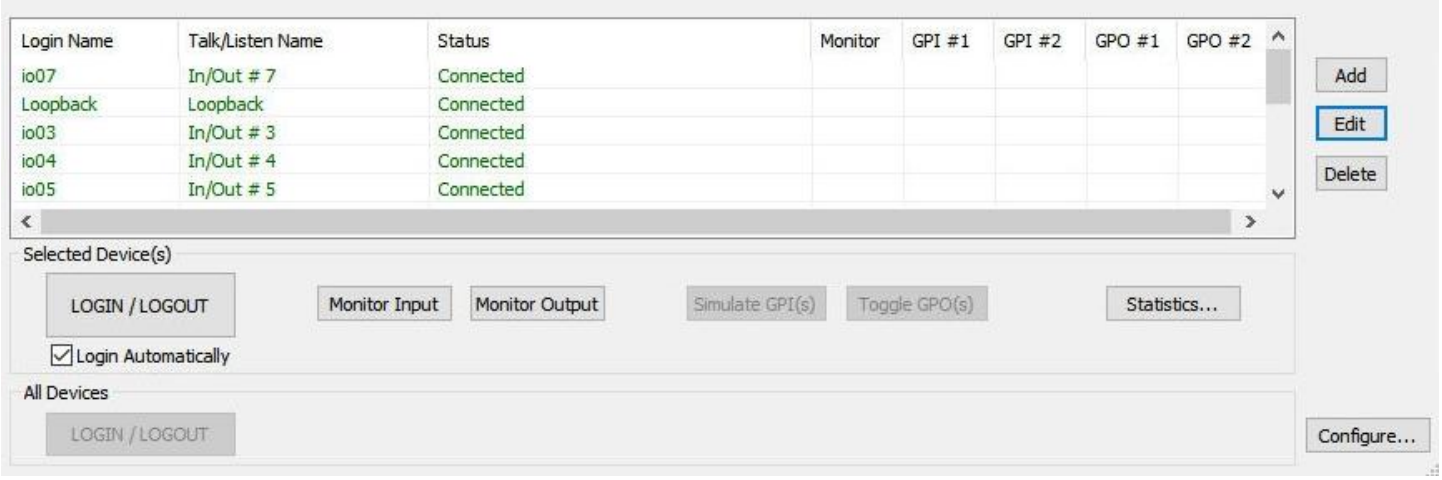
Select Input/Output Channel: Allows selection of Mono, Stereo – Left, or Stereo – Right.

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

Copyright Bosch Security Systems

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 / 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.

Copyright Bosch Security Systems

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.

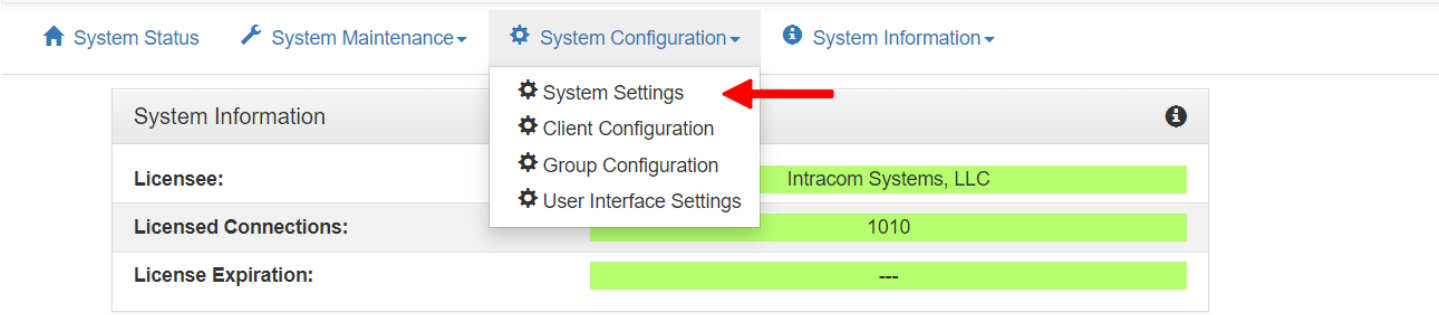
Q: When attempting to login to the Virtual Matrix, why do I get a “Provided user name and/or password is invalid!” message?
A: The Control Panel is unable to validate the username and password. Check to ensure the name is typed exactly as provided as the username and password are both case sensitive.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

Copyright Bosch Security Systems

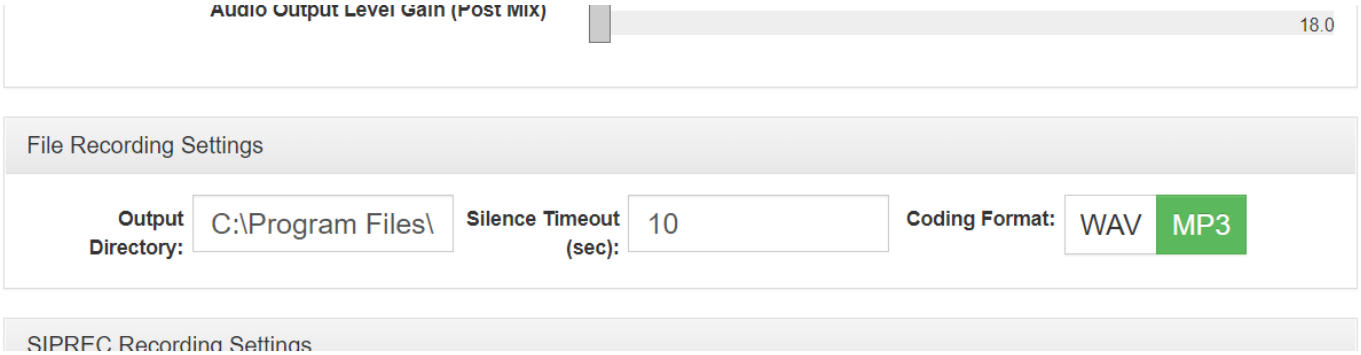
13. Audio Recording

Two different models of recording are supported in VLink. 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



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



Scroll down to the File Recording Settings section.

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

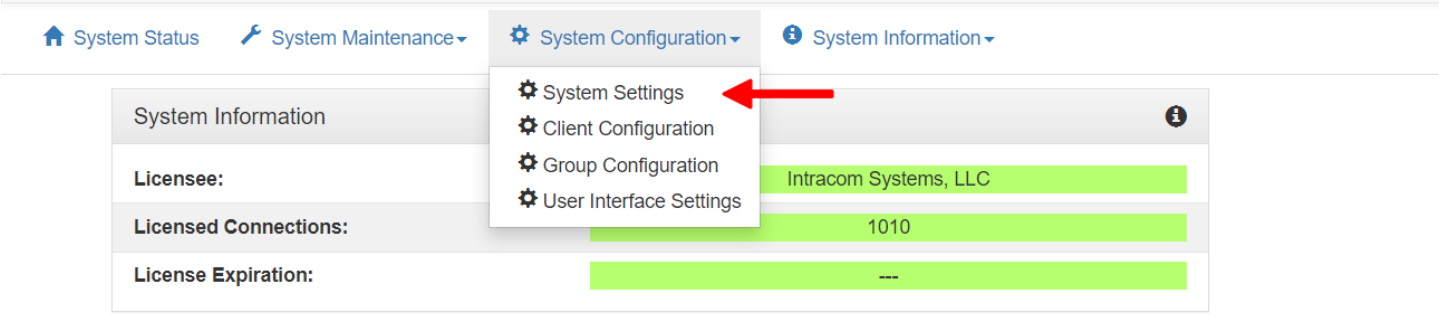
Silence Timeout (sec): The duration after silence is detected on the Client that the system will wait to end the audio recording file. The default is 10 seconds.

Copyright Bosch Security Systems

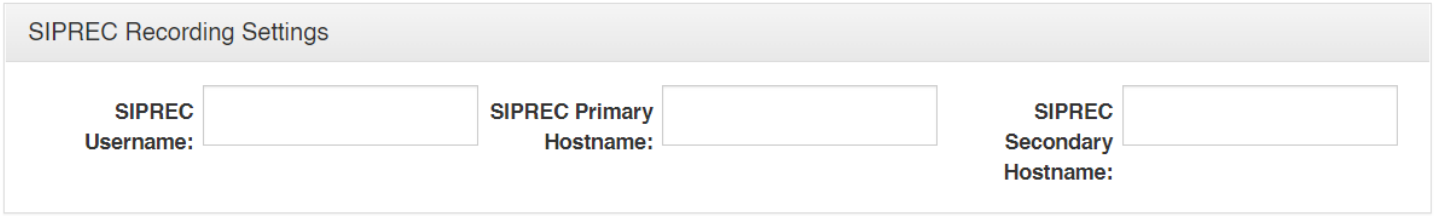
Adjust the settings if needed then click the Save button.

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



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



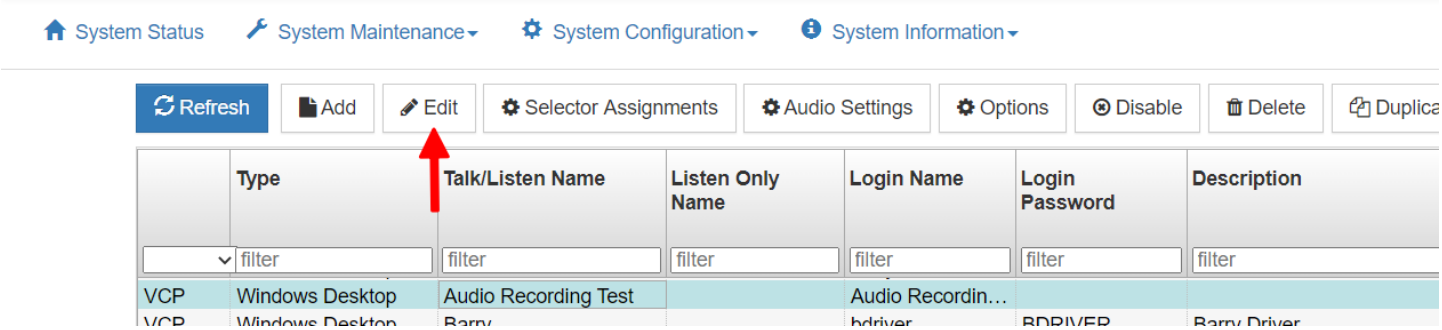
Scroll down to the SIPREC Recording Settings section and fill out the requisite fields to allow VLink Virtual Matrix to connect to your SIPREC server.

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.

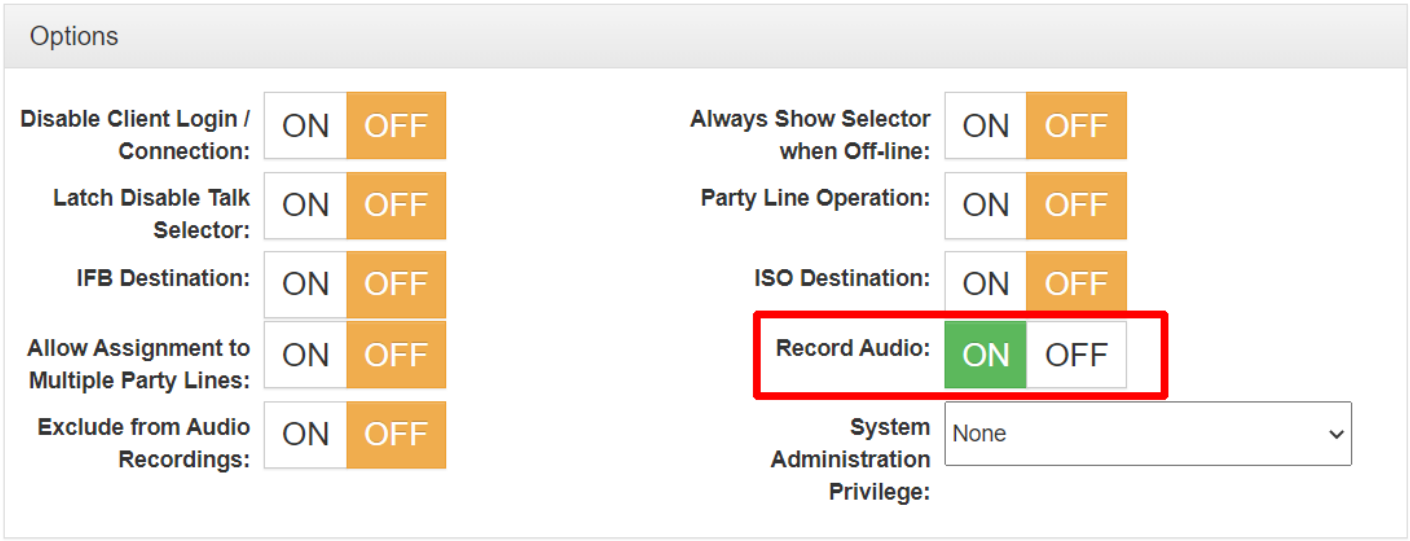
13.3 Enable Audio Recording

From the System Configuration menu select Client Configuration.

Copyright Bosch Security Systems



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



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.

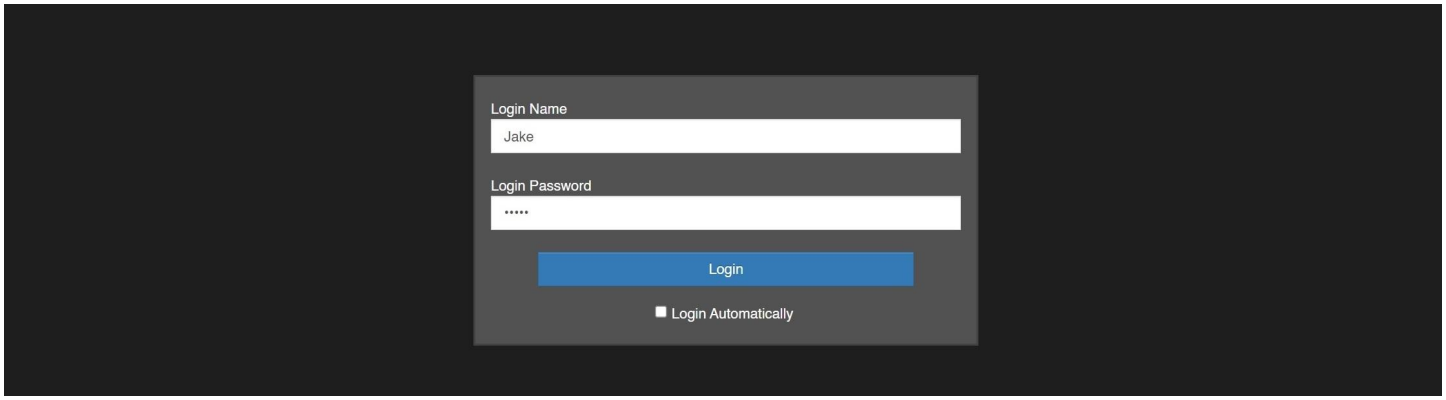
Note: The Exclude from Audio Recordings option allows a client to be excluded from recording such as a program feed so that if one is recording a client that is listening to the program feed it will record every else except the program feed.

Copyright Bosch Security Systems

14. VLink WebRTC Control Panel

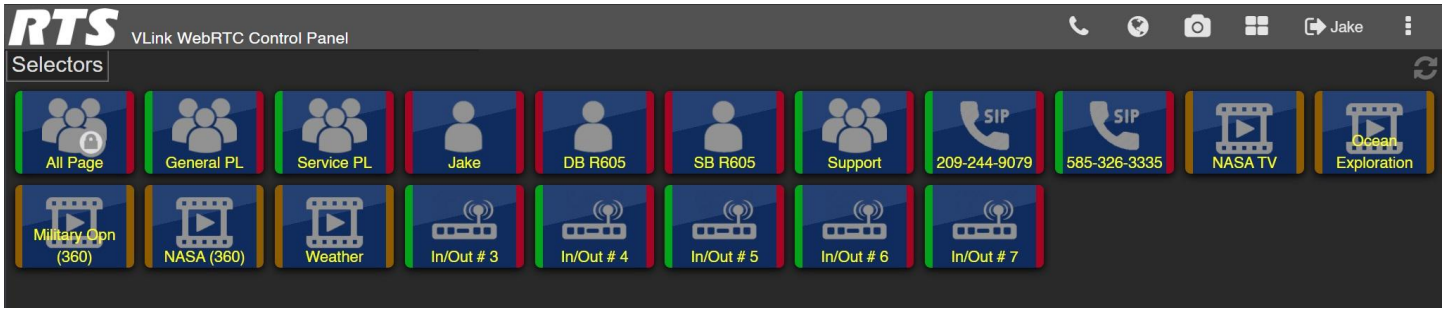
Logging In

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



VLink 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 VLink 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

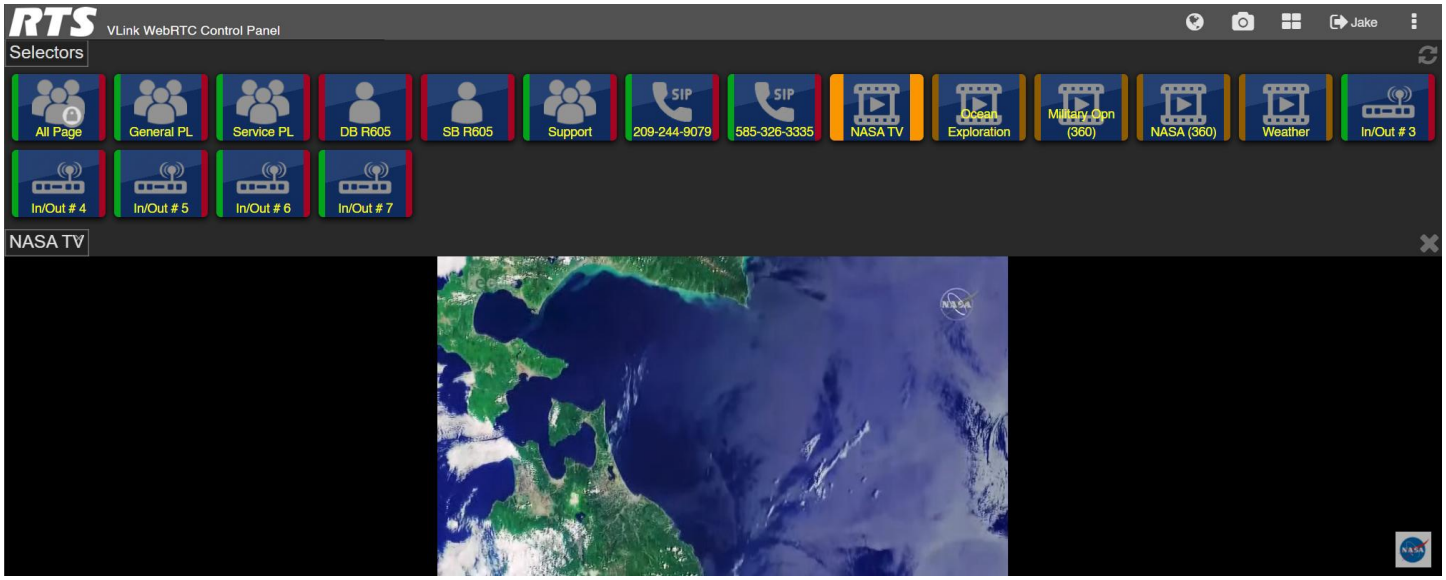
Copyright Bosch Security Systems

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.

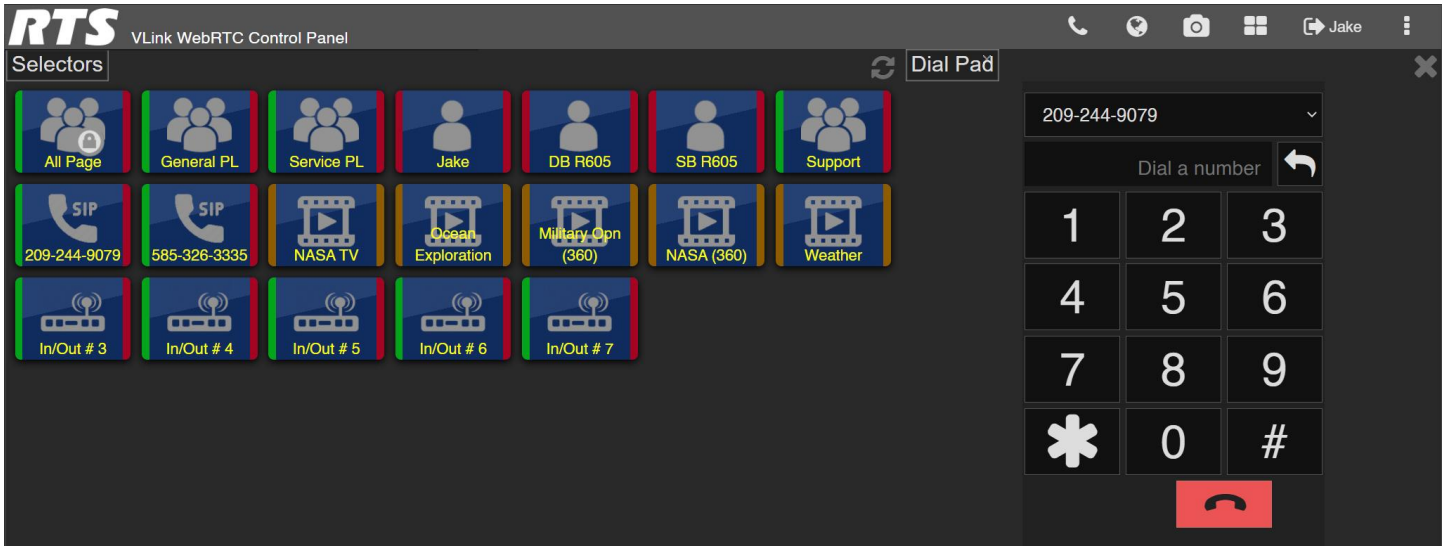
Video Selectors



Clicking on an orange selector will display its corresponding video.

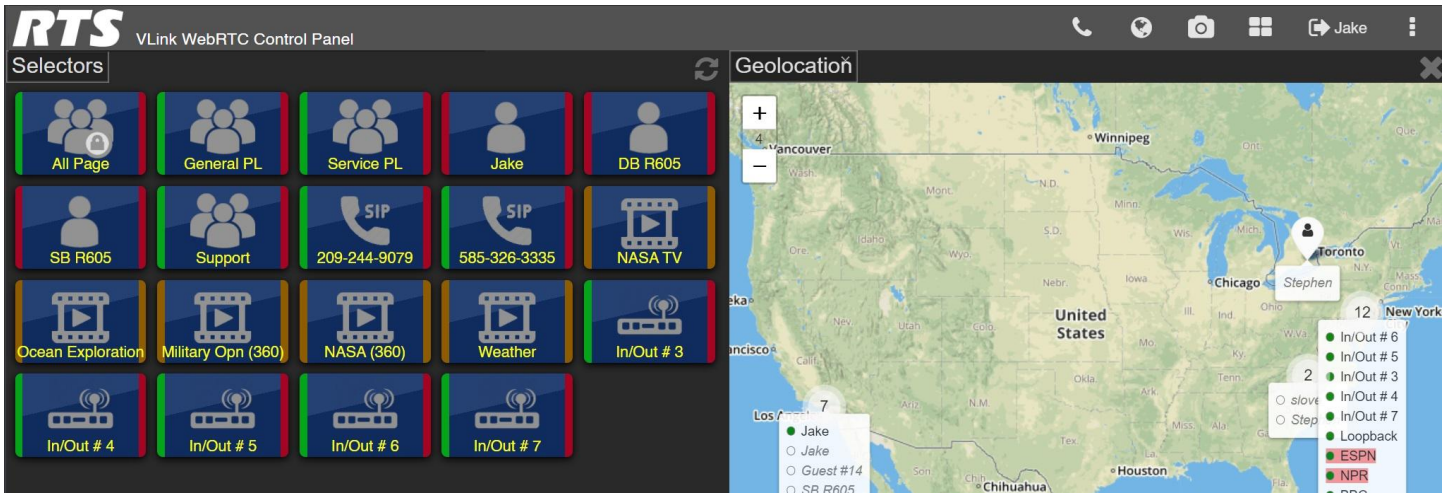
Copyright Bosch Security Systems

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.

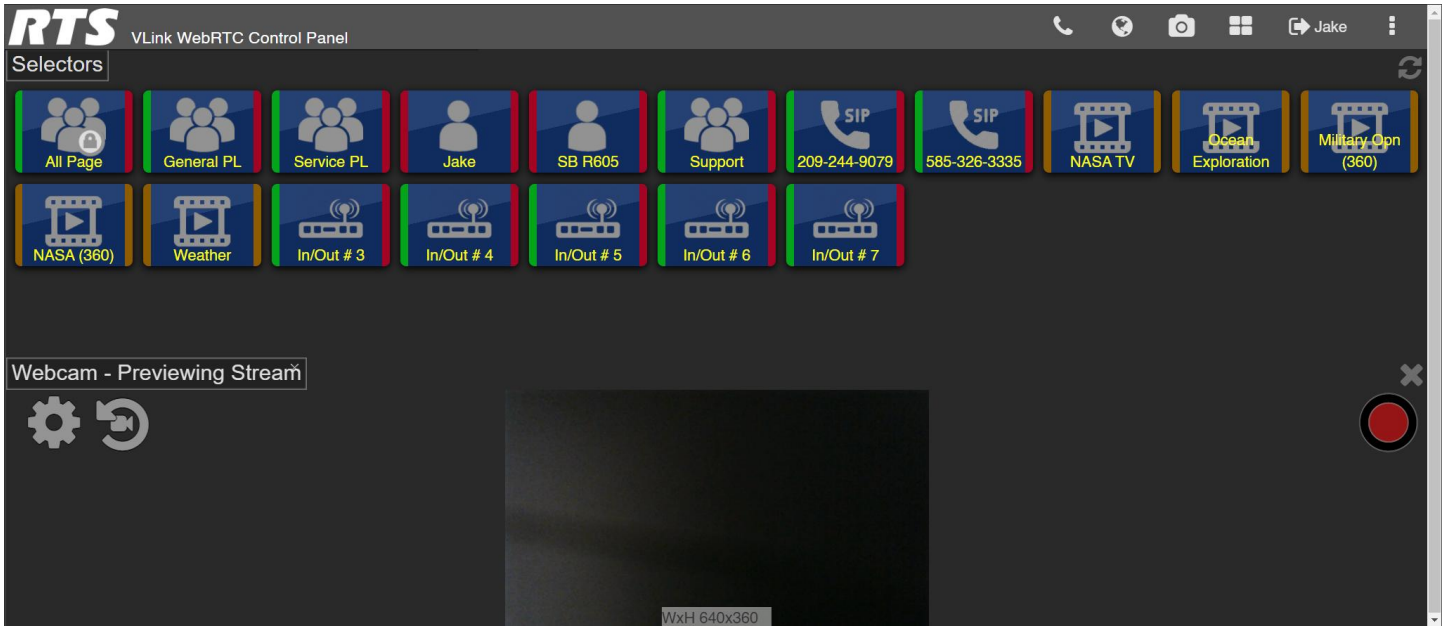
Geolocation



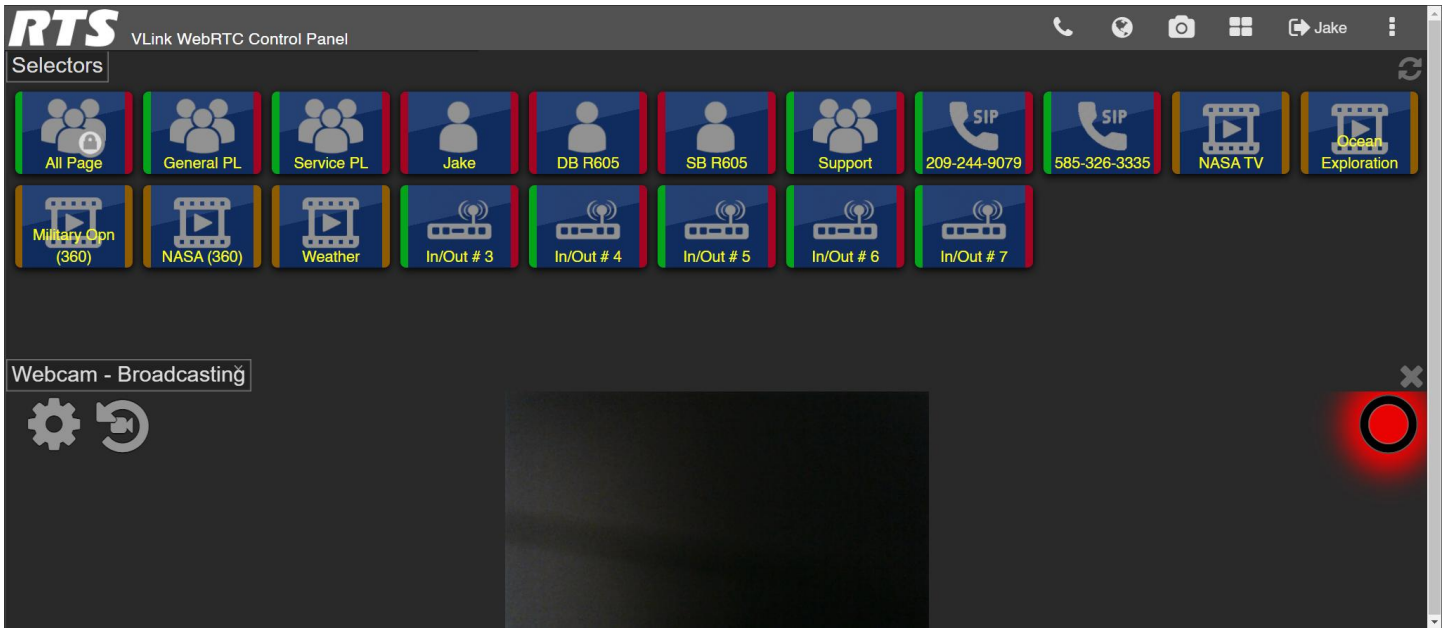
If the Client is configured in the System Administration with the "Enable Geolocation Button" set to On then a globe icon will be shown in the top bar. Pressing this button will display a global-scale map with other users appearing as pin-points beside their name along with longitude/latitude coordinates.

Copyright Bosch Security Systems

Video Streaming



If VLink 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.

Copyright Bosch Security Systems

15. VLink Interoperability with Simple Network Management Protocol (SNMP)

15.1 Installation

Prior to installing the VLink 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 VLink Virtual Matrix will automatically install and configure VLink 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 VLink Virtual Matrix (both Primary and Secondary).

15.2 Operation

The SNMP implementation is limited only to the generation of SNMP Trap messages. There is no VLink 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:

Copyright Bosch Security Systems

• VDI/SIP Client Disconnect - An SNMP Trap will be generated for every VLink 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 VLink 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.

15.3 SNMP TRAP Message Detail

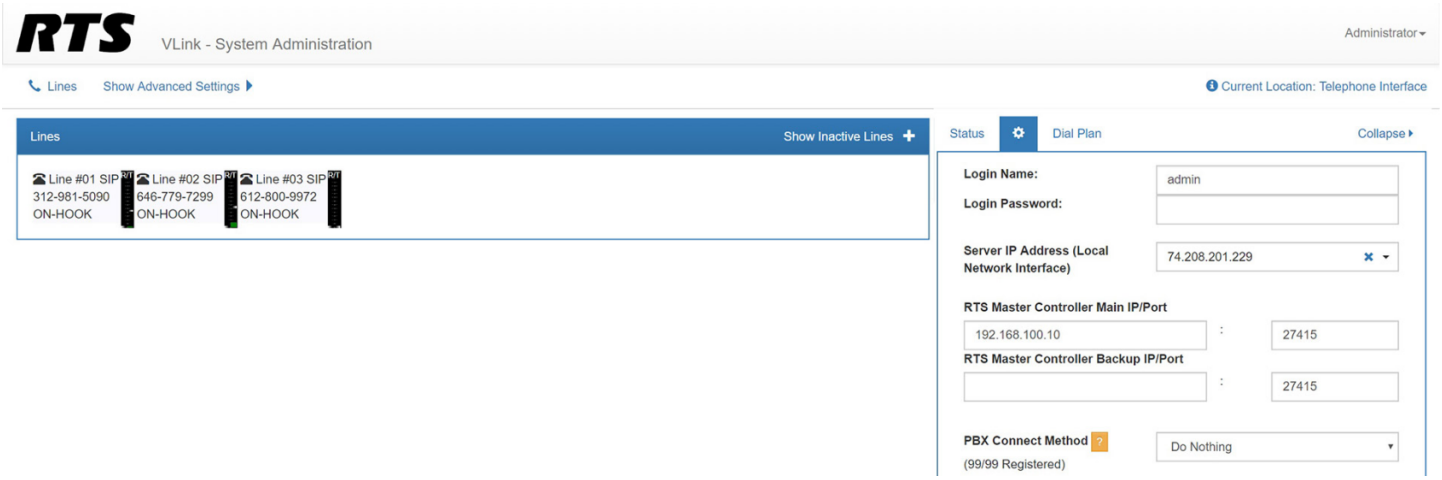
MIB Object Identifier	Message Function	Data Type (bytes)	Data Length	Data Description
1.3.6.1.4.1.41961.0.0.2	VDI/SIP Client Disconnect	Octet String	variable	Selector Name as configured in VVM
1.3.6.1.4.1.41961.0.0.3	Failover Status Change	Integer	4	0 - Failover is not licensed 1 - Failover is not configured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

Copyright Bosch Security Systems

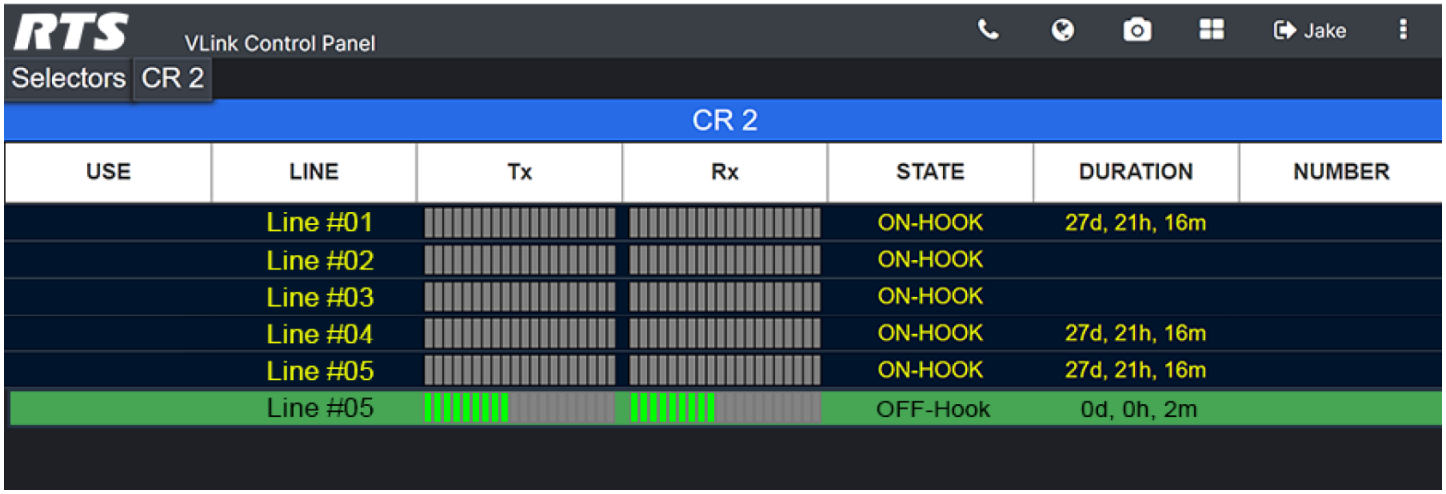
15.4 Control Rooms

Introduction

For businesses leveraging the VLink 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.



Introducing the VLink 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.

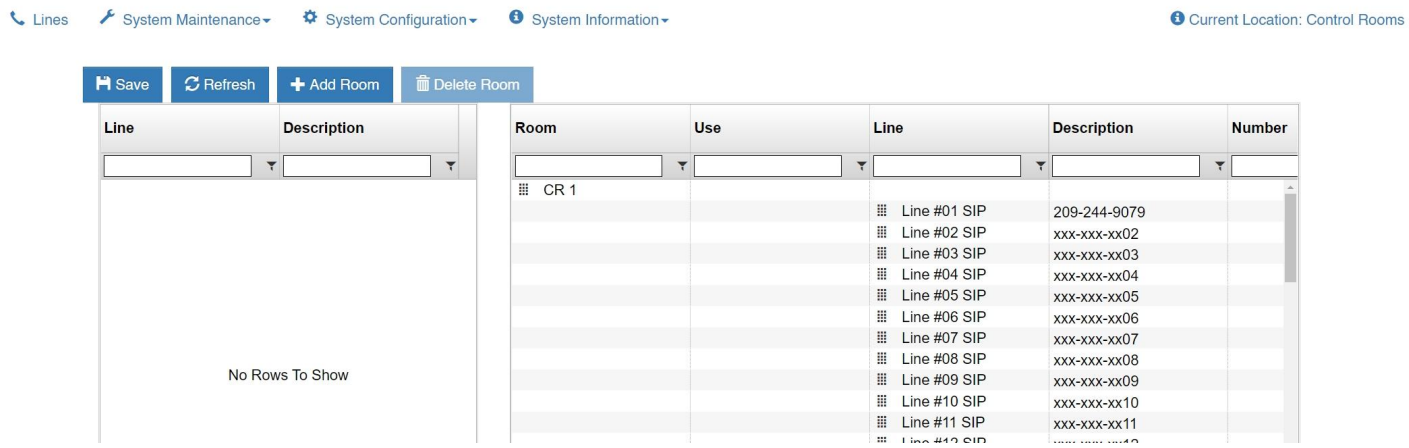


Copyright Bosch Security Systems

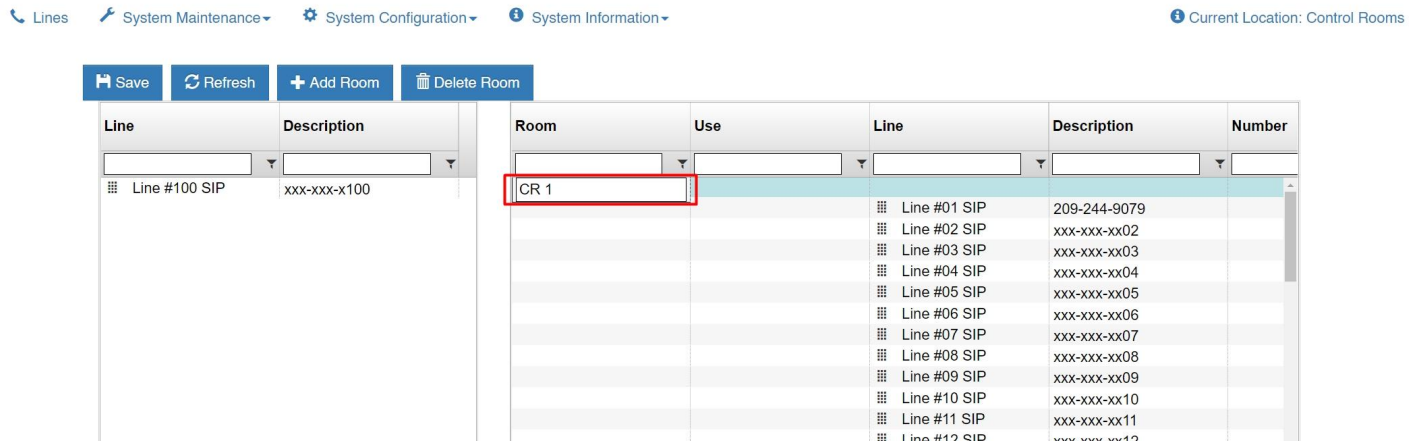
Experience unmatched monitoring ease with the VLink WebRTC Control Panel. Each room, organized into tabs, offers a streamlined view of your phone lines, allowing for quick access and real-time monitoring. This intuitive interface ensures that every call is managed efficiently, providing you with the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

To utilize the Control Rooms feature, users must first access the VLink WebRTC Control Panel. This requires an available Control Panel port on the system. It's important to note that VLink 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

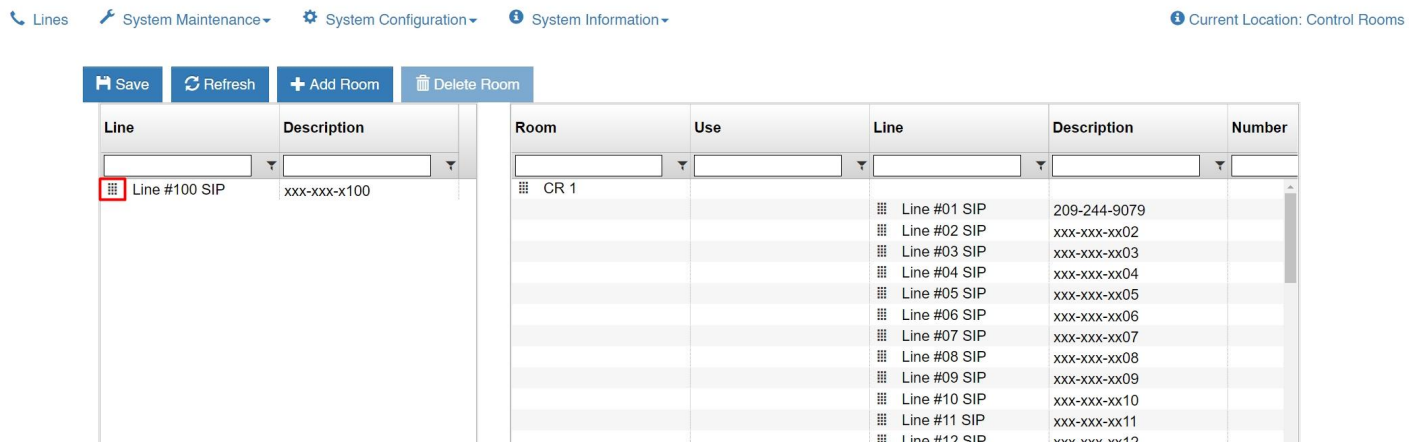


Click the Add Room button to create a new Control Room.



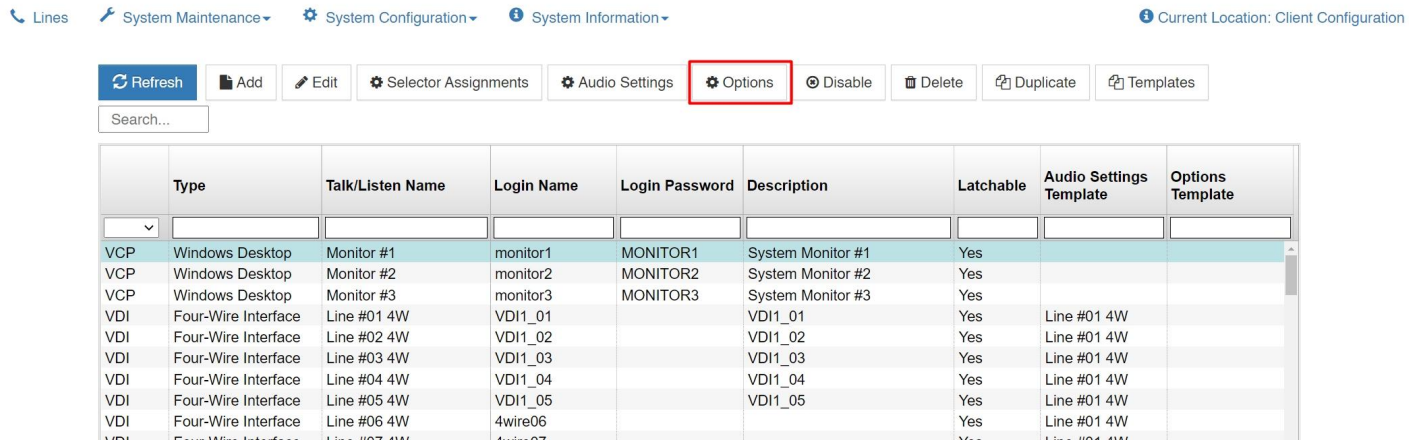
Double click the name of the Control Room to edit its name.

Copyright Bosch Security Systems

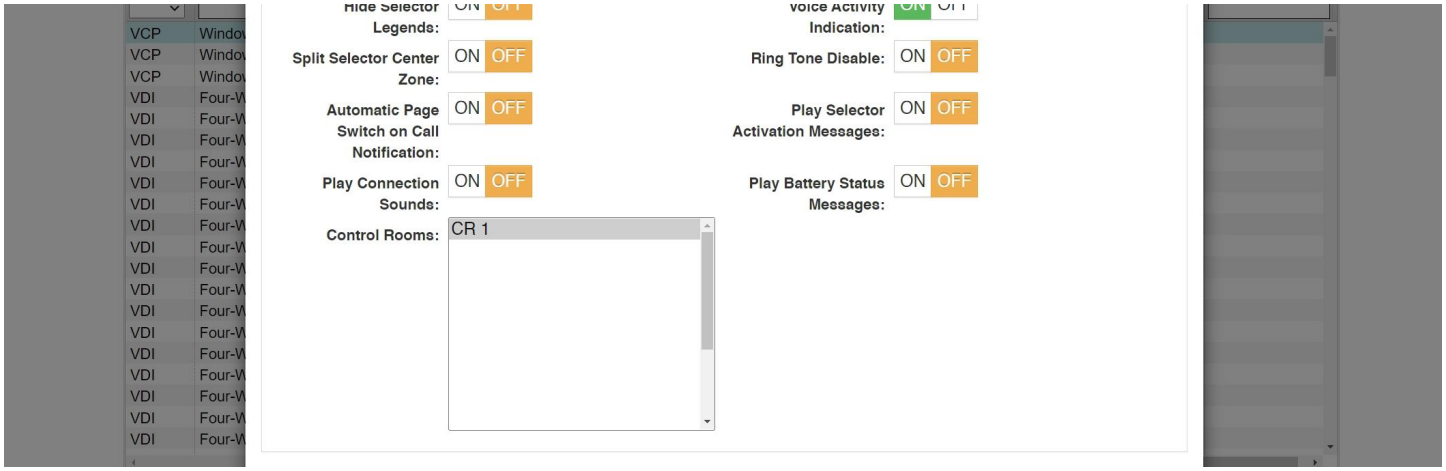


Drag a SIP line from the left side of the screen over the name of the Control Room to assign it to the room.

Assigning and Viewing the Control Room



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.



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

Copyright Bosch Security Systems

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

Control Rooms can also be monitored on Comscreen hardphones.

Copyright Bosch Security Systems